SQL Injection Vulnerability Assessment

(Learning Project)

Name: Arko Das

Field: Cyber Security

Platform: Port Swigger Web Security Academy

Purpose: Educational & Project

1.Introduction

This project focuses on learning and understanding SQL Injection vulnerabilities through hands-on practice in a controlled lab environment. The objective is to identify, analyze, and document SQL Injection flaws using ethical web application testing techniques.

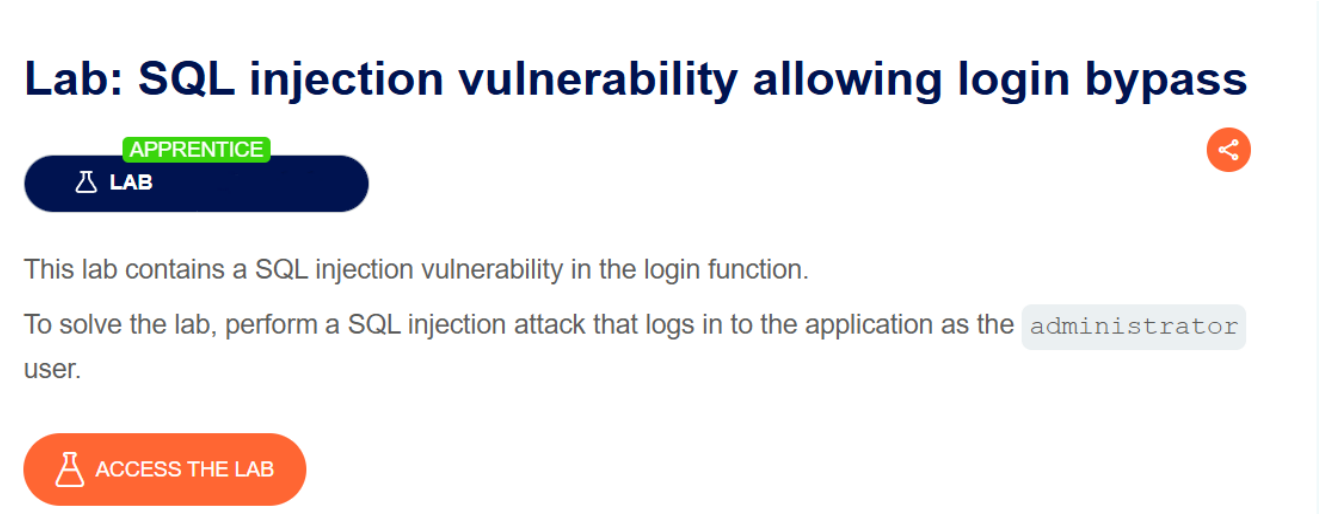
2. Lab Environment Setup

The testing environment was set up using Kali Linux with pre-installed security tools. The target applications were provided by Port Swigger Web Security Academy, which offers intentionally vulnerable labs for educational purposes.

Tools Used:

- Kali Linux
- Port Swigger Web Security Academy
- Burp Suite
- Web Browser

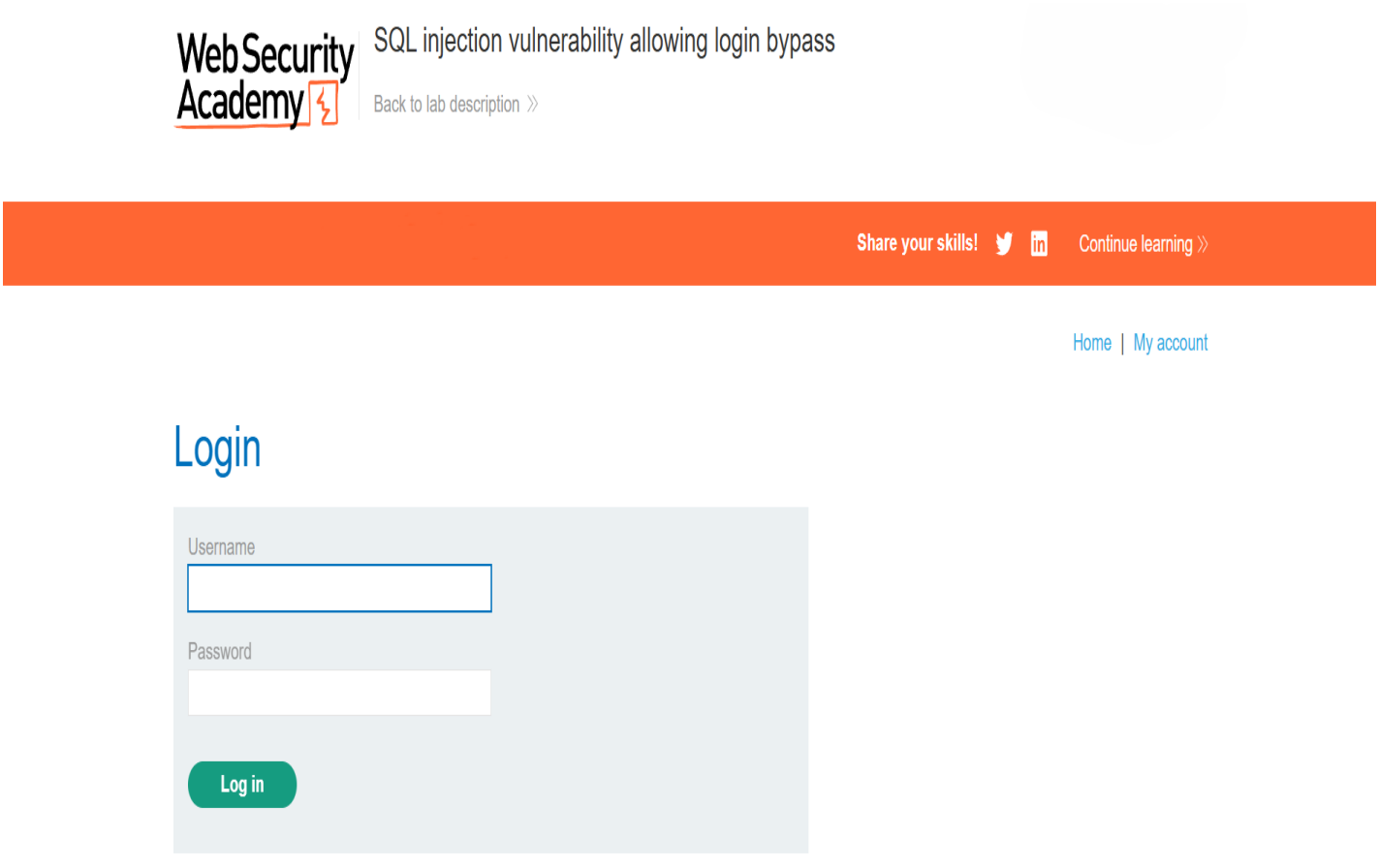
Figure 1: Overview of the vulnerable lab environment



3. Vulnerable Code Analysis

The vulnerable functionality relied on dynamically constructed SQL queries without proper input validation. User-supplied input was directly embedded into SQL statements, making the application susceptible to SQL Injection.

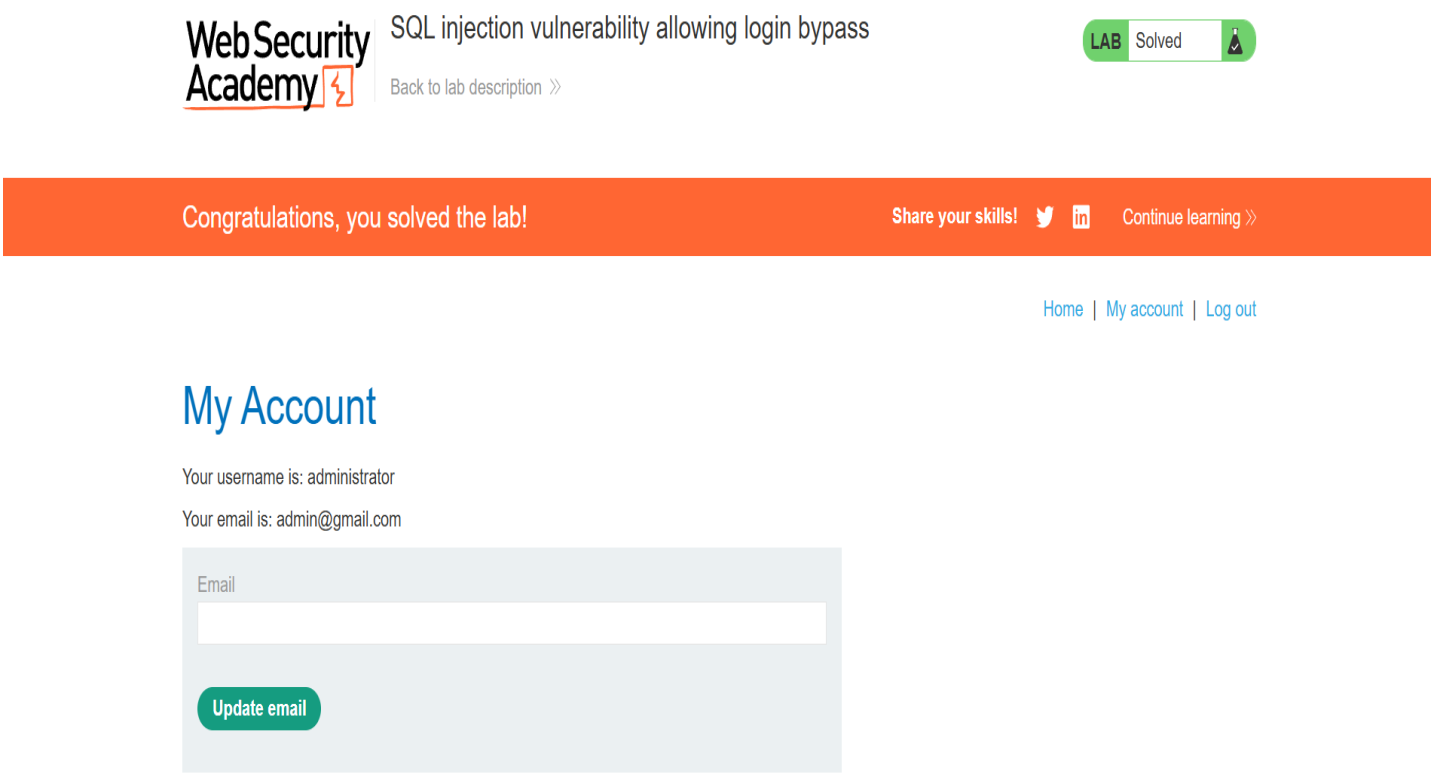
Figure 2: Identified input parameter susceptible to SQL Injection



4.Proof of Concept (PoC)

During testing, an authentication bypass vulnerability was identified. By manipulating input parameters, it was possible to alter the logic of the SQL query and gain unauthorized access within the lab environment.

Figure 3: Intercepted HTTP request during SQL Injection testing



5. Remediation

To mitigate SQL Injection vulnerabilities, the application should implement parameterized queries (prepared statements), strict input validation, and proper error handling. Using ORM frameworks can also reduce the risk of injection flaws.

6. Conclusion

This project enhanced practical knowledge of SQL Injection vulnerabilities and strengthened manual web application testing skills. Multiple SQL Injection labs from the Port Swigger Web Security Academy were completed, including authentication bypass, UNION-based, and blind SQL injection scenarios. Through hands-on practice, this project improved the ability to identify, analyze, and remediate critical web application security issues in a controlled lab environment.

7. Disclaimer

This project and all associated laboratory exercises were conducted strictly for educational and learning purposes within a private, controlled, and intentionally vulnerable lab environment provided by the Port Swigger Web Security Academy. All testing activities were performed in accordance with ethical cybersecurity practices and did not involve any real-world systems or unauthorized targets.

Unauthorized testing, exploitation, or access to external systems, networks, or applications without explicit permission is illegal and unethical. The knowledge gained from this project is intended solely for defensive security learning, skill development and demonstration purposes.