Internship Project Report

Task 3: Name: Sibiraj B

Company: Oasis Infobyte

Duration: [15 july 2025 – 15 augest 2025]

Submitted as part of the internship program

1. Objective

The objective of this project is to demonstrate an SQL Injection vulnerability on a web application using DVWA (Damn Vulnerable Web Application) with the security level set to low.

2. Tools & Technologies

- DVWA (Damn Vulnerable Web Application)

- Operating System: Kali Linux / Ubuntu / Windows with XAMPP

- Web Browser: Firefox / Chrome

- Database: MySQL / MariaDB

3. Implementation Steps

Step 1: Install and Configure DVWA

Command (Example on Kali Linux):

```
sudo apt update && sudo apt install dvwa -y
```

Or configure DVWA manually using XAMPP/WAMP and enable MySQL/PHP services.

Step 2: Set DVWA Security Level to Low

Navigate to DVWA Security tab and select 'Low'.

Step 3: Perform SQL Injection on the Login Page

Example payload for authentication bypass:

```
' OR '1'='1 --
```

This forces the SQL query to always return true, bypassing authentication.

Step 4: Capture Output and Explain Vulnerability

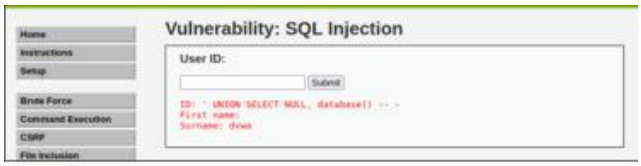
Observe that the application logs you in without valid credentials, indicating that the input was directly concatenated into the SQL query without sanitization.

4. GitHub Deliverables

1. sql_injection_exploit.sh – Script containing SQL injection steps (if applicable).

2. Screenshots of the SQL injection process and successful exploitation.

3. README.md – Documentation explaining the vulnerability, payload, and mitigation.



(a) DVWA SQLi Vulnerability

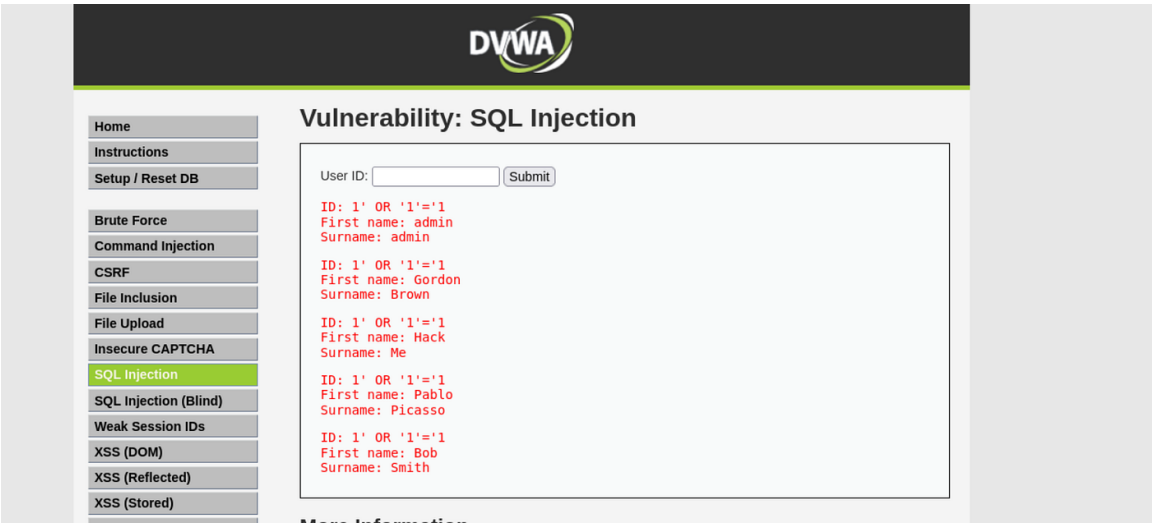
(b) Vulnado Vulnerable Endpoint

(c) Authentication Bypassed

5. Demo Video Idea

Create a video demonstrating:

1. Setting DVWA security level to low
2. Using SQL injection payload on the login page
3. Gaining unauthorized access
4. Explaining why the attack works



6. Conclusion

This project successfully demonstrates the exploitation of an SQL Injection vulnerability in a web application running DVWA with low security settings. It highlights the importance of input validation, parameterized queries, and secure coding practices.