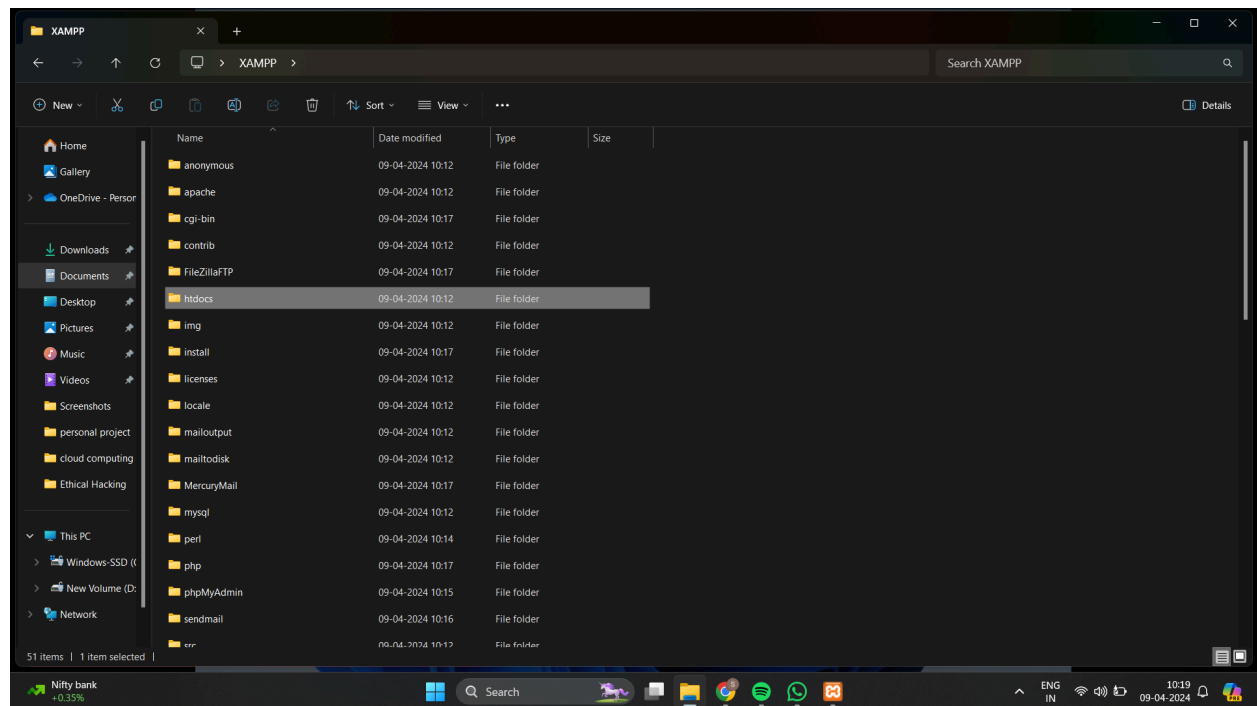
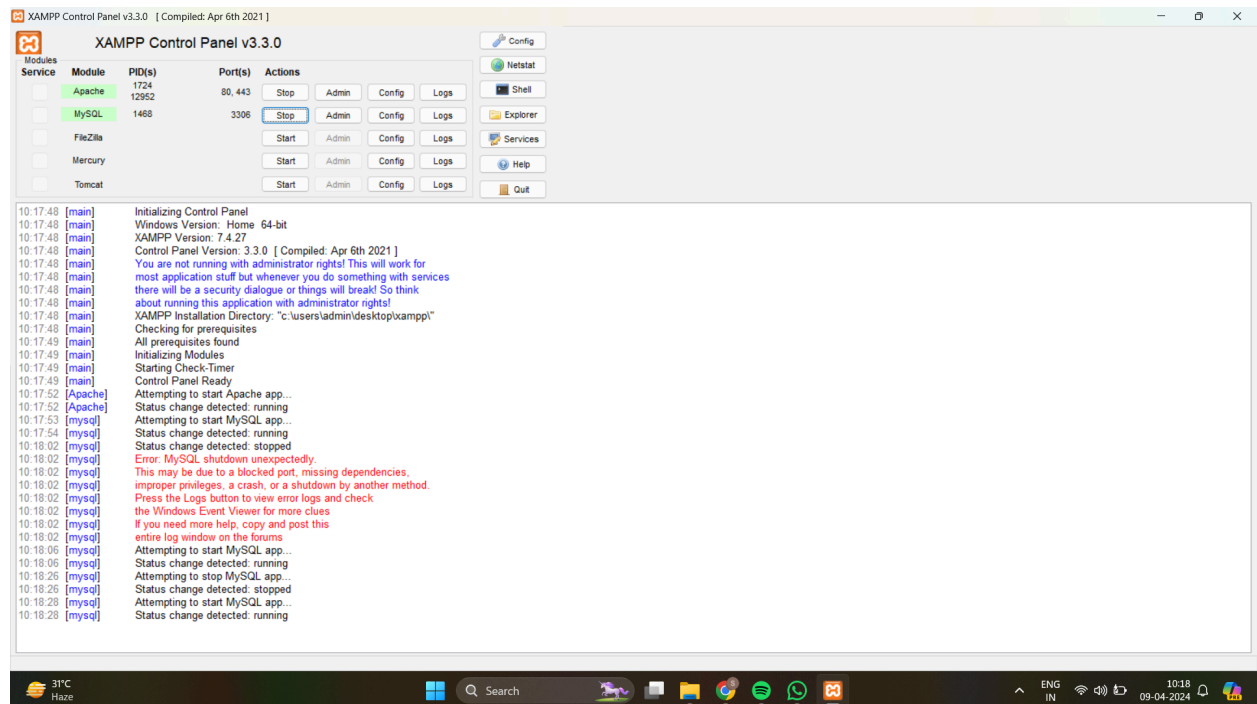


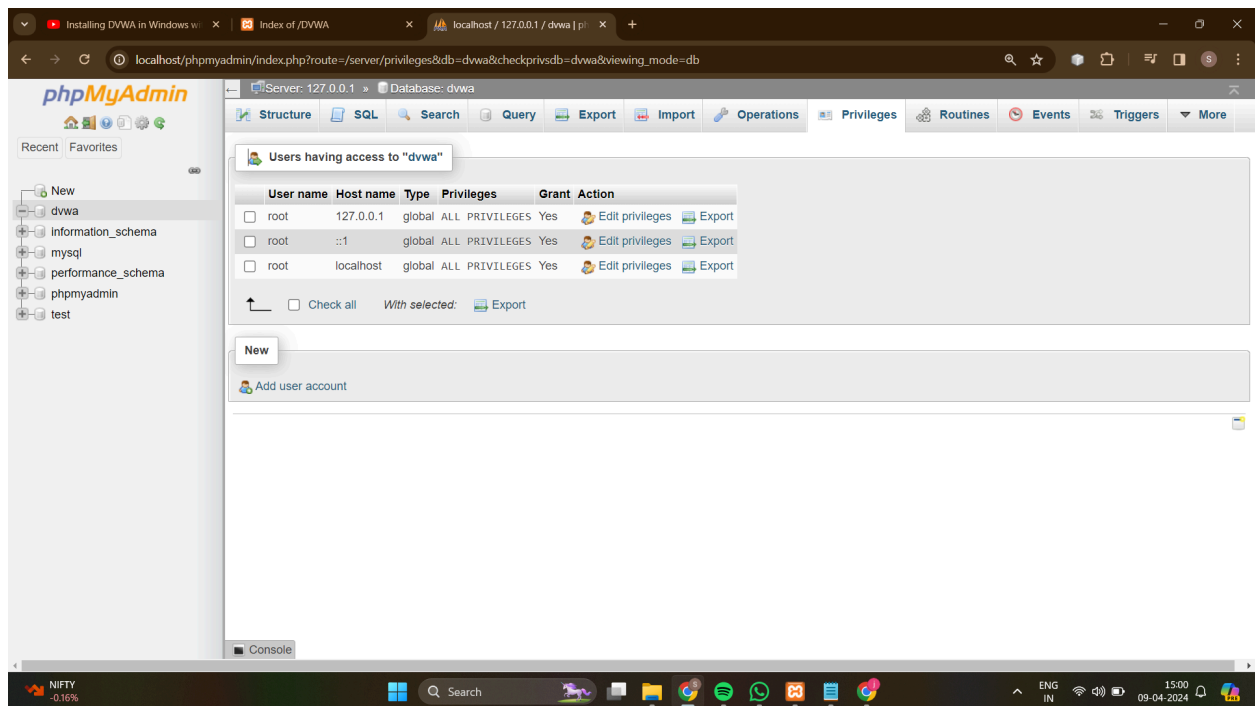
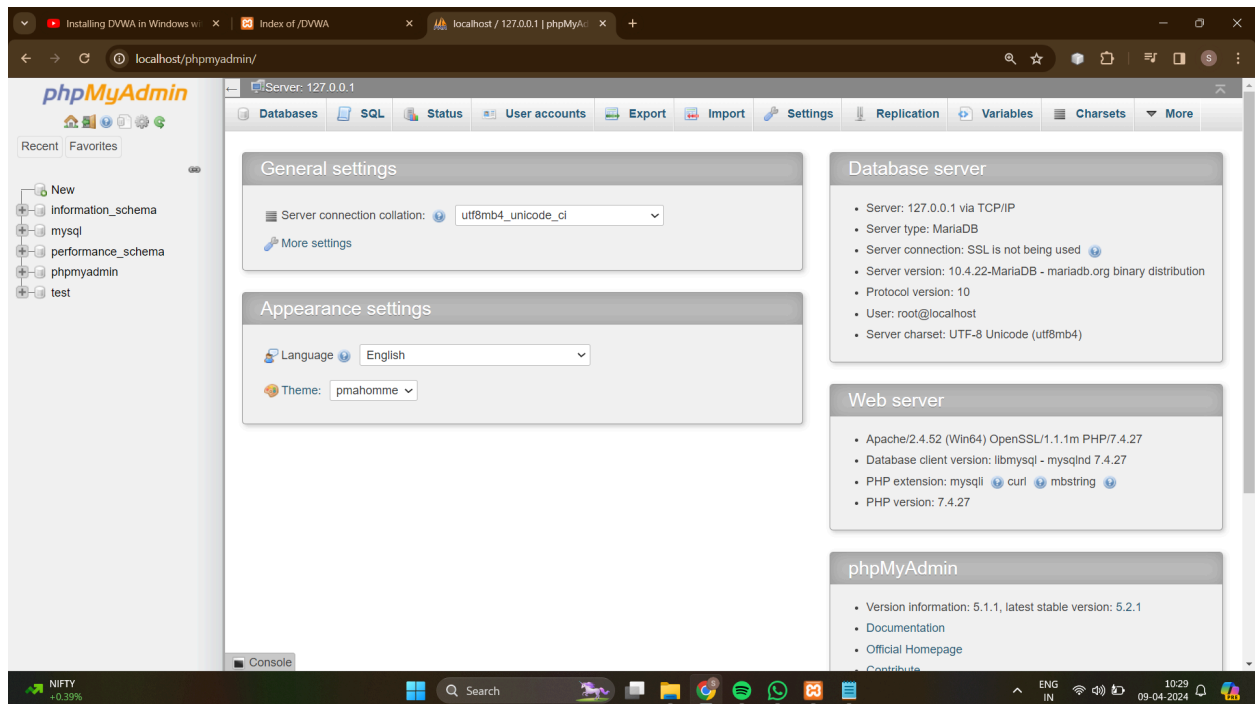
Sheth L.U.J. College Of Arts & Sir M.V. College of Science & Commerce

Department Of Science

Jayesh mali T084 Pract_ 8 Ethical hacking



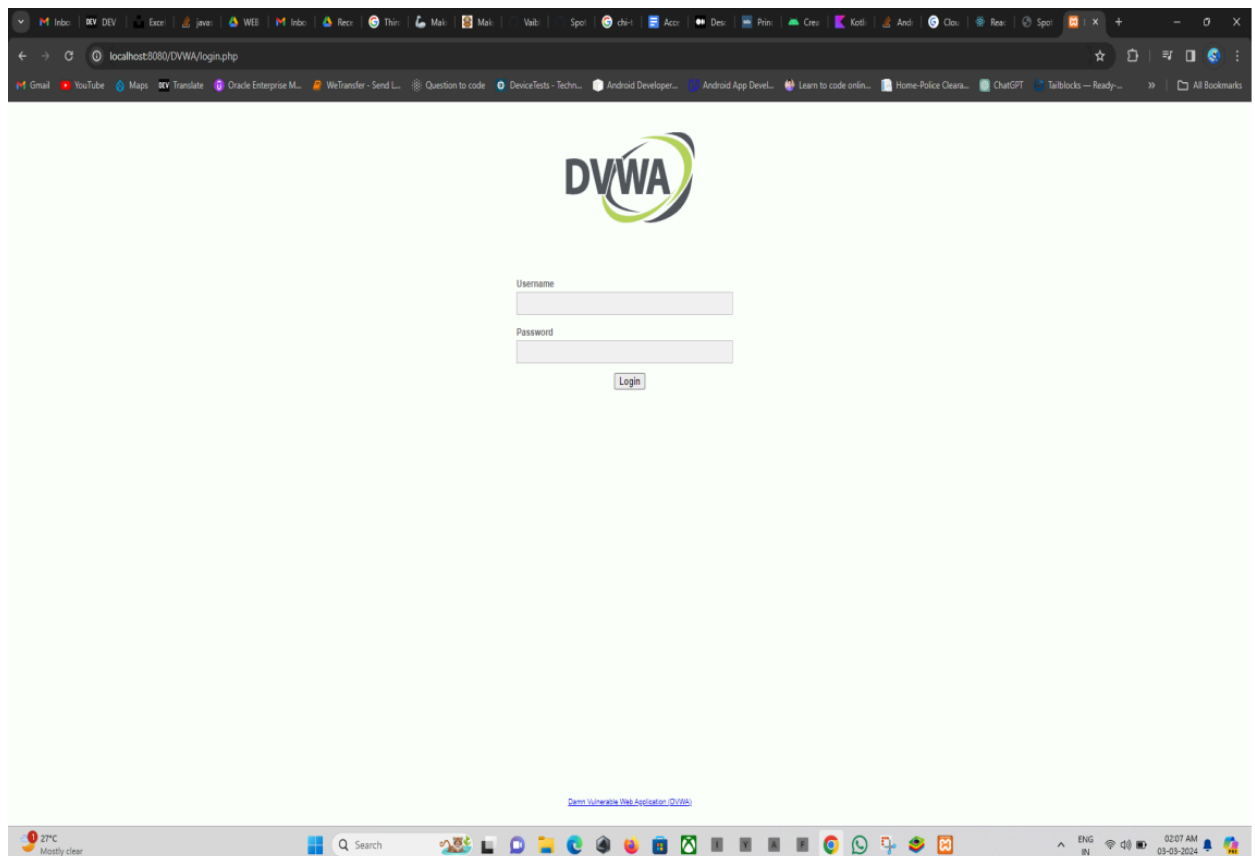
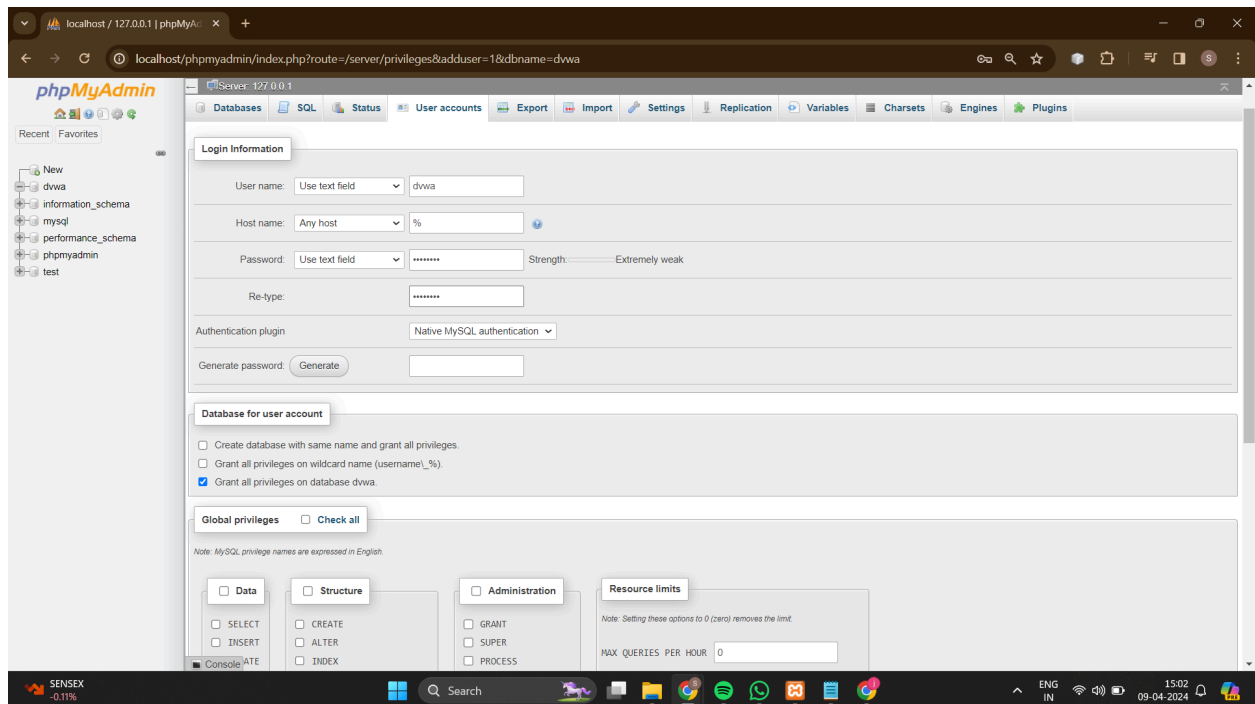
Sheth L.U.J. College Of Arts & Sir M.V. College of Science & Commerce
Department Of Science
Jayesh mali T084 Pract_8 Ethical hacking



Sheth L.U.J. College Of Arts & Sir M.V. College of Science & Commerce

Department Of Science

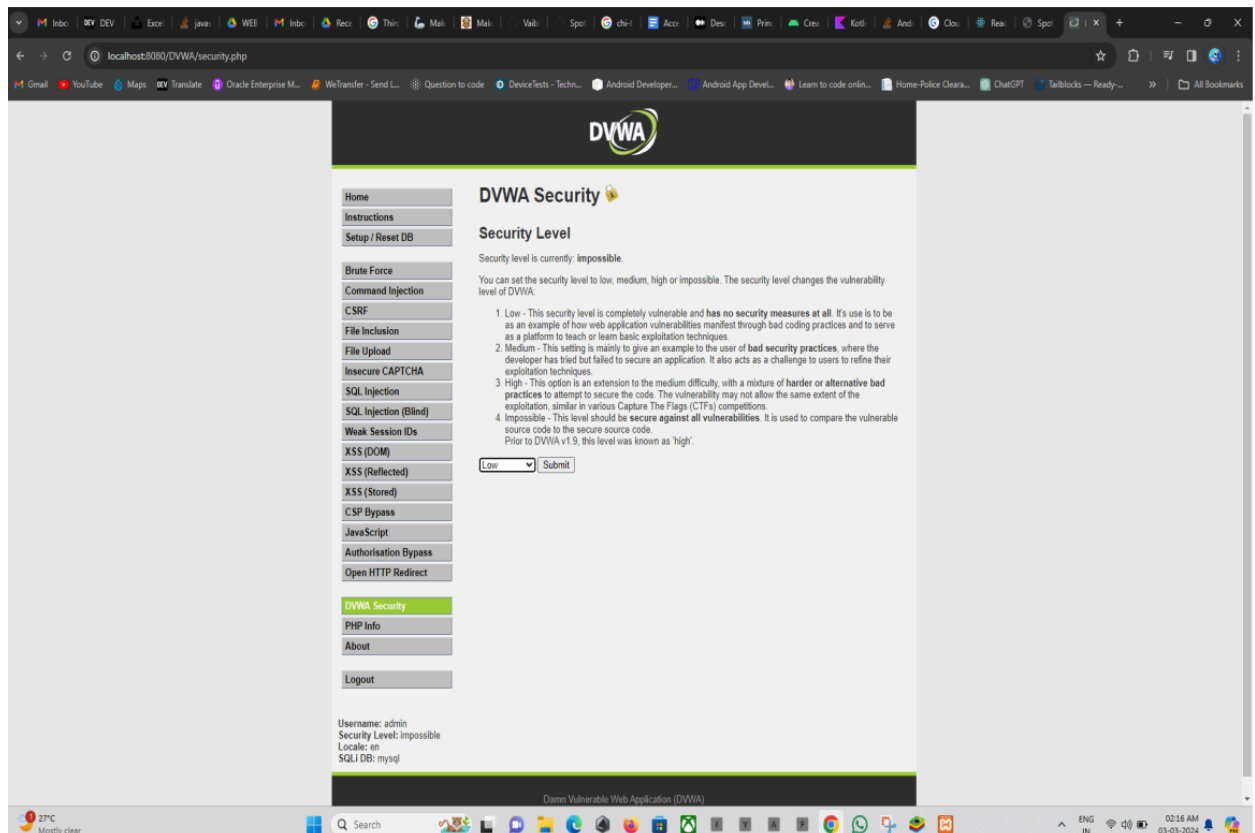
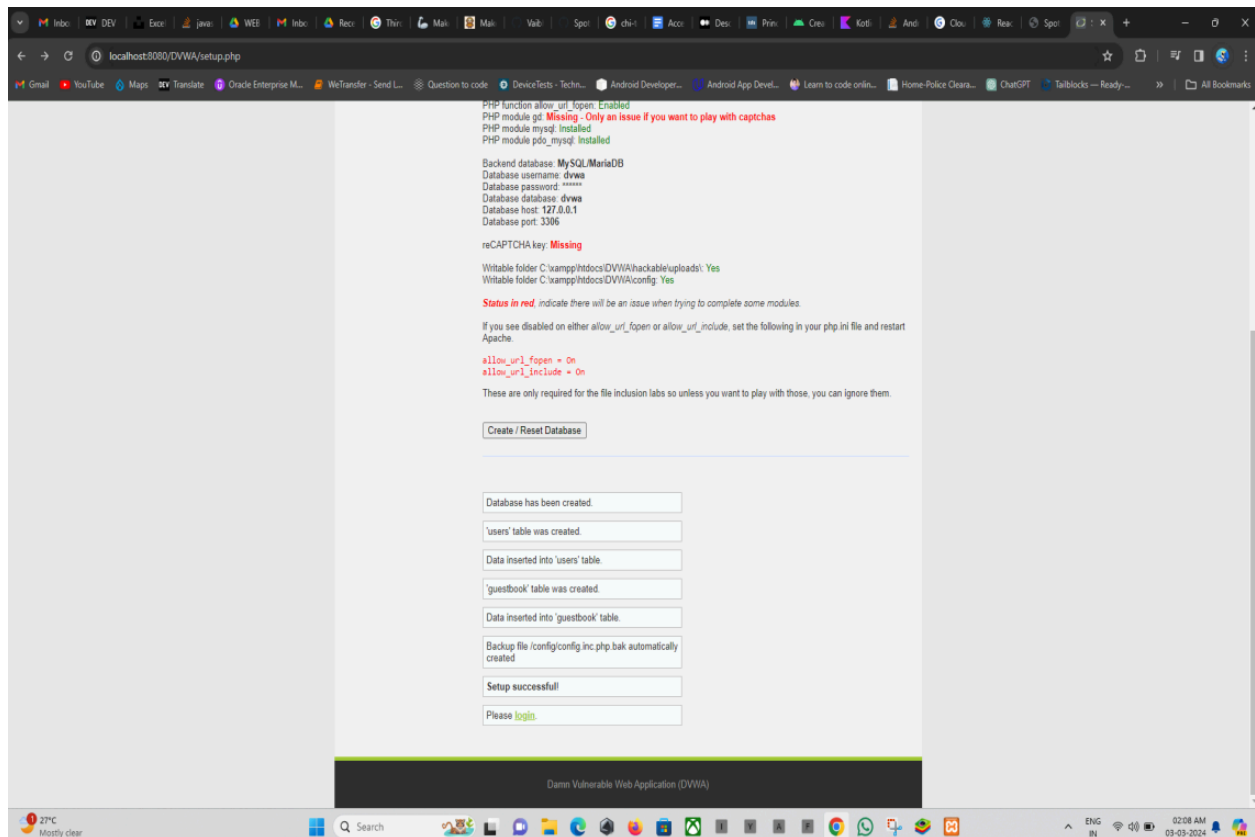
Jayesh mali T084 Pract_8 Ethical hacking



Sheth L.U.J. College Of Arts & Sir M.V. College of Science & Commerce

Department Of Science

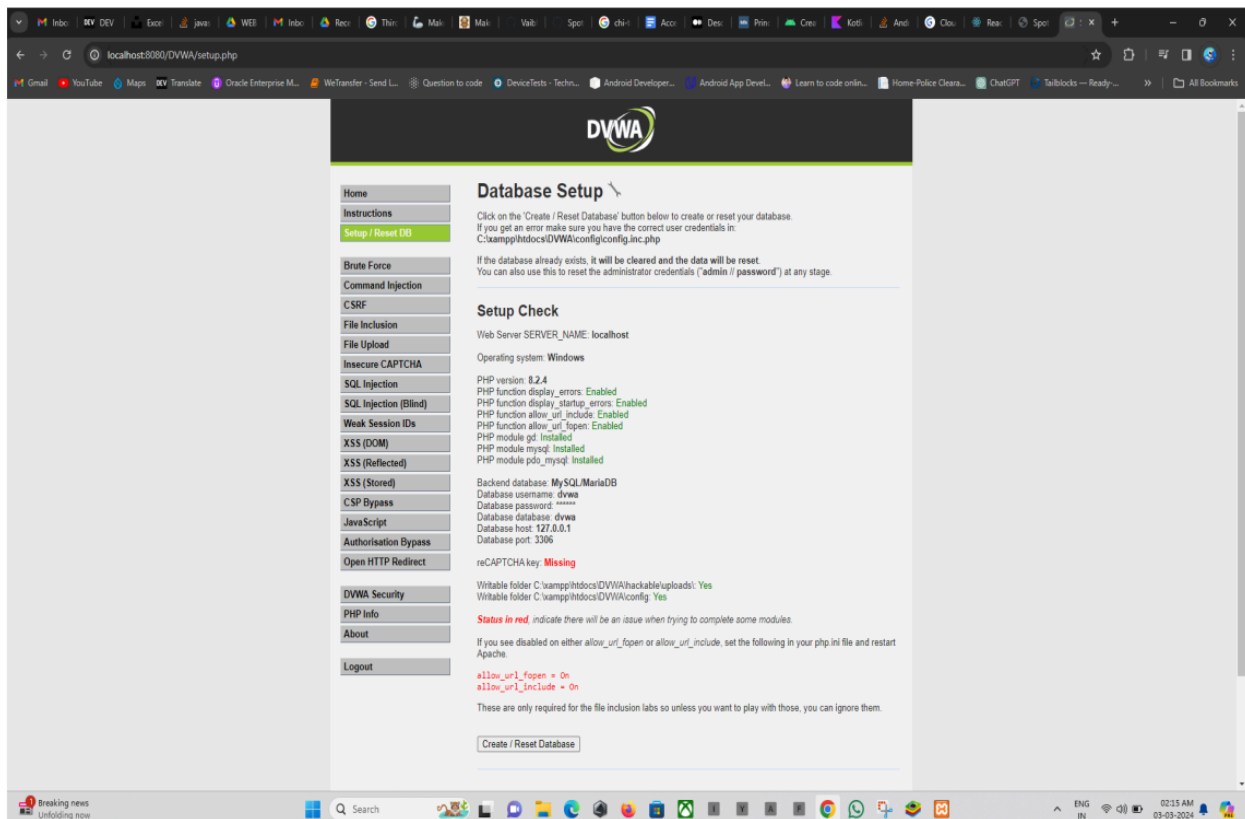
Jayesh mali T084 Pract_8 Ethical hacking



Sheth L.U.J. College Of Arts & Sir M.V. College of Science & Commerce

Department Of Science

Jayesh mali T084 Pract_8 Ethical hacking



The screenshot shows the DVWA (Damn Vulnerable Web Application) Setup page. The page has a dark header with the DVWA logo. On the left is a sidebar menu with links to Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, Authorisation Bypass, Open HTTP Redirect, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Database Setup" and contains instructions for creating or resetting the database. It mentions that if the database already exists, it will be cleared and the data will be reset. Below this is a "Setup Check" section that displays various system and application details: Web Server (SERVER_NAME: localhost), Operating system (Windows), PHP version (8.2.4), PHP function display_errors (Enabled), PHP function display_startup_errors (Enabled), PHP function allow_url_include (Enabled), PHP function allow_url_fopen (Enabled), PHP module gd (Installed), PHP module mysql (Installed), PHP module pdo_mysql (Installed), Backend database (MySQL/MariaDB), Database username (dwva), Database password (*****), Database database (dwva), Database host (127.0.0.1), Database port (3306), reCAPTCHA key (Missing), Writable folder C:\xampp\htdocs\DVWA\hackable\uploads\ (Yes), and Writable folder C:\xampp\htdocs\DVWA\config\ (Yes). A red status message indicates that if any status is in red, there will be an issue when trying to complete some modules. It also provides instructions on how to fix disabled allow_url_fopen or allow_url_include settings in the php.ini file. At the bottom of the main content area is a "Create / Reset Database" button.

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in:
C:\xampp\htdocs\DVWA\config\config.inc.php

If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ('admin' / 'password') at any stage

Setup Check

Web Server SERVER_NAME: localhost

Operating system: Windows

PHP version: 8.2.4
PHP function display_errors: Enabled
PHP function display_startup_errors: Enabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: MySQL/MariaDB
Database username: dwva
Database password: *****
Database database: dwva
Database host: 127.0.0.1
Database port: 3306

reCAPTCHA key: Missing

Writable folder C:\xampp\htdocs\DVWA\hackable\uploads\ Yes
Writable folder C:\xampp\htdocs\DVWA\config\ Yes

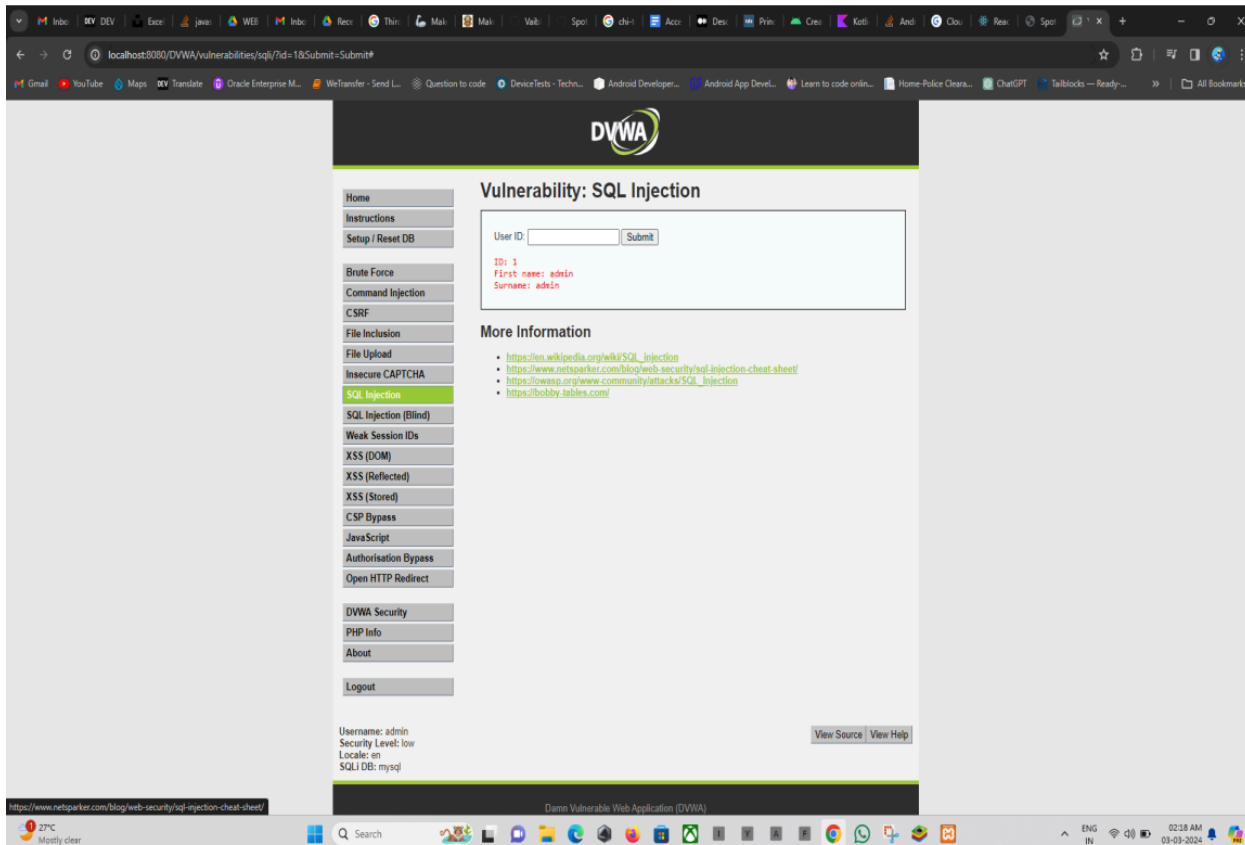
Status in red indicate there will be an issue when trying to complete some modules.

If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.

allow_url_fopen = On
allow_url_include = On

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database



The screenshot shows the DVWA SQL Injection page. The sidebar menu is the same as the previous page, but the "SQL Injection" link is highlighted. The main content area is titled "Vulnerability: SQL Injection" and contains a form with a "User ID" input field and a "Submit" button. Below the form, the results of the query are displayed: "ID: 1", "First name: admin", and "Surname: admin". Below the results is a "More Information" section with a list of links to external resources: https://en.wikipedia.org/wiki/SQL_injection, <https://www.netsecfor.com/blog/web-security/sql-injection-cheat-sheet/>, https://owasp.org/www-community/attacks/SQL_injection, and <https://bobby-tables.com/>. At the bottom of the page, there is a "View Source" button and a "View Help" button. The footer of the page displays the URL "https://www.netsecfor.com/blog/web-security/sql-injection-cheat-sheet/" and the text "Damn Vulnerable Web Application (DVWA)".

Vulnerability: SQL Injection

User ID: Submit

ID: 1
First name: admin
Surname: admin

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsecfor.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

View Source View Help

Username: admin
Security Level: low
Locale: en
SQL DB: mysql

https://www.netsecfor.com/blog/web-security/sql-injection-cheat-sheet/ Damn Vulnerable Web Application (DVWA)