Report Title: SQL Injection Testing using DVWA (Damn Vulnerable Web Application)

1. Introduction This report documents the step-by-step process of identifying and exploiting SQL Injection vulnerabilities using DVWA. DVWA is a vulnerable PHP/MySQL web application created for security professionals and students to test their skills in a legal environment.

2. Environment Setup

- **Platform**: Windows 11
- **Tools Used**: XAMPP, DVWA, Web Browser (Chrome)
- **DVWA Security Level**: Set to "Low"
- **URL Accessed**: `http://localhost/dvwa/vulnerabilities/sqli/`

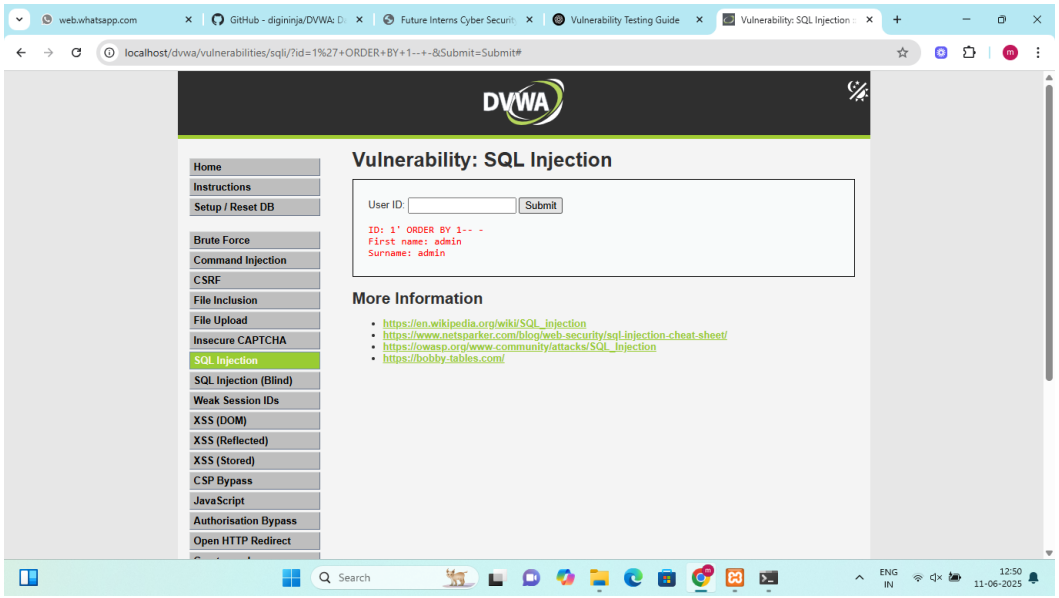
3. Objective The goal is to perform basic SQL Injection attacks to:

- Bypass authentication or extract information.
- Enumerate database structure (table names, column names).
- Extract sensitive data such as usernames.

4. Step-by-Step Procedure

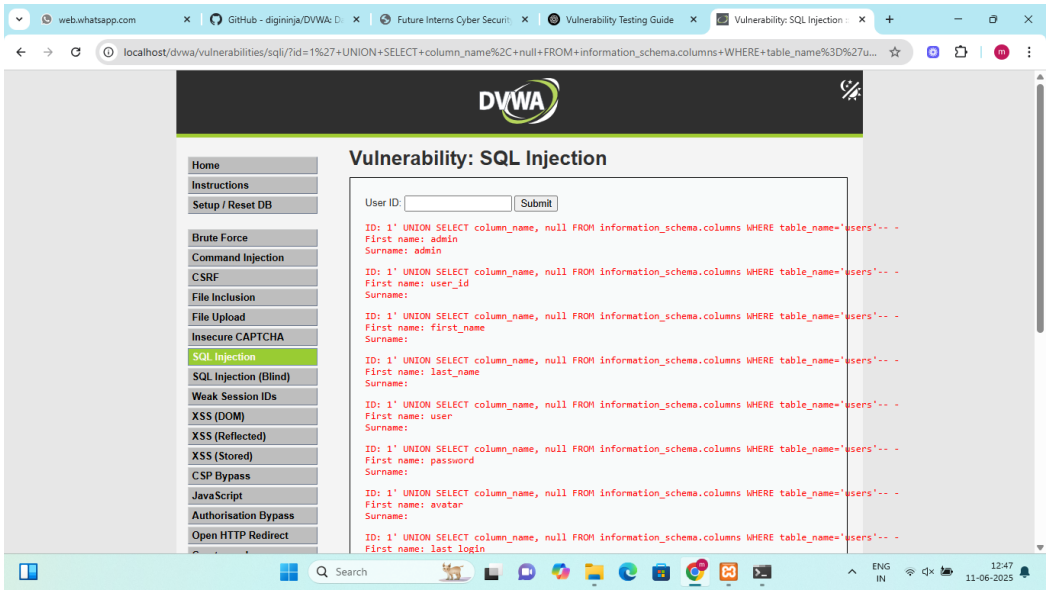
Step 1: Test Basic SQL Injection

- Payload used: `1' OR '1'='1`
- Action: Entered in the User ID field and submitted.
- Result: Retrieved a list of users from the database, confirming vulnerability.



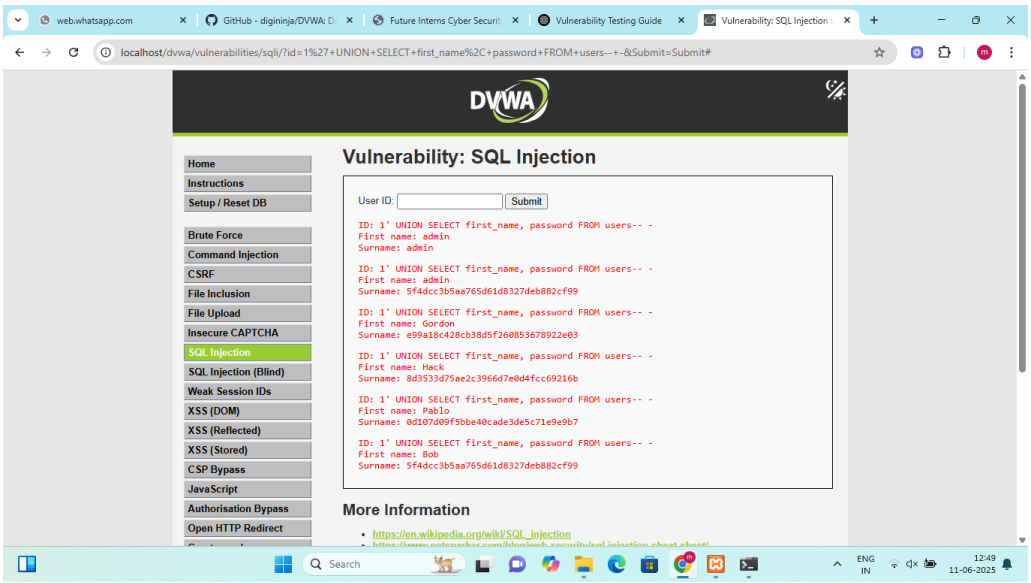
Step 2: Extract Data Using UNION SELECT

- Goal: Determine the number of columns for UNION SELECT.
- Payload tried: `1' UNION SELECT NULL, NULL --` , then increased number of NULLs until the correct number of columns matched.
- Once determined, used:
  `1' UNION SELECT first_name, surname FROM users –`
- Result: Fetched first name and surname data from the users table.



Step 3: Finding Column Names

- Explored SQL injection queries to extract schema information.
- Used enumeration techniques on MySQL's `information_schema` to find table and column names (if applicable).



5. Observations

- The application does not sanitize input.
- SQL injection is successful, allowing attackers to retrieve arbitrary database data.
- Demonstrates a common web vulnerability that can be exploited if not properly protected.

6. Prevention and Remediation

- Use of Prepared Statements (Parameterized Queries)
- Input Validation and Sanitization
- Least Privilege Access on Databases
- Regular Code Reviews and Vulnerability Scanning

7. Conclusion The DVWA environment successfully demonstrated SQL Injection vulnerabilities and how attackers can exploit them. This practical exercise helps understand the impact of insecure coding practices and the importance of input validation in web applications.