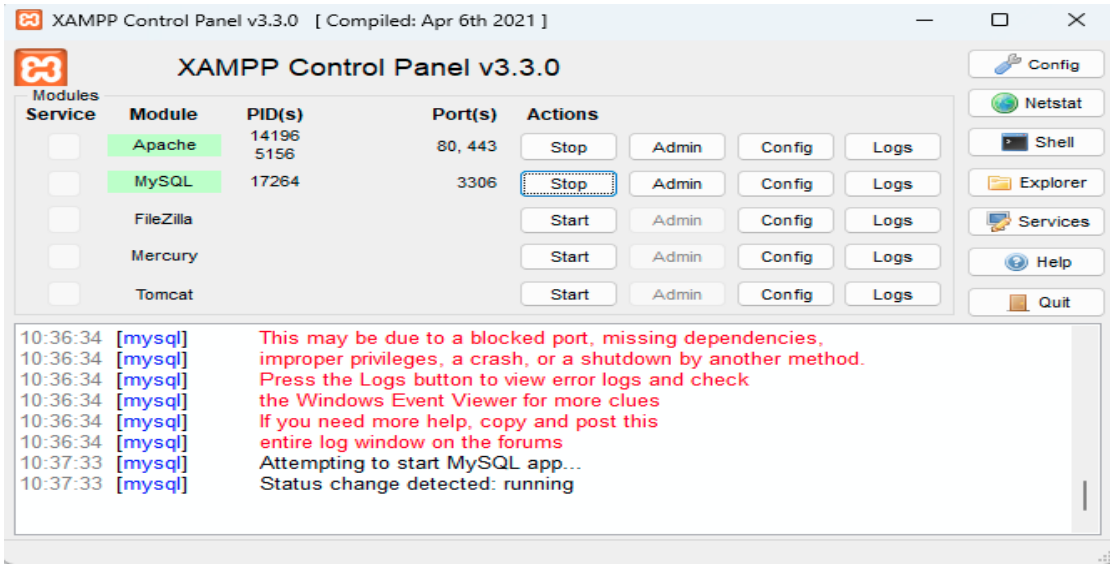
Perform SQL injection attack.

Introduction: This document explores the process of simulating SQL injection attacks using the Damn Vulnerable Web Application (DVWA). The objective is to understand how SQL injections can exploit weaknesses in a web application's database handling.

STEPS & OUTPUT :

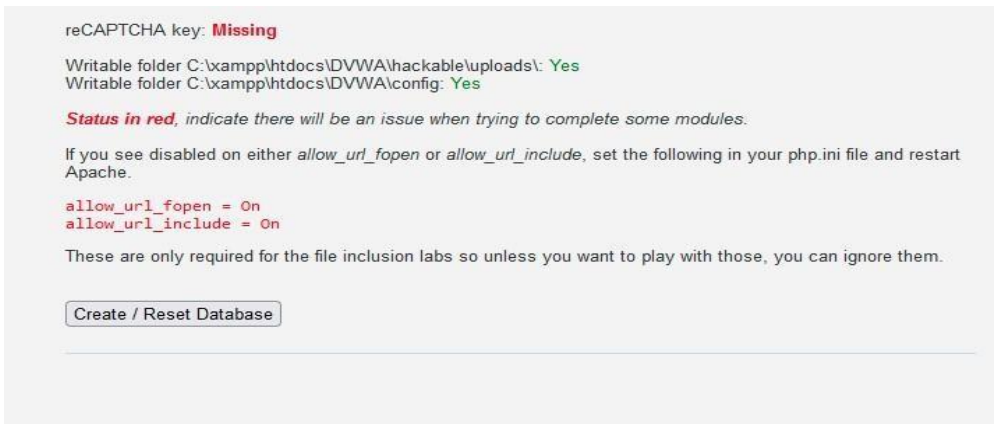
1] Download XAMPP, install it without changes, and run the MySQL and Apache Server.



2] Download Damn Vulnerable Web Application(DVWA) in the ZIP form, extract it, rename it to DVWA and move the folder to C/xampp/htdocs/.

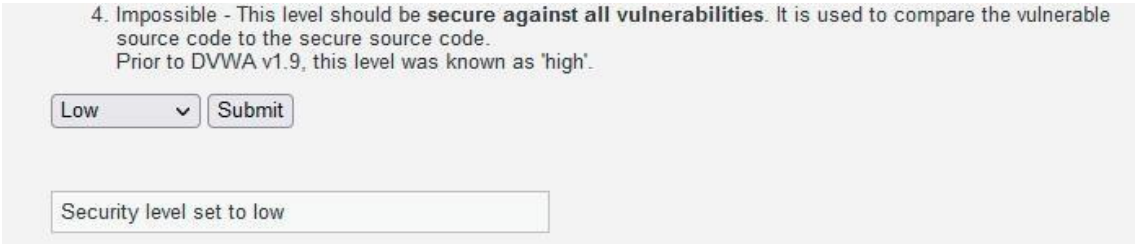
3] Navigate to the config file in the DVWA folder and rename it to 'config.inc.php'.Then open the config file with notepad and change the username to 'root' and password to ''.

4] Open a browser and type the URL 'localhost/DVWA/setup.php', scroll down and click on 'create/reset DB' to set your DVWA up.

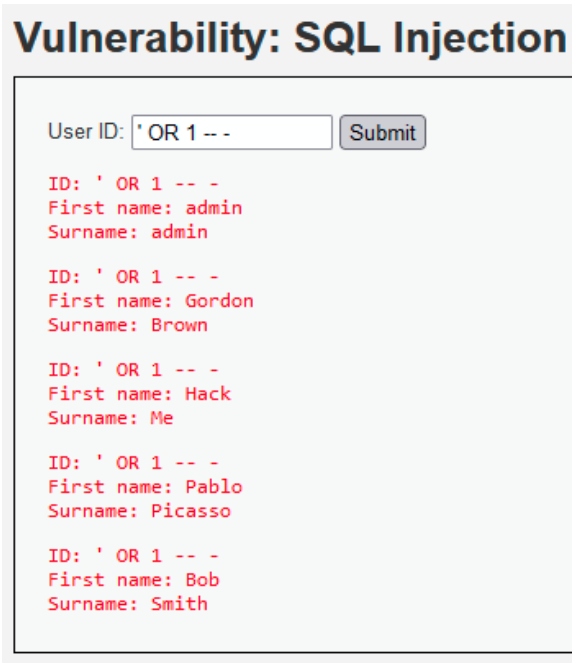


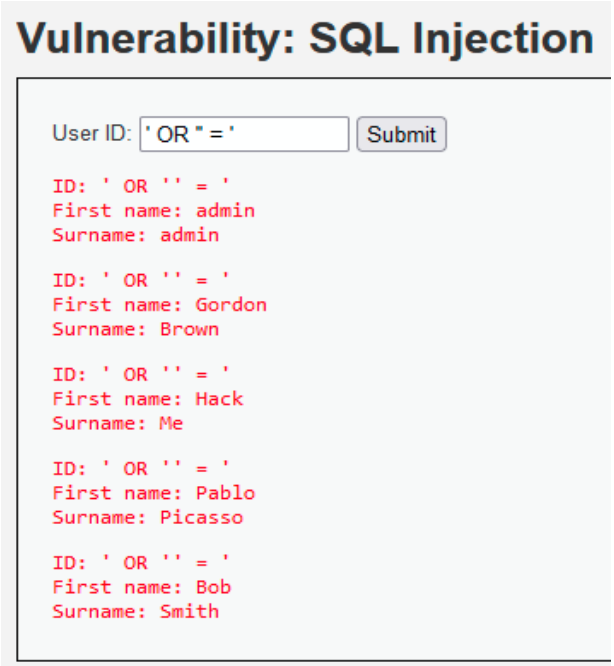
5] Now go to ‘localhost/DVWA/login.php’, the username is ‘admin’ and password is ‘password’.

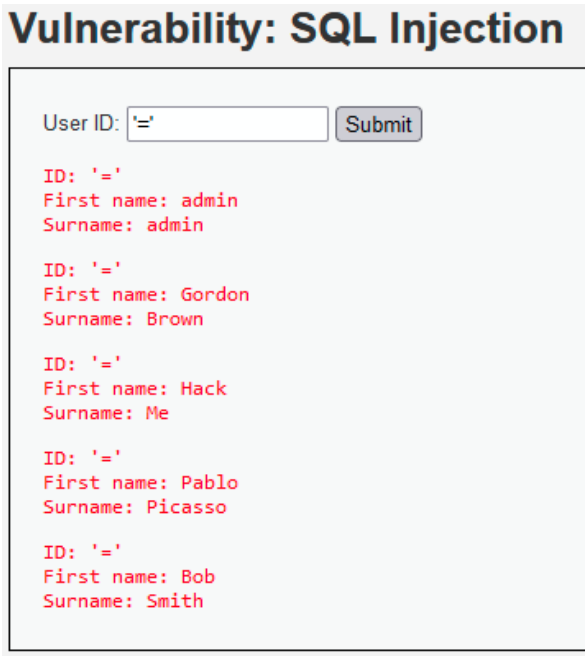
6] Go to ‘DVWA security’ and change the security level from impossible to low.

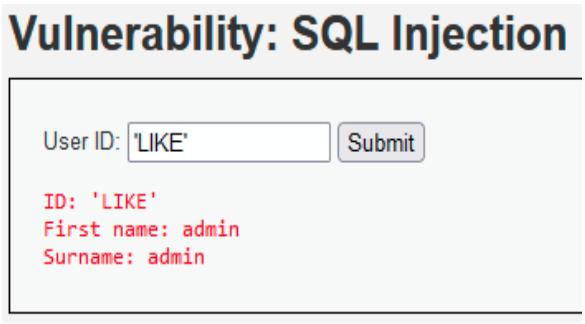


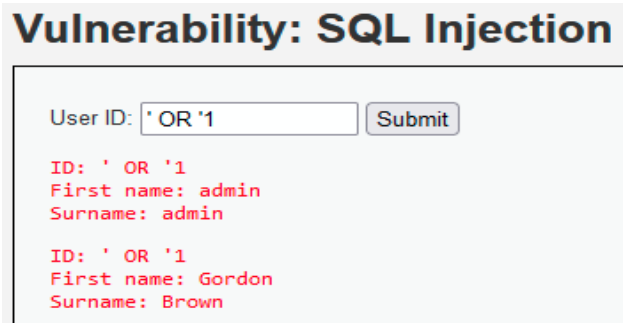
7] Perform 5 SQL Injection queries











Conclusion: The SQL injection attack simulation provides insight into how unauthorized database access can be achieved through injection vulnerabilities, emphasizing the need for secure coding practices to prevent such attacks.