SQL Injection Vulnerability Report

Lab: SQL Injection – Extracting Hidden Data

Platform: PortSwigger Web Security Academy

Tester: Praisegod Aliyu

Date: [06 Jan, 2026]

Objective

The objective of this lab was to identify and exploit a SQL Injection vulnerability

that allows extraction of hidden data from the database.

Vulnerability Type

SQL Injection (Boolean-based)

OWASP Category: A03 – Injection

Target Description

The target application contains a product listing page that uses a SQL query

to retrieve products from the backend database based on category input.

Vulnerability Discovery

The category parameter was tested by injecting a single quote (')

which resulted in an SQL error, indicating improper input sanitization.

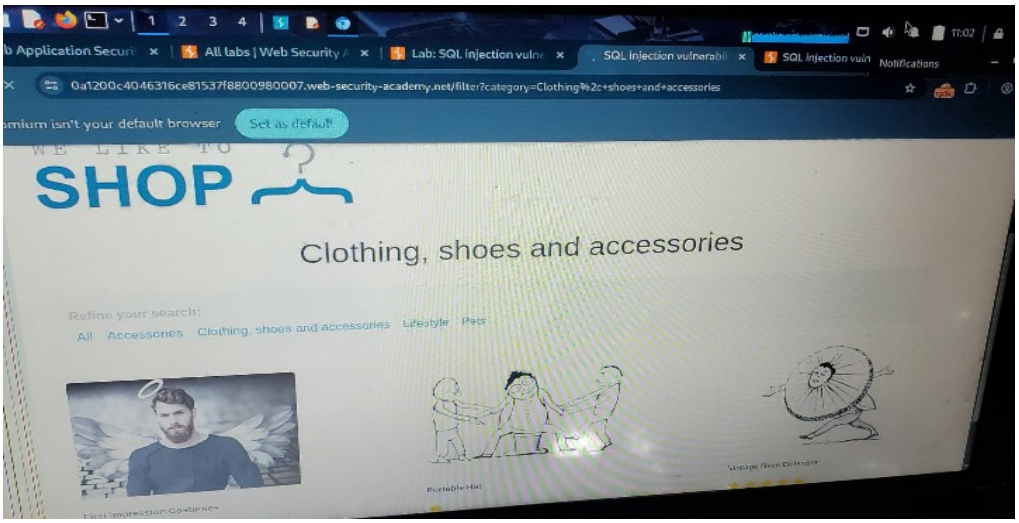
Exploitation Steps

1. Intercepted the request using Burp Suite.

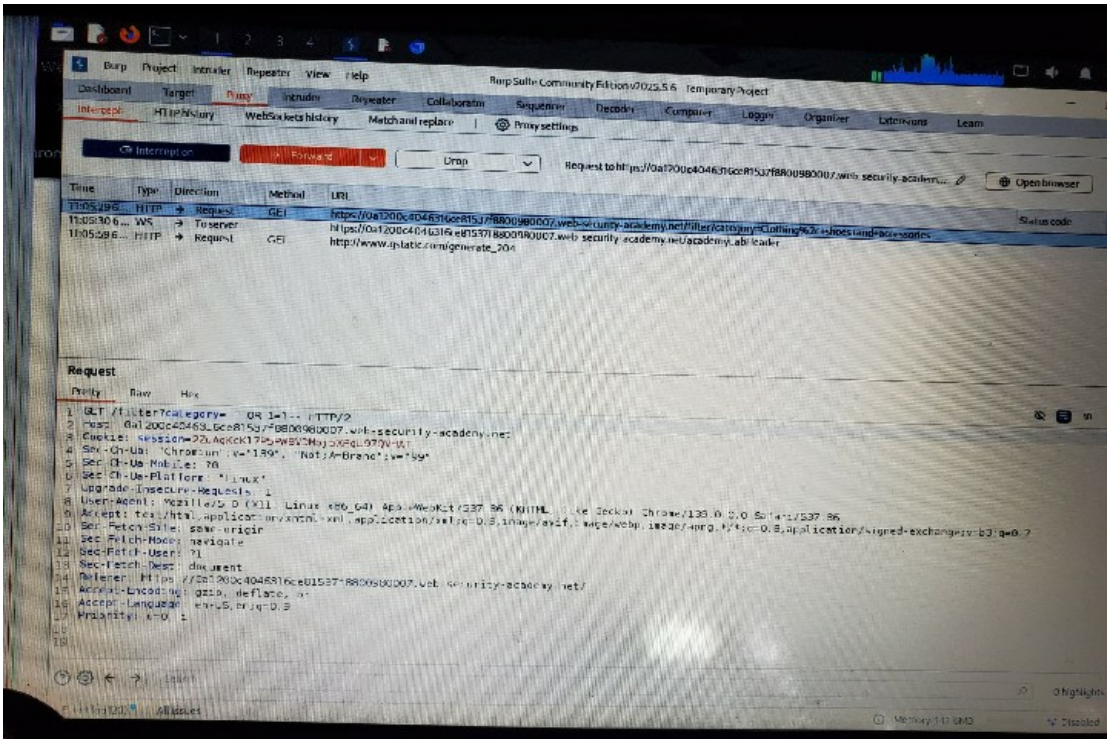
2. Identified the vulnerable 'category' parameter.

3. Injected the following payload: ' OR 1=1--

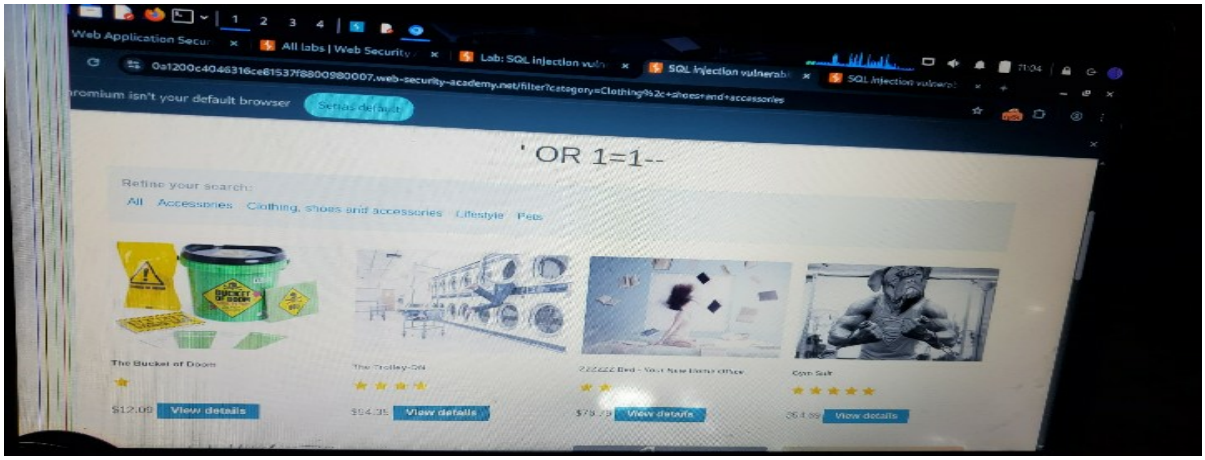
4. The application returned all products, including hidden items.



Before injection



Injecting the payload



After injection (hidden items visible)

Impact

An attacker could exploit this vulnerability to access unauthorized data, potentially exposing sensitive business information.

Remediation

- Use prepared statements (parameterized queries)
- Implement proper input validation
- Avoid dynamic SQL queries