SQL Injection Vulnerability Report

Lab: SQL Injection – Login Bypass

Platform: PortSwigger Web Security Academy

Tester: Praisegod Aliyu

Date: 06 Jan 2026

Objective

The objective of this lab was to bypass authentication by exploiting

a SQL Injection vulnerability in the login functionality.

Vulnerability Type

SQL Injection – Authentication Bypass

OWASP Category: A03 – Injection

Target Description

The target application contains a login form that verifies user credentials

using dynamically constructed SQL queries.

Vulnerability Discovery

Testing revealed that the username parameter was vulnerable to SQL Injection.

Injecting a single quote disrupted the query logic, indicating improper input handling.

Exploitation Steps

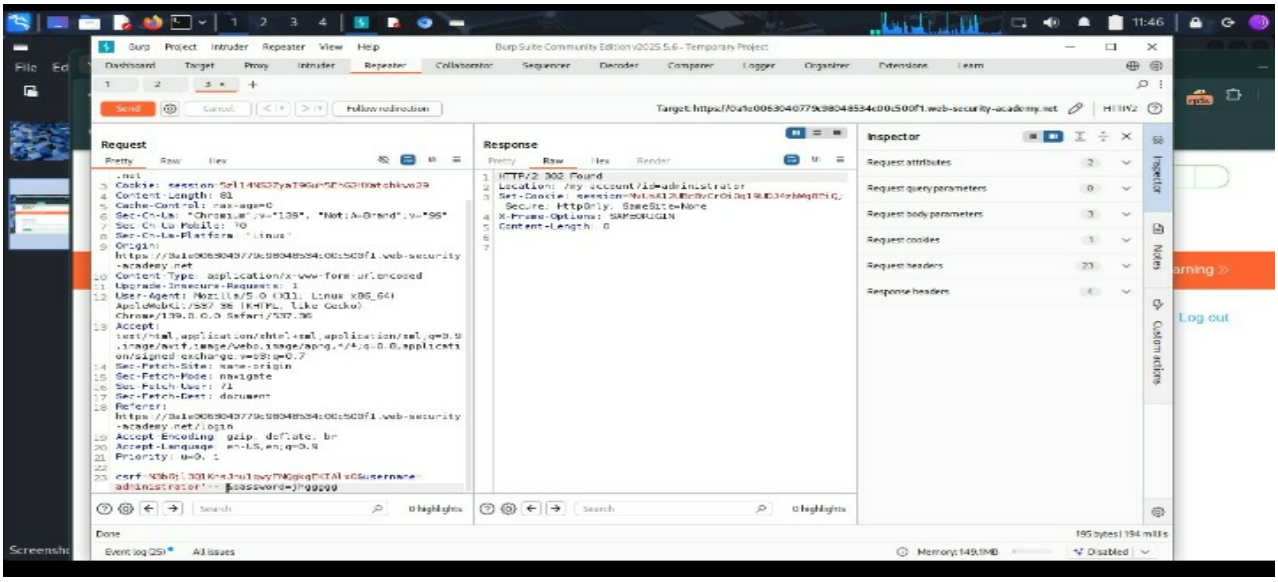
1. Intercepted the login request using Burp Suite.

2. Identified the vulnerable username parameter.

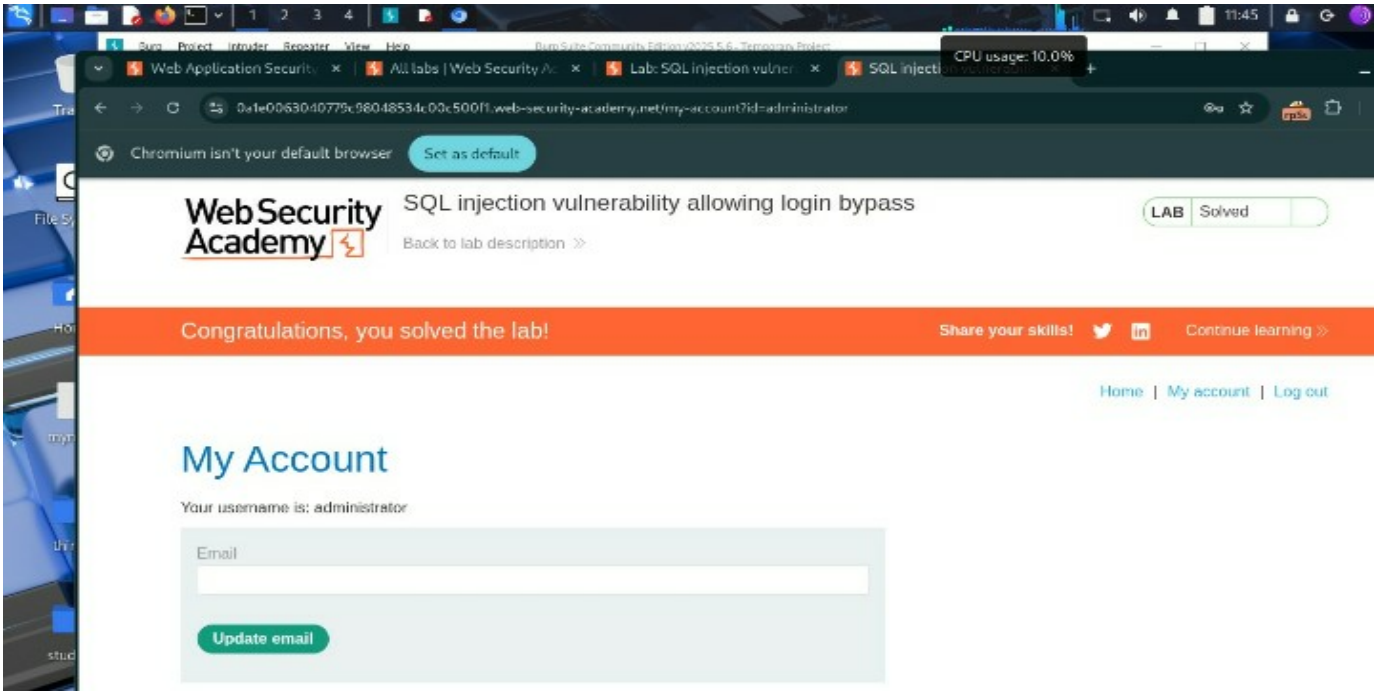
3. Injected the payload:

administrator'--

4. The SQL query was terminated, allowing authentication as the administrator user.



Capturing the request and inserting the payload



After Injection (logged in as administrator)

Impact

An attacker could gain unauthorized access to administrative accounts, leading to full compromise of the application.

Remediation

- Use parameterized queries
- Implement strong input validation
- Use secure password hashing