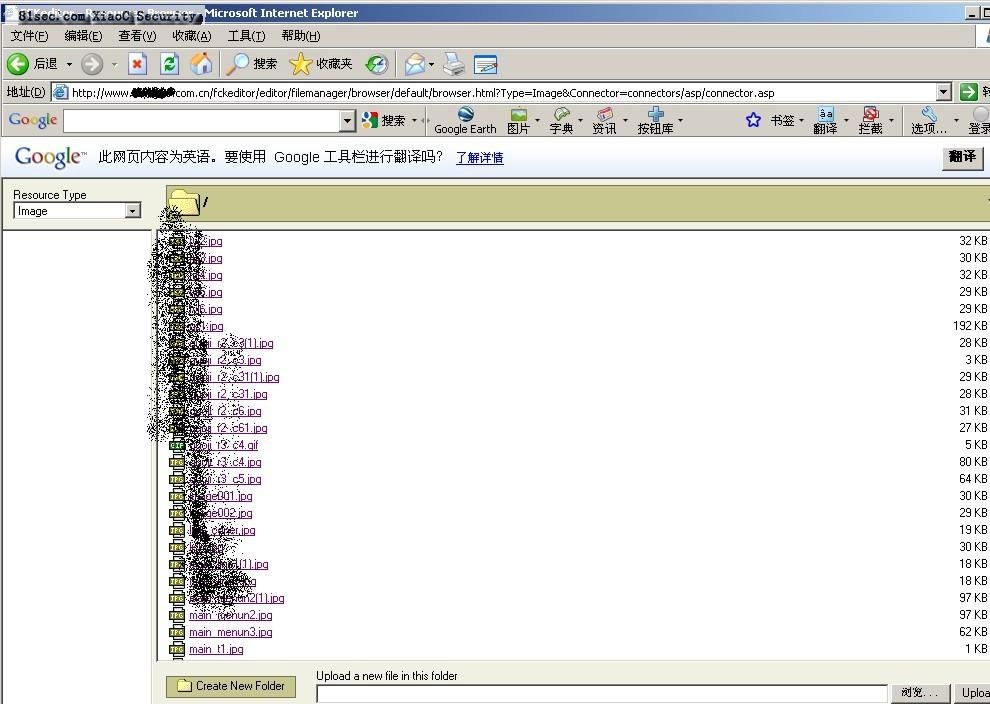
**[Fckeditor的一些漏洞总结](http://www.81sec.com/read.php/75.htm)**

2010-10-29 阅读: 146 评论: 1

转载请注明Minghacker's Blog：http://yxmhero1989.blog.163.com  
笔者将会总结前人经验，不断更新，不断发问，不断提高。  
转自闷死兄弟的博客，其实笔者也想写，只是无奈没时间，改天总结eweb吧，虽然很多人做过了。  
当然这都是网上公开过的....这次把他总结出来..放到blog上希望对大家有所帮助  
Fckeditor版本多..支持很多语言..所以本文不针对任何版本或者什么语言.只讲利用方法

fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/asp/connector.Asp

当你知道fckeditor目录时..你输入以上地址..就会看到有个上传的地方..如图所示:  
[](http://www.81sec.com/attachment.php?fid=115)  
这 里有个上传的地方...老版本的fckeditor可以上传.Asa后缀的文件(也就是你的马) 如果不行的话...我们可以利用iis的路径解析漏洞.建一个hx.Asp的目录.再这目录下上传马还可以上传“图片”.这里指的图片是.Jpg格式后缀 的马(结合iis6.0的解析漏洞hx.Asp;.Jpg)以上效果如图所示:  
[](http://www.81sec.com/attachment.php?fid=116)  
因为版本的不同..有些管理员会把一些没用的目录删除..比如我是aspx的站..就会把asp.Php的目录删了..那么这时候自己就要改

..fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/aspx/connector.Aspx

改成这样是一样的..也有时候有的站会把asp破坏掉..而这时假到aspx php都没有做任何破坏..所以有时修自己多跳下目录..browser.html?Type=Image这里image是表示类型..如果你打不开

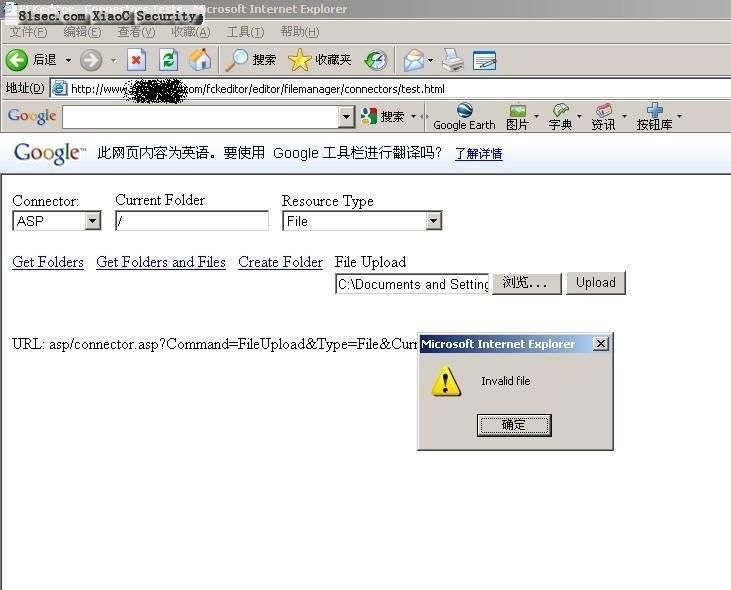
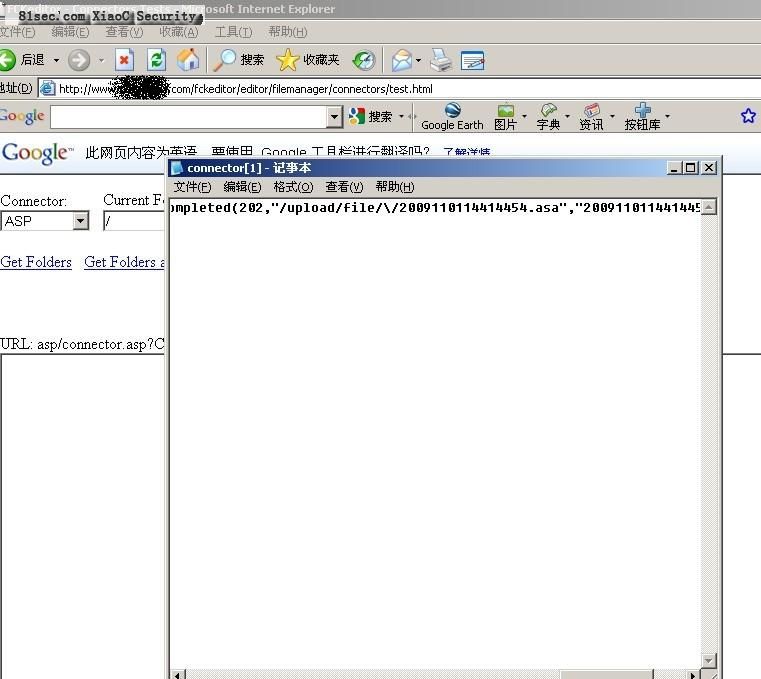
fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/asp/connector.Asp

里..可以试着打开

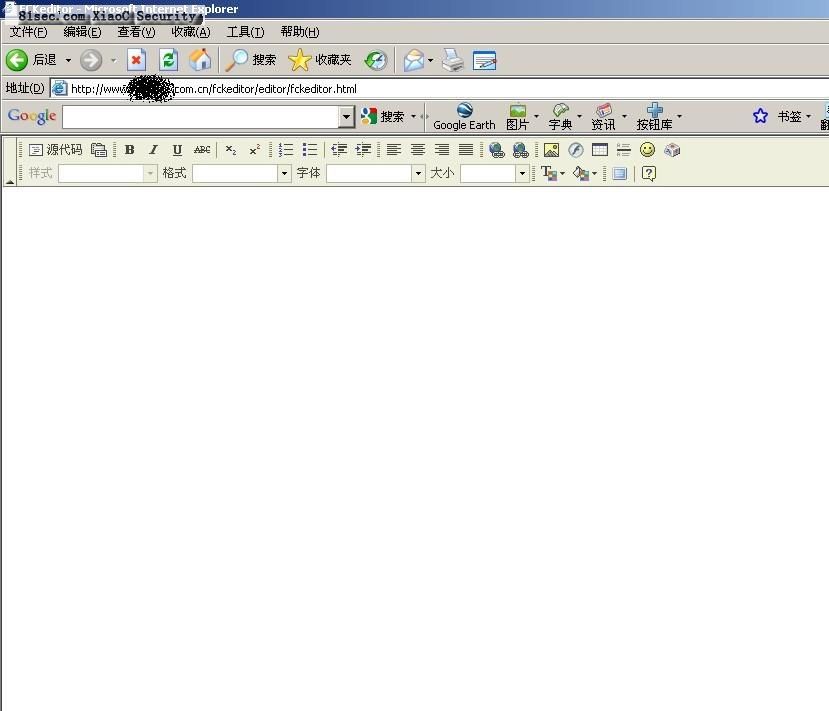
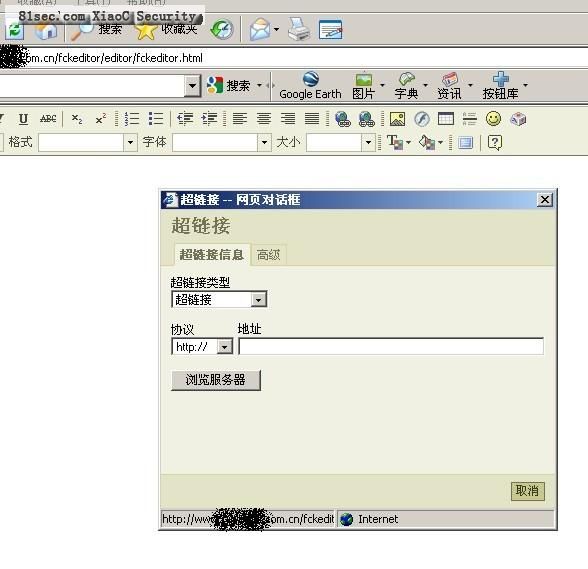
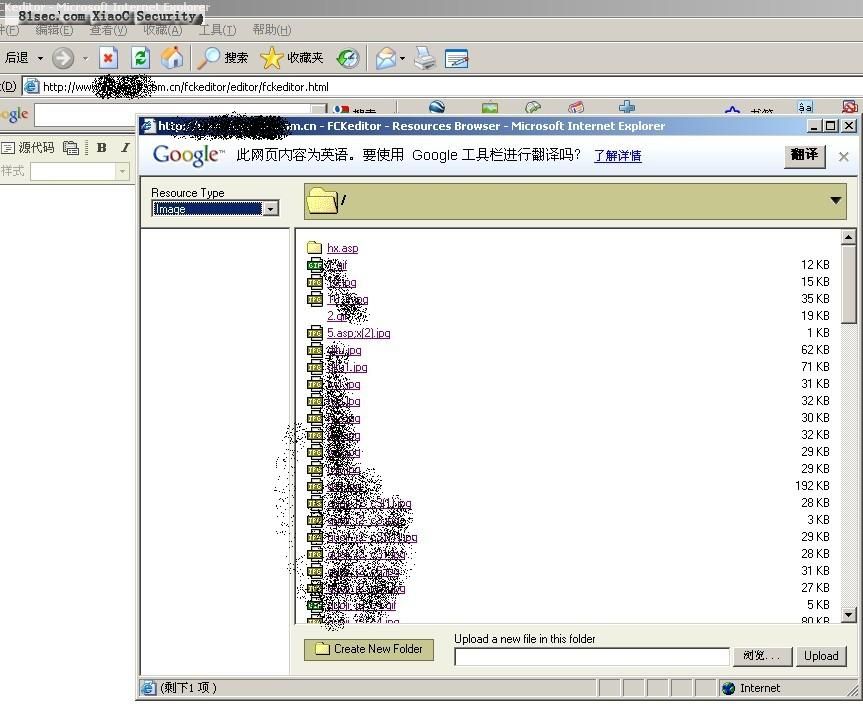
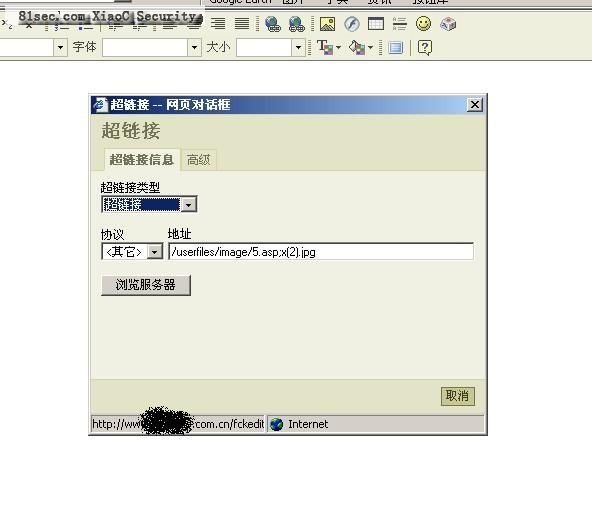
fckeditor/editor/filemanager/browser/default/browser.html?Type=file&Connector=connectors/asp/connector.Asp

..Type类型可以自己改.我没碰到过..

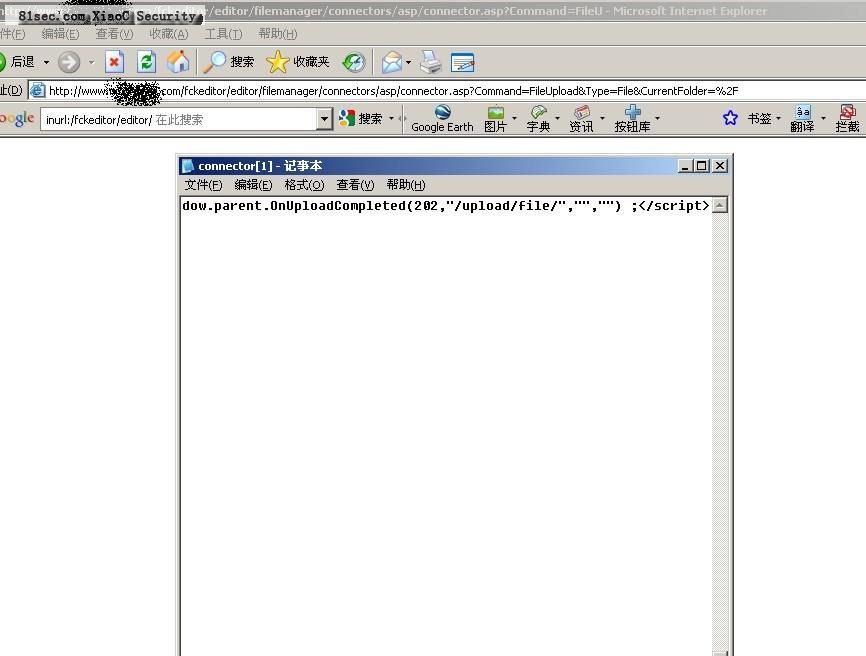
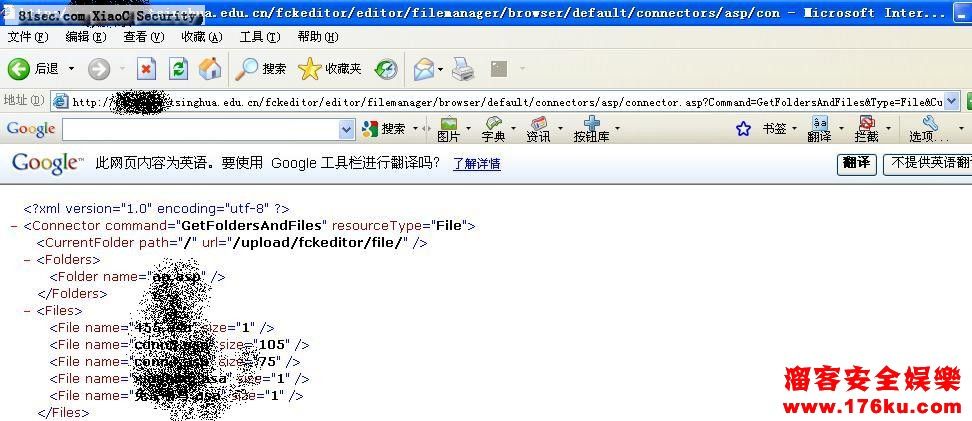
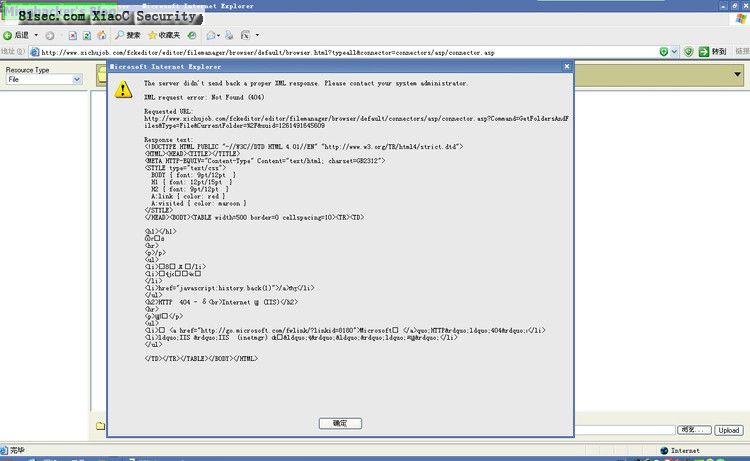
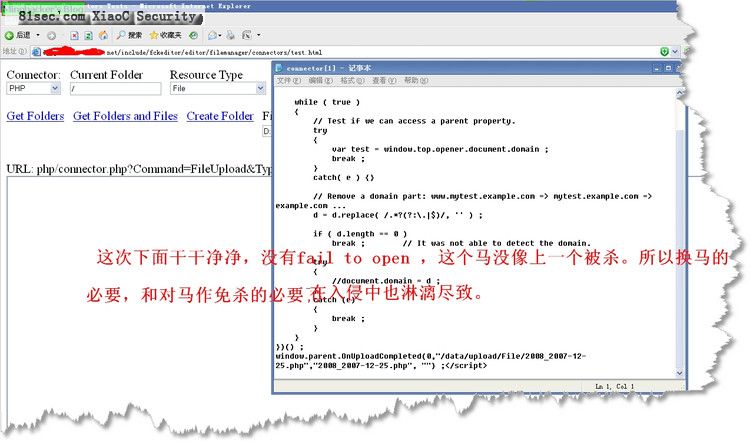
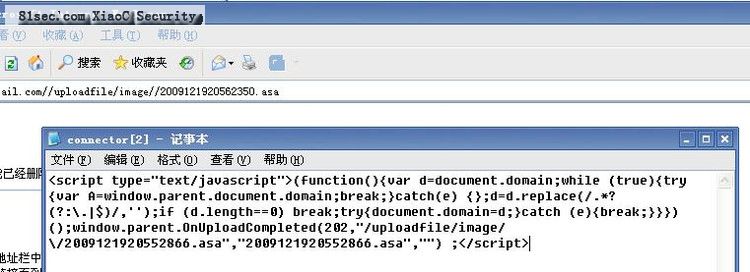
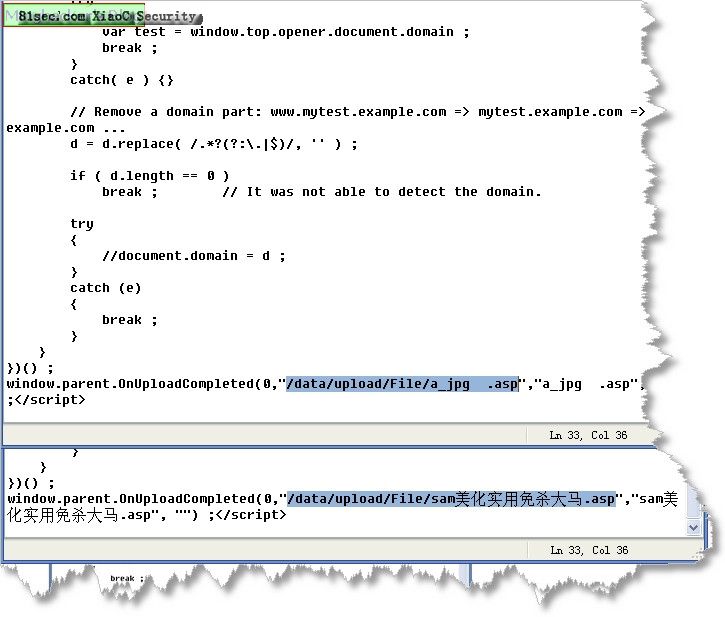
fckeditor/editor/filemanager/browser/default/browser.html?Type=../&Connector=connectors/asp/connector.Asp

这样的可以跳到根目录...很少碰到...不过也不是不存在这样的站...这里也可以把全站目录列出来..那么这样都被破坏了..也都不行了...那要怎么办呢..在connectors目录下有个test.Html  
文件..那里也可以上传..可以上传任意文件他都会返回一个地址给你..如图所示：  
[](http://www.81sec.com/attachment.php?fid=117)  
虽然是返回不允许上传的类型..但还是会返回地址..那个路径是在下面框里查看源文件得到的...  
[](http://www.81sec.com/attachment.php?fid=118)  
上传cer有时候也行.hx.Jpg;hx.Jpg 都行...在test.Html页面里有几个地方要注意..  
Connector 也就是Connector=connectors/asp/connector.Asp是一个样的哈..有aspx php  
等..其实都只是调用..如果asp不行..换aspx php 同上方法...还有一个是本地构造上传  
的源码如下:

<form id="frmUpload" enctype="multipart/form-data" action="http://www.xxx.com.cn/fckeditor/editor/filemanager/browser/default/connectors/asp/upload.asp?Type=Media" method="post">  
Upload a new file:<br>  
<input type="file" name="NewFile" size="50"><br>  
<input id="btnUpload" type="submit" value="Upload">  
</form>

没 了test.Html这里也还可以上传..一样的效果..有些网站的connectors/asp/upload.Asp 所在的目录不一定相同...有的是fckeditor/editor/connectors/asp/upload.Asp这路径..And so on 补上一个知识...有时候上传的木马名hx.Asp;hx.Jpg hx.Asp这个时候会被过滤掉前面的.我们可以把.进行url编码下成%2E（成功机率没测试过）  
   下面就是找路径的方法了...上传上去的马别找不到路径那就完了..在  
fckeditor/editor/目录下有个fckeditor.Html文件..我们访问如图所示:那么我们怎么找  
上传马的路径呢??我们打开上面一个超链接的按钮..如图所示：  
[](http://www.81sec.com/attachment.php?fid=119)  
有个浏览服务器..我们打开.如图所示:  
[](http://www.81sec.com/attachment.php?fid=120)  
找到自己的马点两下你就会发现马的路径已经在你面前了...如图所示：  
[](http://www.81sec.com/attachment.php?fid=121)  
[](http://www.81sec.com/attachment.php?fid=122)  
里面有个图片上传(同理)  
那么要是没有这个fckeditor.Html 或者fckeditor.Html打开是“空白页面”呢？我们还有种方法来列出目录..如图所示:

fckeditor/editor/filemanager/connectors/asp/connector.asp?Command=FileUpload&Type=File&CurrentFolder=%2F

这是列出file目录的路径.有的可以列..当然版本不同  
[](http://www.81sec.com/attachment.php?fid=123)  
[](http://www.81sec.com/attachment.php?fid=124)  
有的显示不同..也有的不能列出来..还有种是那个本地构造的上传怎么找马...当你按下  
upload按钮时就会跳到一个页面..右键查看源文件就可以知道路径了...再还有网上的一  
种用遨游浏览器的方法..比较麻烦...呵呵...还有种方法就是经验的老道了...也可以扫全  
站目录来猜你马的目录路径...And so on  
好了总结的也差不多了..如果我哪里没有总结到..请大家指出来... Php jsp等那些版本  
的漏洞..精简版的国内很少了吧.国外的有蛮多的...这里都不提了...  
Minghacker补充：  
fck修复过的就没搞头了，如图  
[](http://www.81sec.com/attachment.php?fid=125)  
fckeditor/editor/filemanager/connectors/test.html方法实战中会出现一些问题。  
[](http://www.81sec.com/attachment.php?fid=126)  
具体路径自己把握，另外，上面典型的是马儿被杀，找到路径却打不开，这个时候换马是最好方法  
[](http://www.81sec.com/attachment.php?fid=127)  
这个成功进去。  
对于下面这个用catch（e）函数做安全的过滤的，绝对路径找到也打不开，目录里根本不存在这个马，难道这个asa马显示是假的？笔者严肃思考中。最可能是被杀了，或不支持asa的。   
[](http://www.81sec.com/attachment.php?fid=128)  
建议马的名称不要使用中文，用数字和英语是可以的，譬如下图，就是对比，中文名称马访问不了。貌似这个和2b的直接上传还是有点差距的。  
[](http://www.81sec.com/attachment.php?fid=129)  
最新出来个上传hx.asp;jpg的传法，未测试。  
后来又出现“畸形文件上传”？  
ASP的可以拿到，PHP和JSP的貌似不行  
[](http://www.81sec.com/attachment.php?fid=130)  
[](http://www.81sec.com/attachment.php?fid=131)  
成功上传。.被改成了下划线，这样我们就没法利用了。我么可以访问试下，没用。好了，看操作。  
[](http://www.81sec.com/attachment.php?fid=132)  
什么也不管，还是那个文件，继续传。出现这个的意思是，服务器上已经有这个文件了，程序将其改名为1.asp;g(1).jpg 。这样我们的目的就达到了。我们访问看看。呵呵，当脚本执行了。

**相关日志**