**DVWA Internship Project Documentation**

**Student Name:** Aman Ahmed Mohammad  
**Internship Project:** Web Application Security Testing using DVWA  
**Date:** 30-09-2025

**1. DVWA Setup**

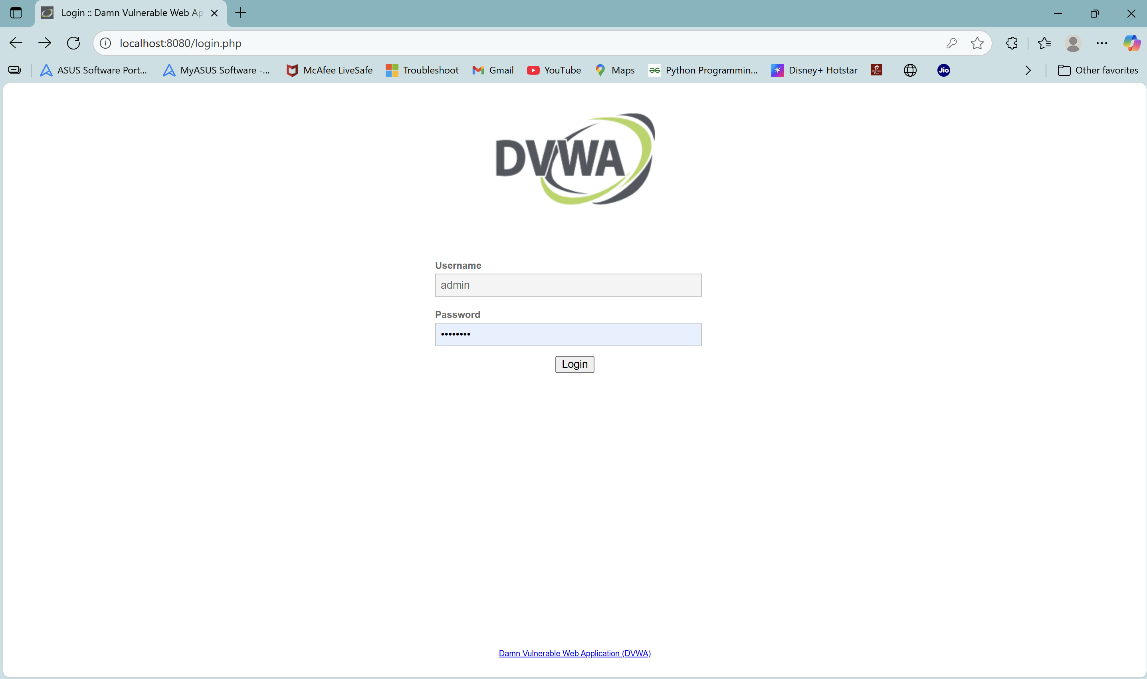
**Description:**  
I installed DVWA (Damn Vulnerable Web Application) using Docker on my local machine. This environment allows testing of common web vulnerabilities in a controlled setting.

**Docker Commands Used:**

docker pull vulnerables/web-dvwa

docker run --rm -it -p 8080:80 vulnerables/web-dvwa

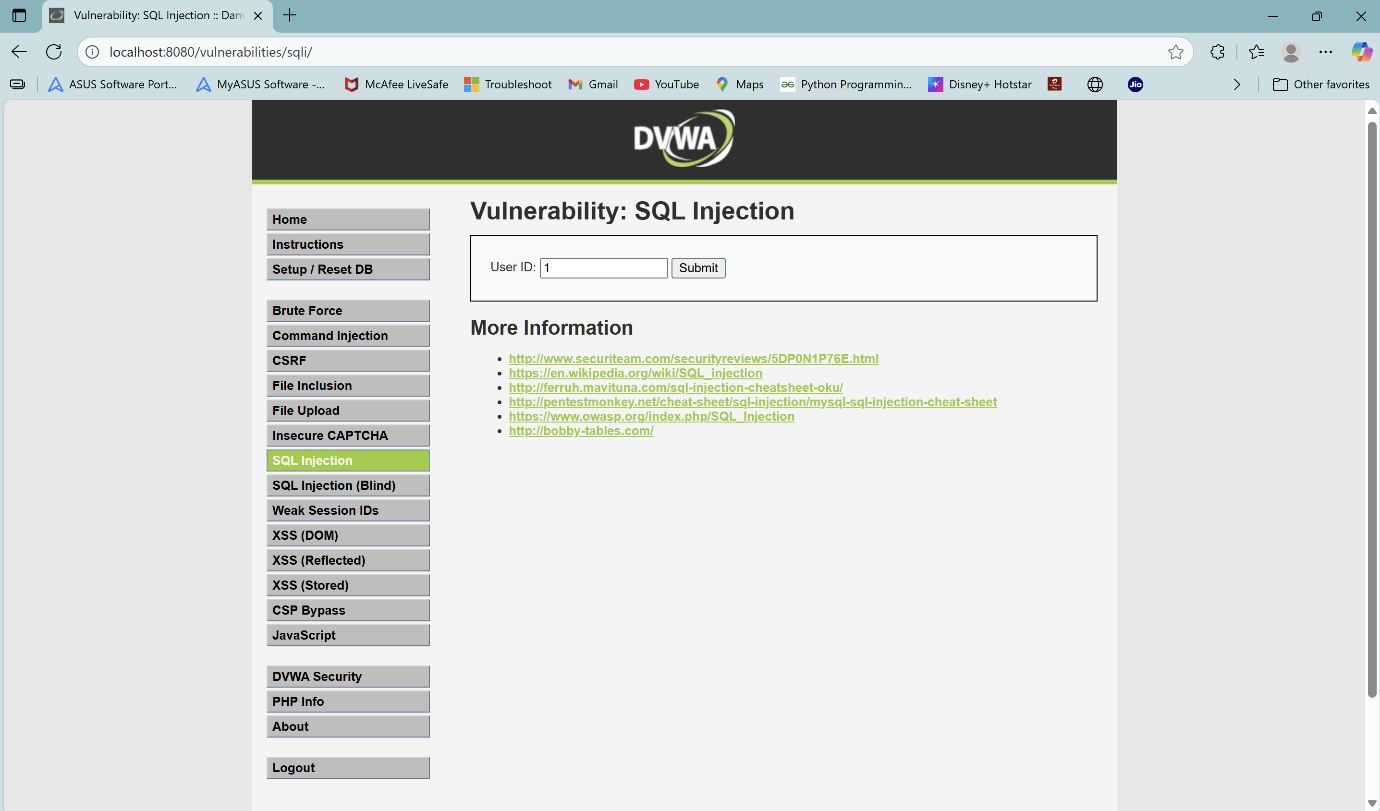
**2. DVWA Login Page**

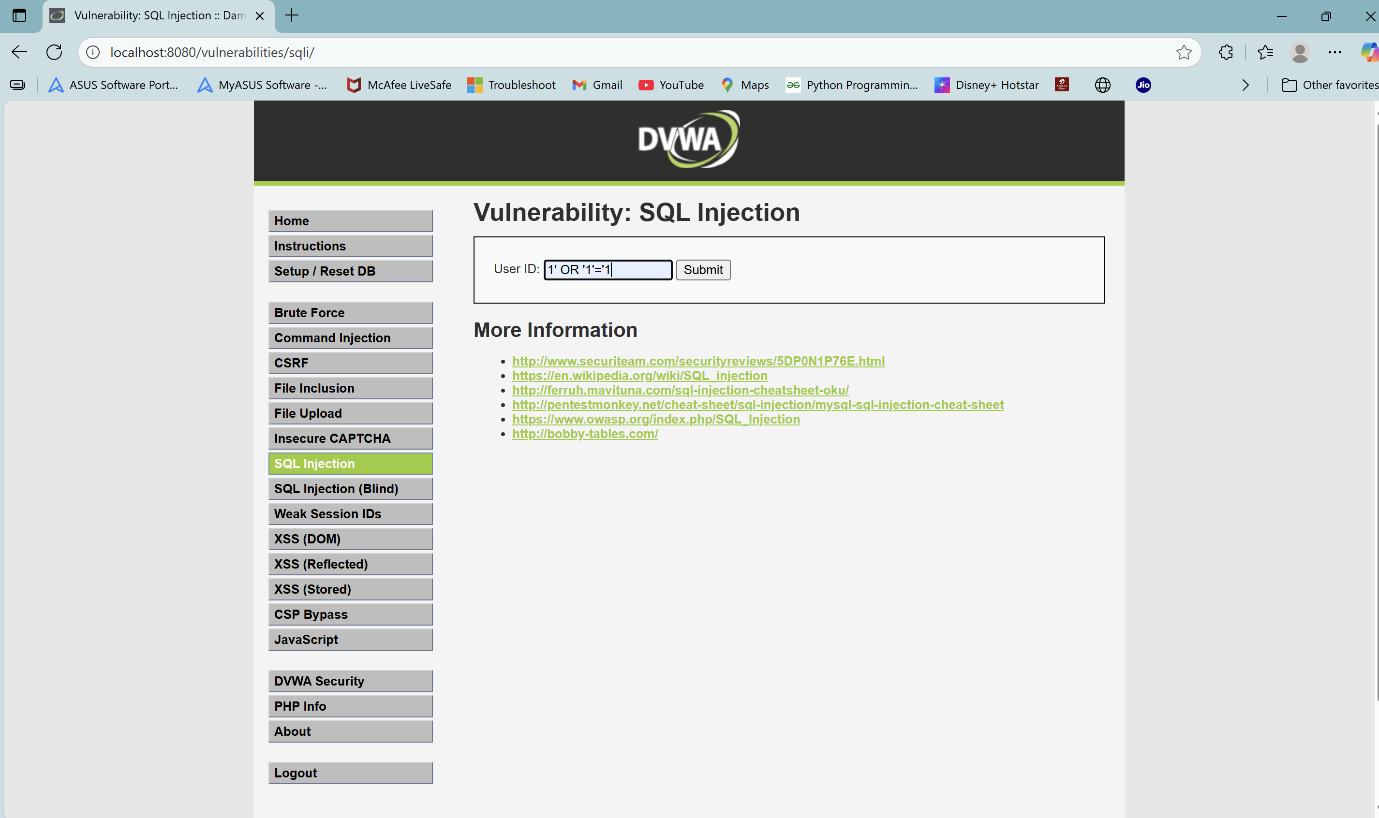


**Explanation:**  
The login page allows access to DVWA. Default credentials used:

* Username: admin
* Password: password

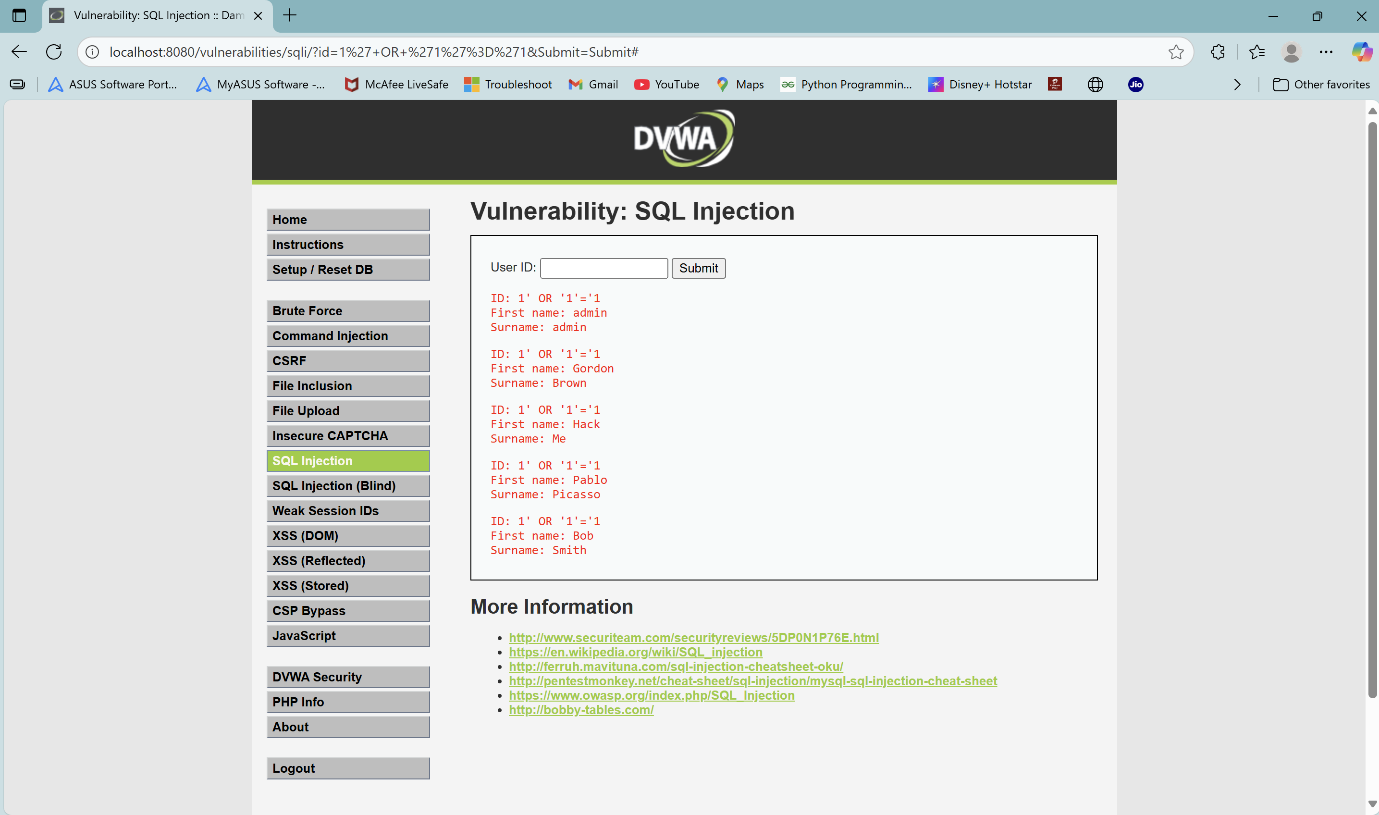
**3. SQL Injection Page (Before Attack)**

****

****

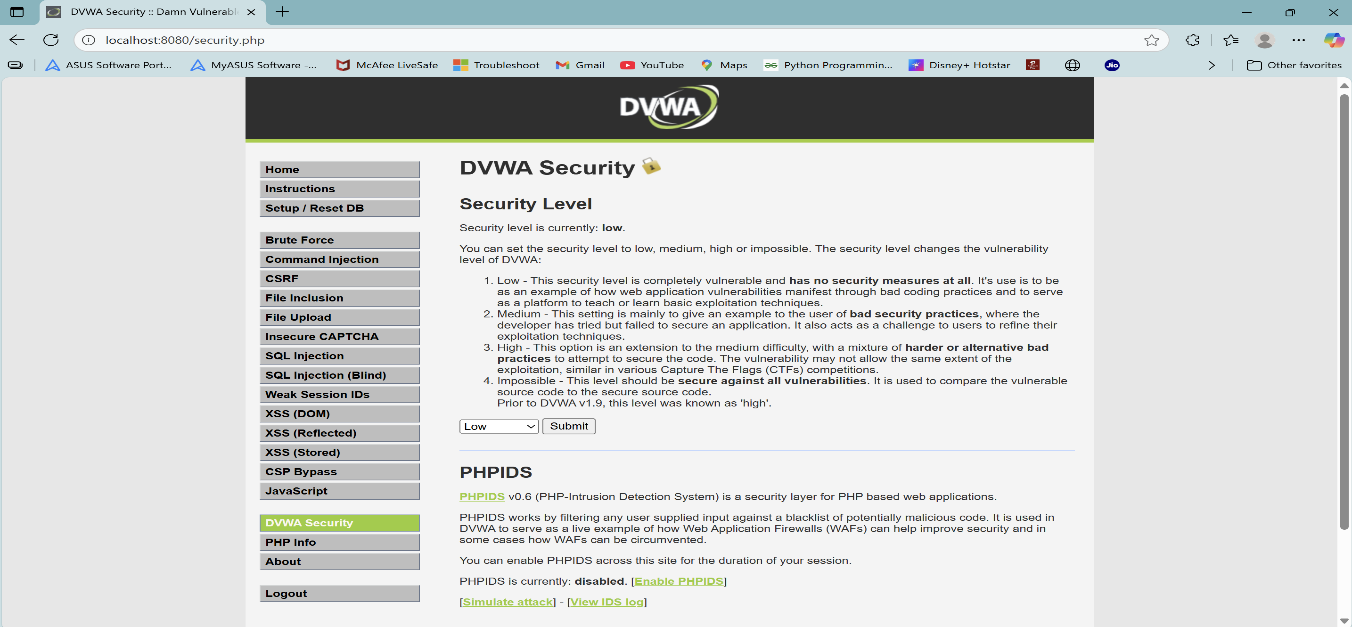
**Explanation:**  
This page contains a vulnerable input field for SQL Injection testing. The security level was set to Low to allow basic vulnerability testing.

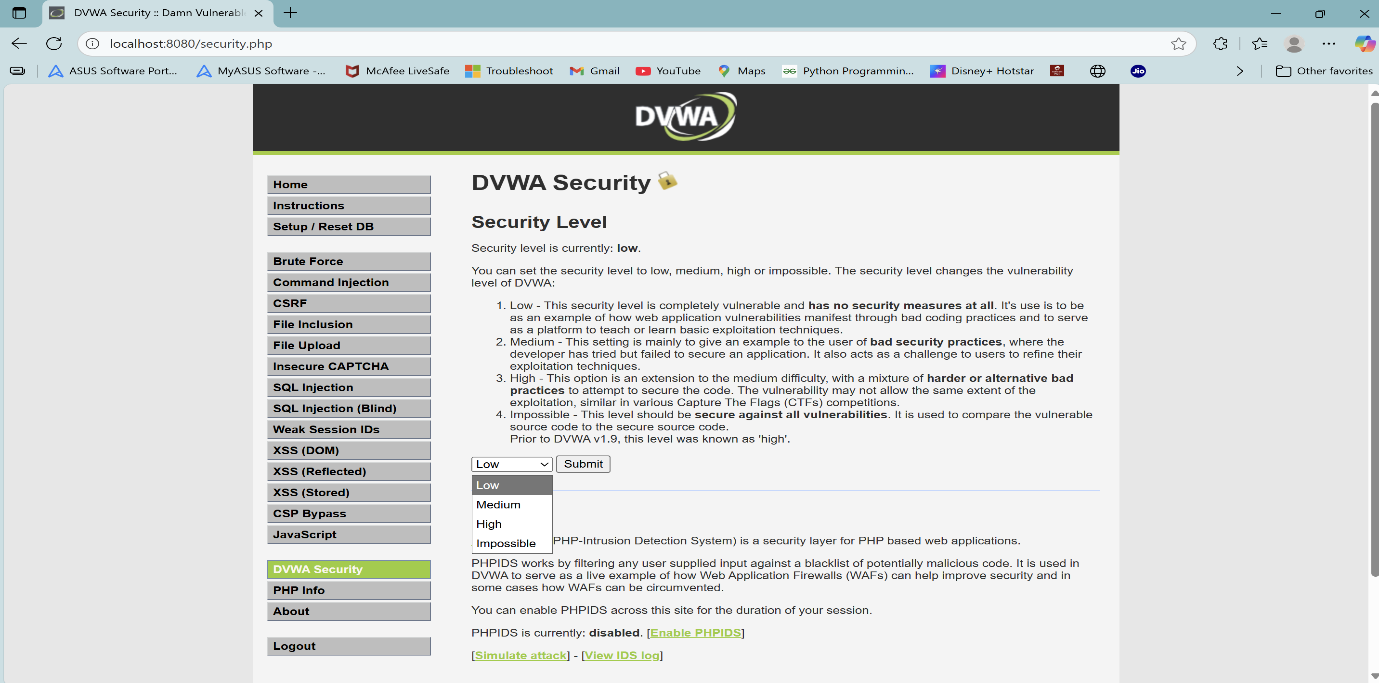
**4. SQL Injection Page (After Attack)**

****

**Explanation:**  
A basic SQL Injection attack was performed, which successfully retrieved all user records from the database. This demonstrates the risks of unprotected input fields in web applications.

**5. DVWA Security Page**

****

****

**Explanation:**  
The security level was configured to Low to facilitate testing and demonstration of vulnerabilities. Higher levels restrict certain attacks.

**6. Conclusion**

DVWA was successfully set up and tested using Docker. Through this project:

* I performed a basic SQL Injection attack.
* I documented the results with screenshots.
* I demonstrated the importance of securing web applications against common vulnerabilities.