

Vulnerability Assessment & Lab Completion Report

Ethical Hacking Internship: Task 1 & 2

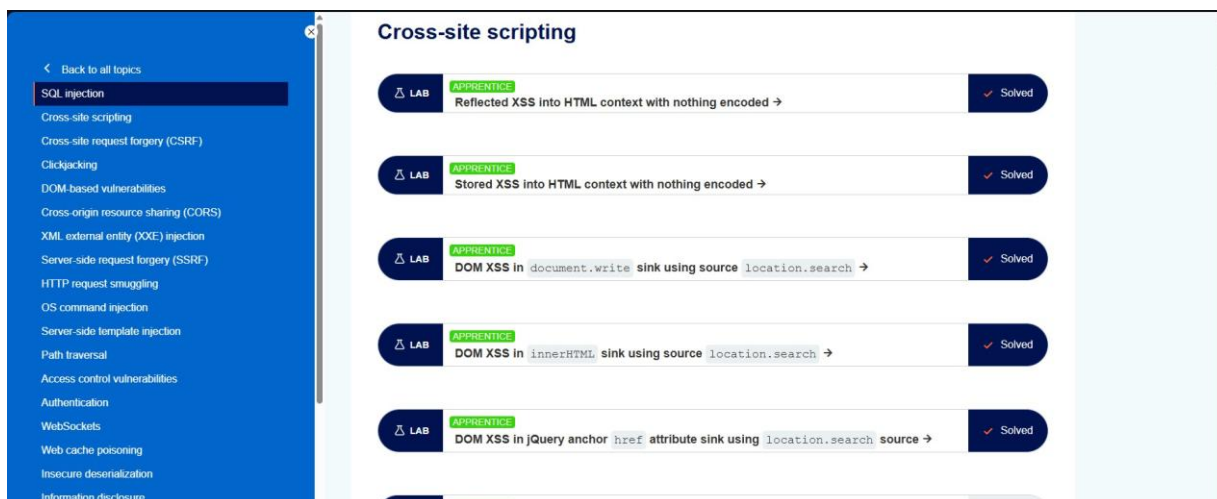
Prepared By: Israel Mbiyavanga David Ethical Hacking Intern

Date: January 23, 2026

Submitted To: Internship Review Committee

Page 1: Task 1 - PortSwigger Labs

• Evidence:



- **Note:** "Successfully completed 5 XSS labs on PortSwigger Academy to demonstrate fundamental understanding of client-side vulnerabilities."

Page 2: Task 2 - Vulnerability Report (testasp.vulnweb.com)

To match the **HackerOne style (#751870)**, use these details for your findings:

Vulnerability 1: Reflected XSS on Search Page

I. Proper Steps:

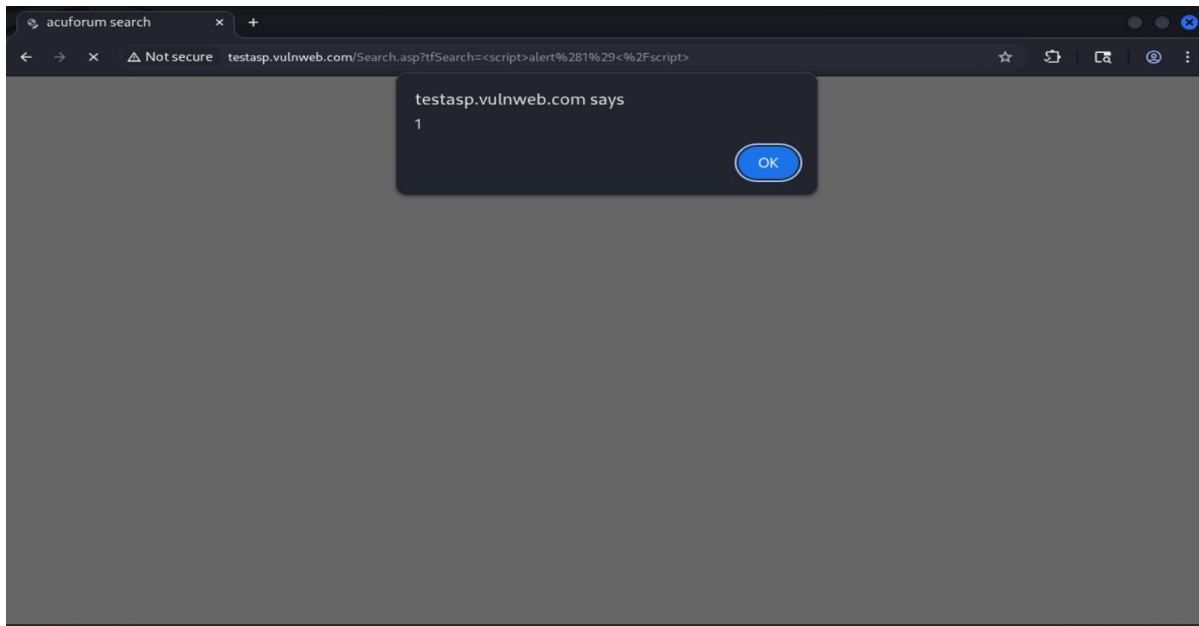
- A. Navigate to <http://testasp.vulnweb.com/Search.asp>.
- B. Enter `<script>alert(1)</script>` into the search field.
- C. Click "Search Posts."

II. Evidence:

A. Video:

<https://drive.google.com/file/d/1ImWx8osV6b-c8uRZGaqRMxL2sDqwFwtj/view?usp=sharing>

B. Screenshot:



Vulnerability 2: SQL Injection on Login Page

I. Proper Steps:

- Navigate to the login page
<http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F>
- Enter ' OR 1=1-- in the username field.
- Intercept the POST request in Burp Suite and send to Repeater.
- Observe the 500 Internal Server Error which confirms the database query was successfully manipulated.

II. Evidence:

A. Screenshot:

