

SQL Injection Vulnerability Report

Lab: SQL Injection – UNION-based Data Extraction

Platform: PortSwigger Web Security Academy

Tester: Praisegod Aliyu

Date: [08 Jan 2026]

Objective

The objective of this lab was to exploit a UNION-based SQL Injection vulnerability to retrieve sensitive data from another database table.

Vulnerability Type

SQL Injection – UNION-based

OWASP Top 10 Category: A03 – Injection

Target Description

The target application displays product listings based on user-selected categories.

User input is included directly in a backend SQL query without proper sanitization.

Vulnerability Discovery

Initial testing of the category parameter using a single quote ('') caused a SQL error,

indicating that the application was vulnerable to SQL Injection.

Further testing confirmed that UNION-based injection was possible.

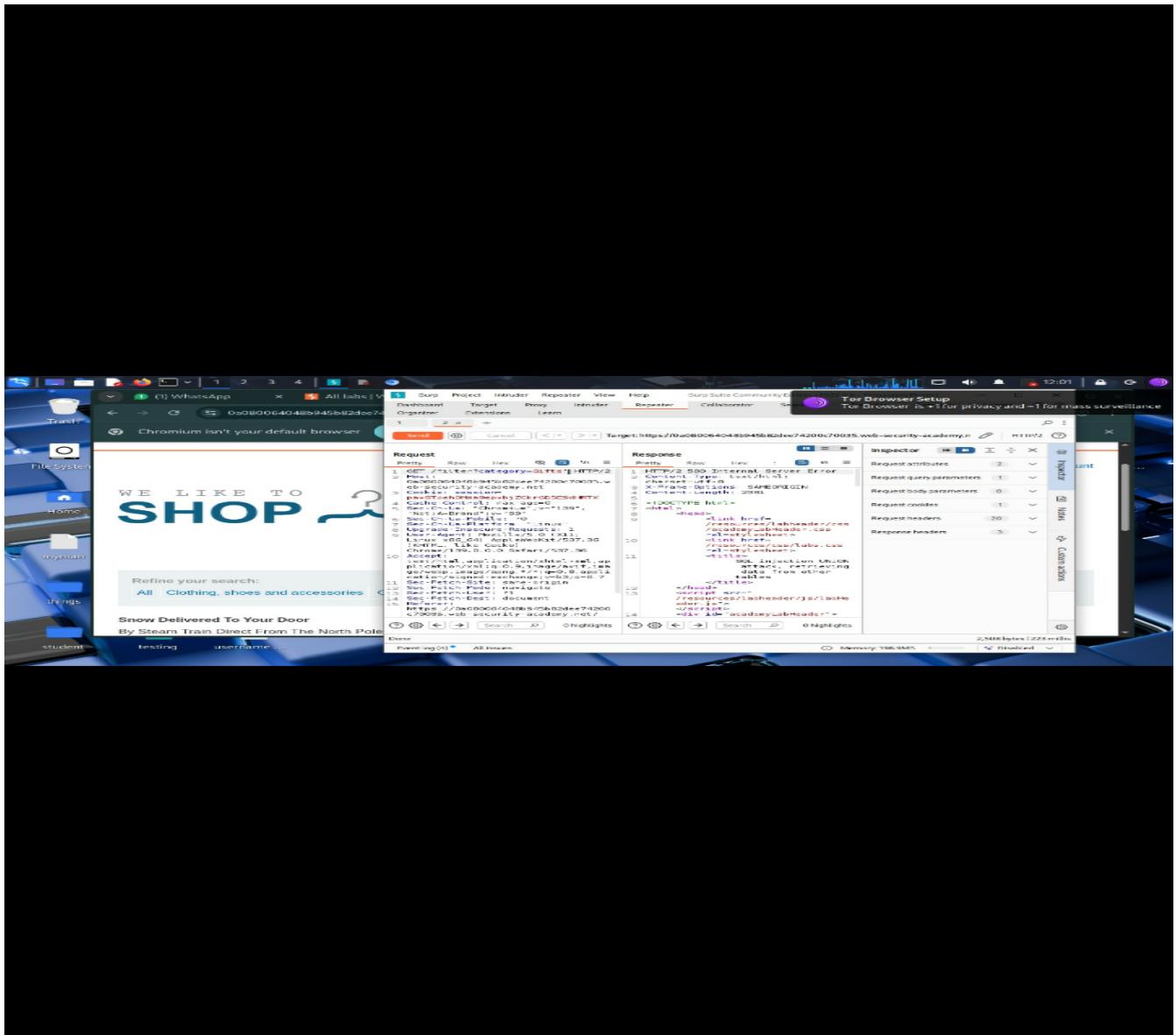
Exploitation Steps

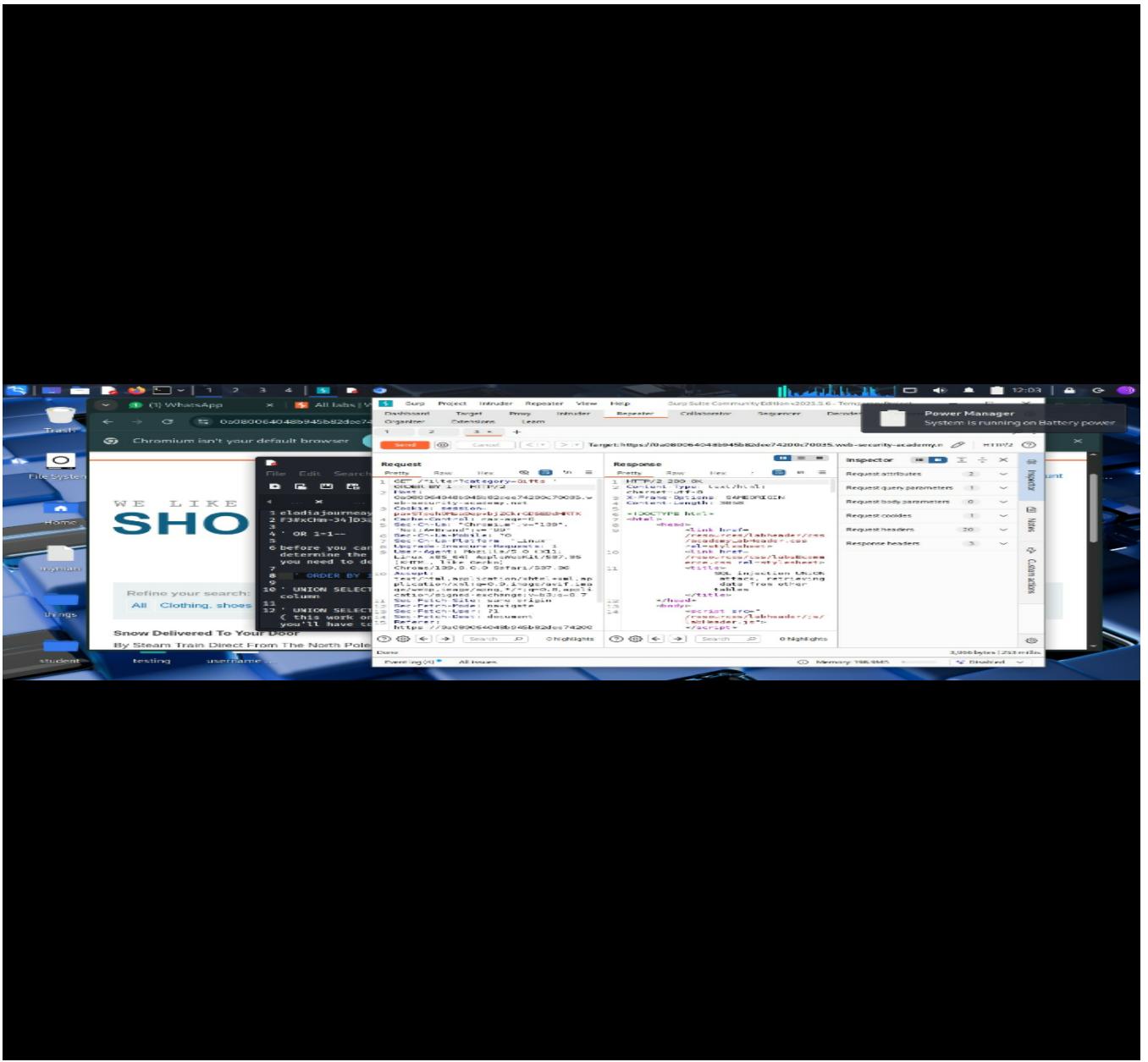
1. Intercepted the request using Burp Suite.
2. Identified the vulnerable category parameter.
3. Determined the number of columns using ORDER BY clauses.
4. Identified which column was reflected on the page using UNION SELECT NULL payloads.
5. Enumerated database tables using information_schema.
6. Extracted usernames and passwords from the users table using a UNION-based payload.

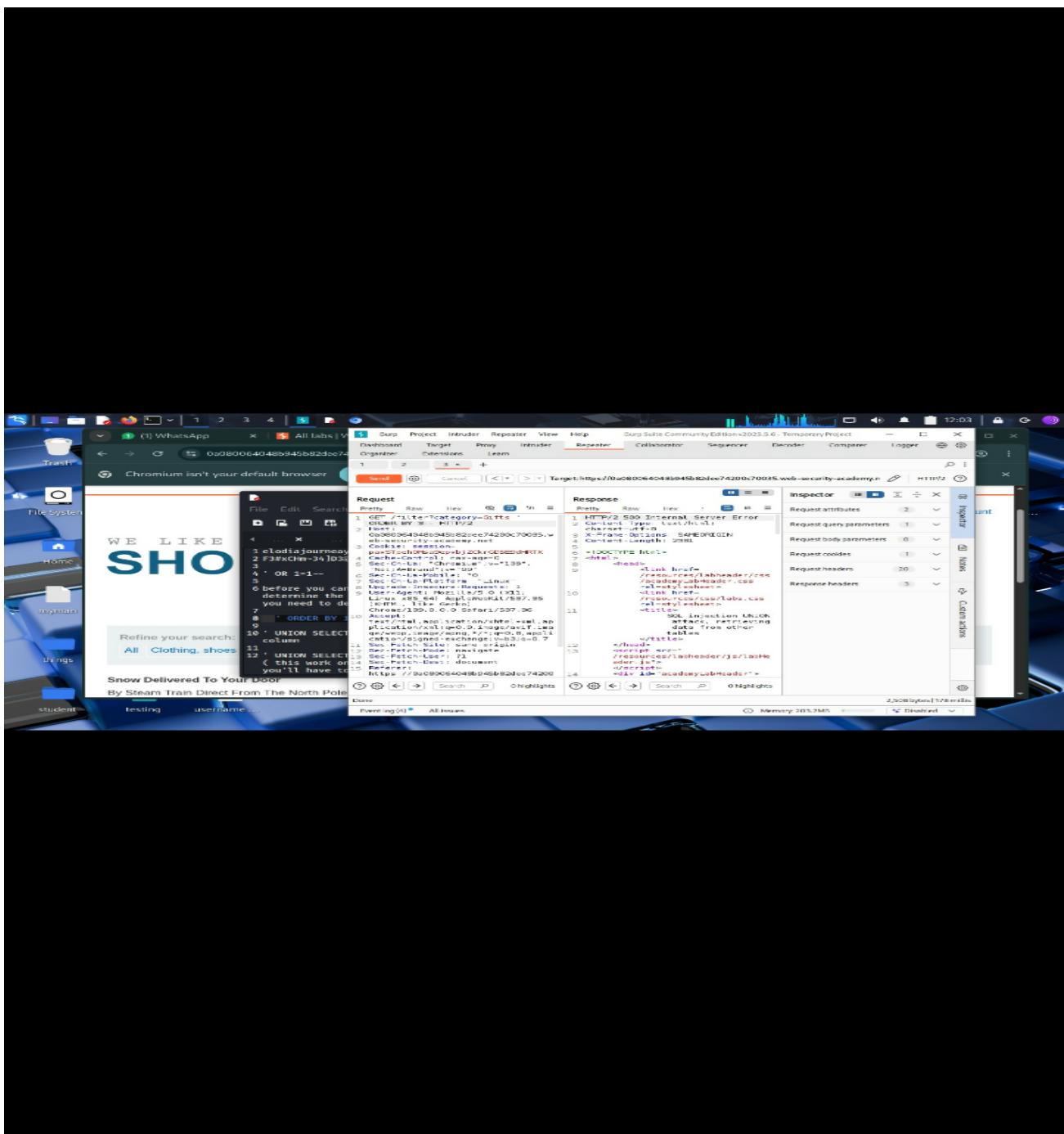
Proof of Exploitation

The screenshots below show successful extraction of sensitive data from the database,

including usernames and passwords, displayed directly on the application page.

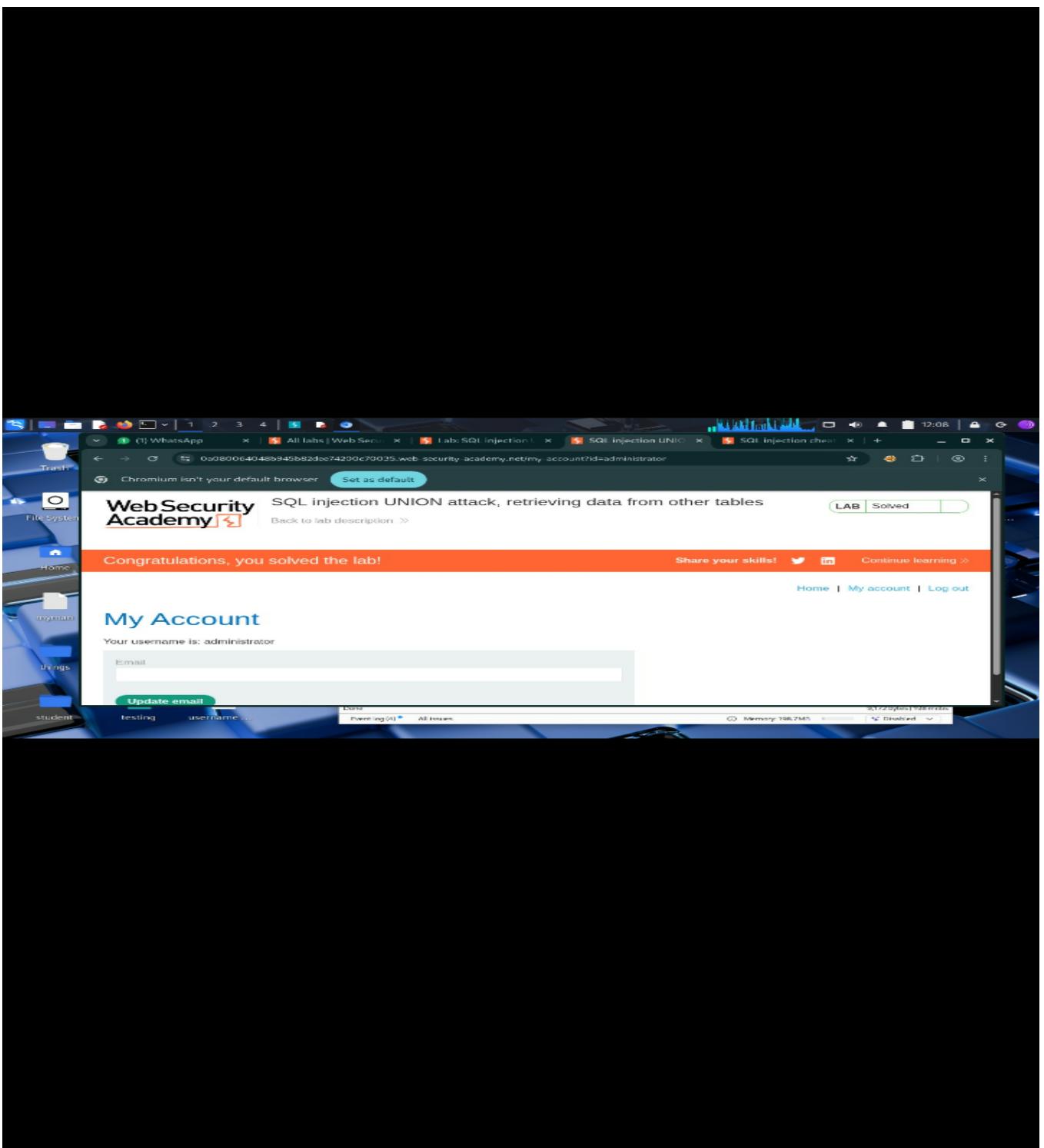












Impact

This vulnerability allows attackers to read sensitive data from the database, including user credentials, which could lead to account compromise and complete application takeover.

Remediation

- Use parameterized queries (prepared statements)
- Enforce strict input validation
- Restrict database user privileges
- Implement proper error handling

Disclaimer

This vulnerability was exploited in a controlled lab environment for educational and portfolio demonstration purposes only.