**PRACTICAL NO 6**

**AIM :** Persistent Cross-Site Scripting Attack

• Set up a vulnerable web application that is susceptible to persistent XSS attacks.

b• Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code.

• Observe the consequences of the attack and understand the potential risks associated with XSS vulnerabilities.

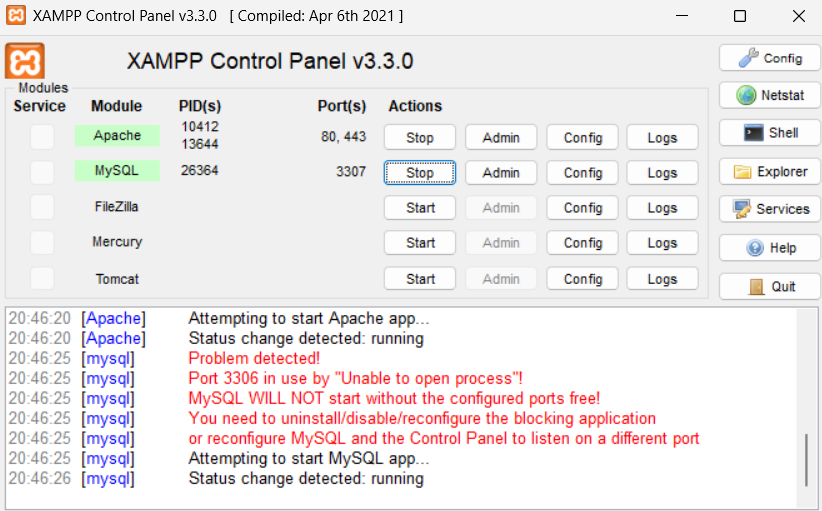
**SOLUTION:**

**Step 1:** Download DVWA from the [DVWA GitHub Repository](https://github.com/digininja/DVWA).

**Step 2 :** Extract the DVWA folder to your web server's root directory, Place the folder inside C:\xampp\htdocs\

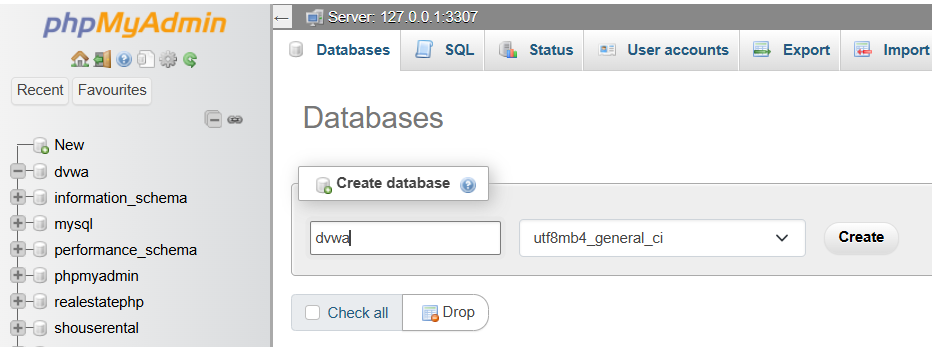
**Step 3 :** Download and install XAMPP Server from the website : <https://www.apachefriends.org/download.html>

**Step 4 :** Open the XAMPP server and start Apache and Mysql by clicking on start



**Step 5 :** Open your browser and navigate to the <http://localhost/phpmyadmin> website to open PhpMyAdmin

**Step 6 :** Click on New to create a database ,give the name of the database as ‘dvwa’ and click on create.



**Step 7 :** Edit the config/config.inc.php file in the DVWA folder to configure your database connection.

Make the following changes in the file

$\_DVWA = array();

$\_DVWA[ 'db\_server' ]   = '127.0.0.1';

$\_DVWA[ 'db\_database' ] = 'dvwa';

$\_DVWA[ 'db\_user' ]     = 'root';

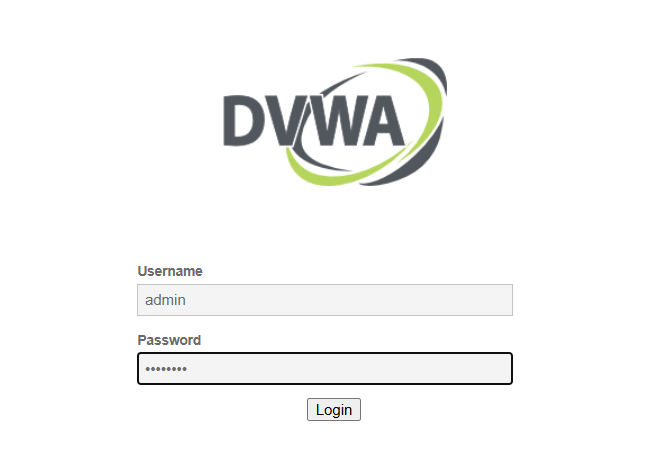
$\_DVWA[ 'db\_password' ] = 'root123';

$\_DVWA[ 'db\_port']      = '3306';

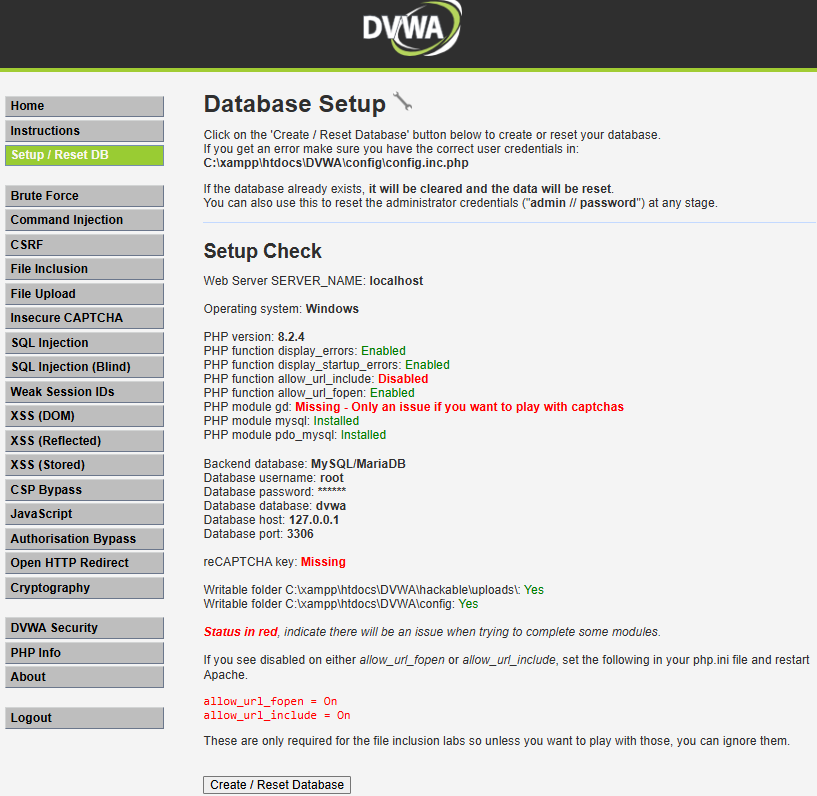
**Step 8 :** Navigate to <http://localhost/dvwa/setup.php> in your web browser to complete the setup.

**Step 9 :** log in to the application using the default credentials:

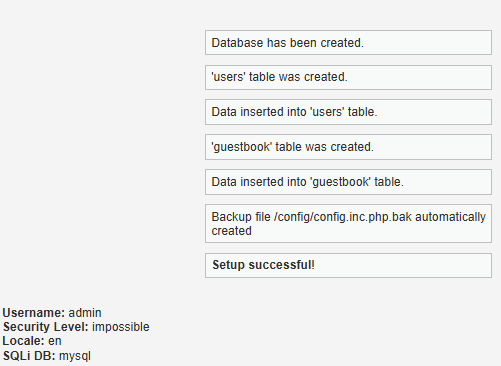
Username: admin , Password: password



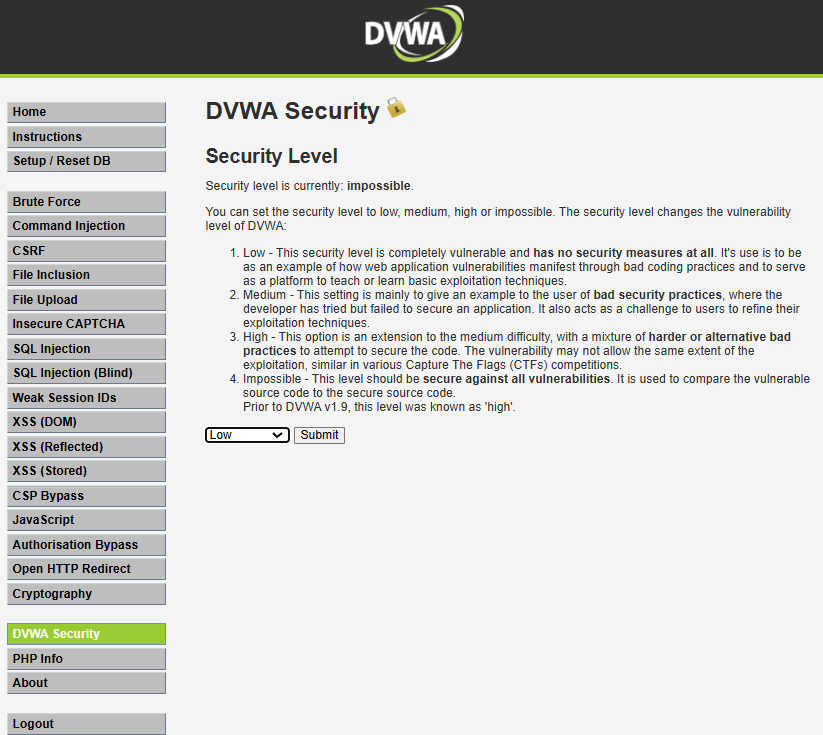
**Step 10 :** Click on Create/ Reset Database



**Step 11 :** You will see the following result

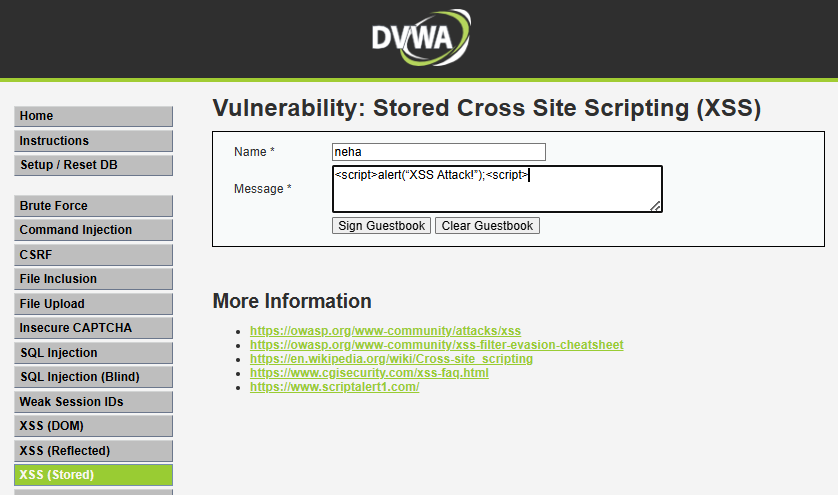


**Step 12 :** Now click on DVWA Security option on the left and set the security level as low and click on submit.



**Step 13 :** Click on the XSS (Stored) option on the left , Fill the name and write script code in message as follows:

<script>alert(‘XSS Attack!’);<script>



**Step 14 :** Click on Sign Guestbook

