# Proof of Concept Report: XSS Vulnerabilities

**Prepared by:** Ishan Chowdhury  
**Intern ID:** 159  
**Team:** SkullFaced

## Introduction

This report demonstrates successful exploitation of two Cross-Site Scripting (XSS) vulnerabilities identified in PortSwigger Web Security Academy labs. Both stored and reflected XSS attacks were tested.

The objective was to validate the presence of XSS, execute proof-of-concept payloads, and record evidence of execution with customized alert messages containing the intern’s details.

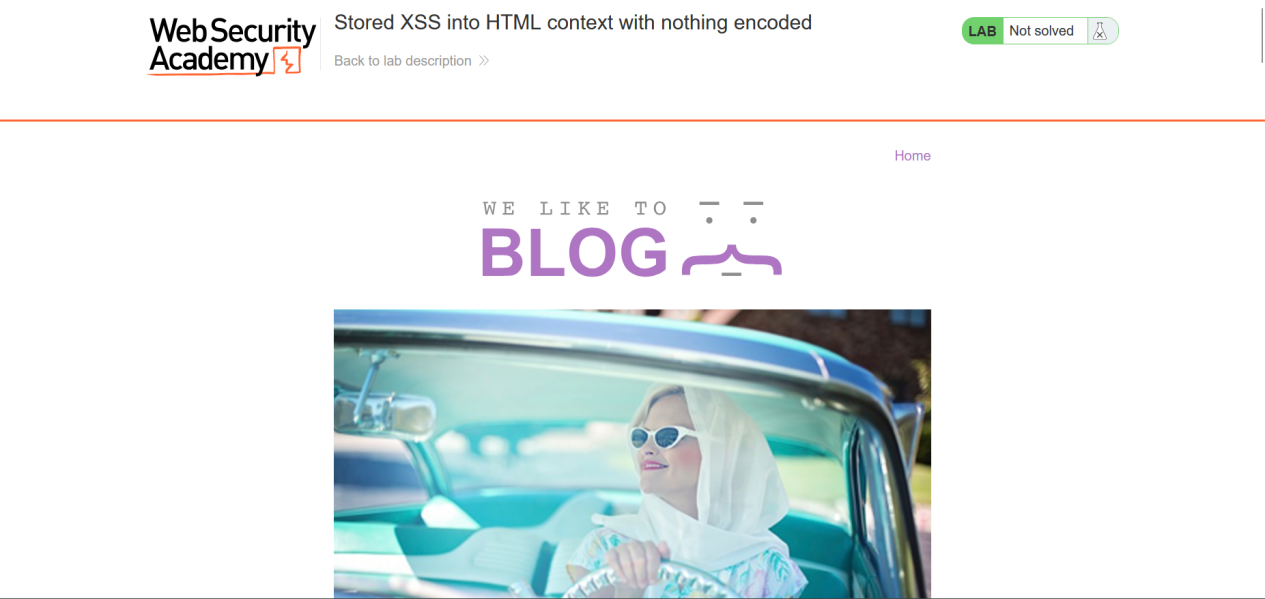
## Stored XSS PoC

**Payload Used:**

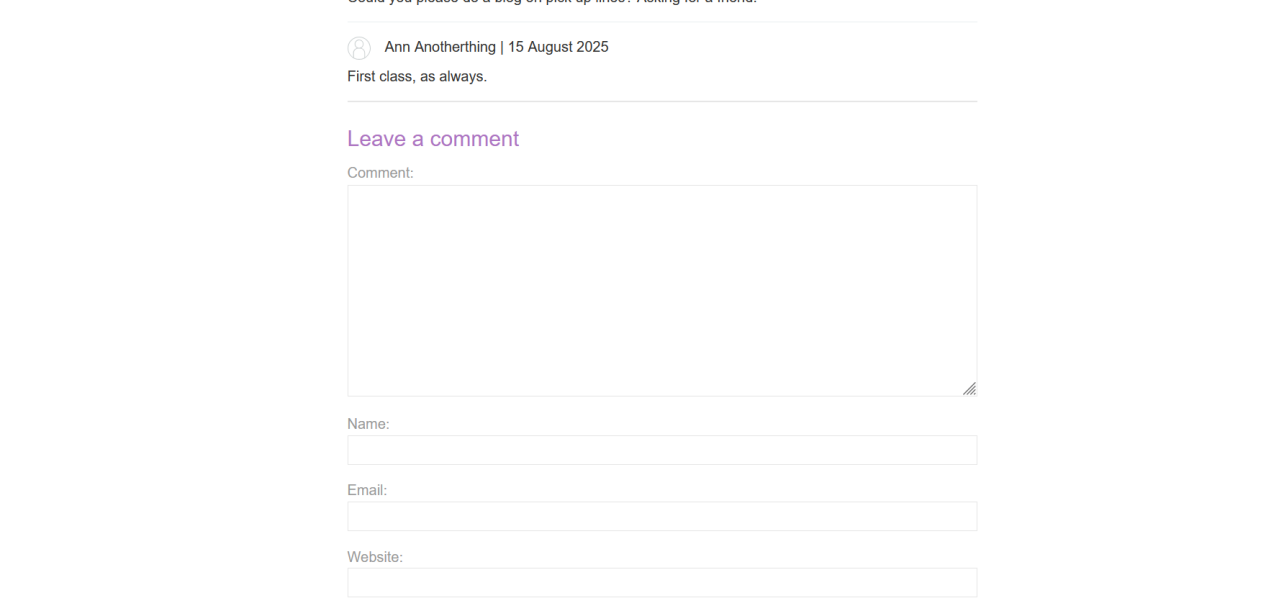
<script>alert(1)</script>

**Steps to Reproduce:**

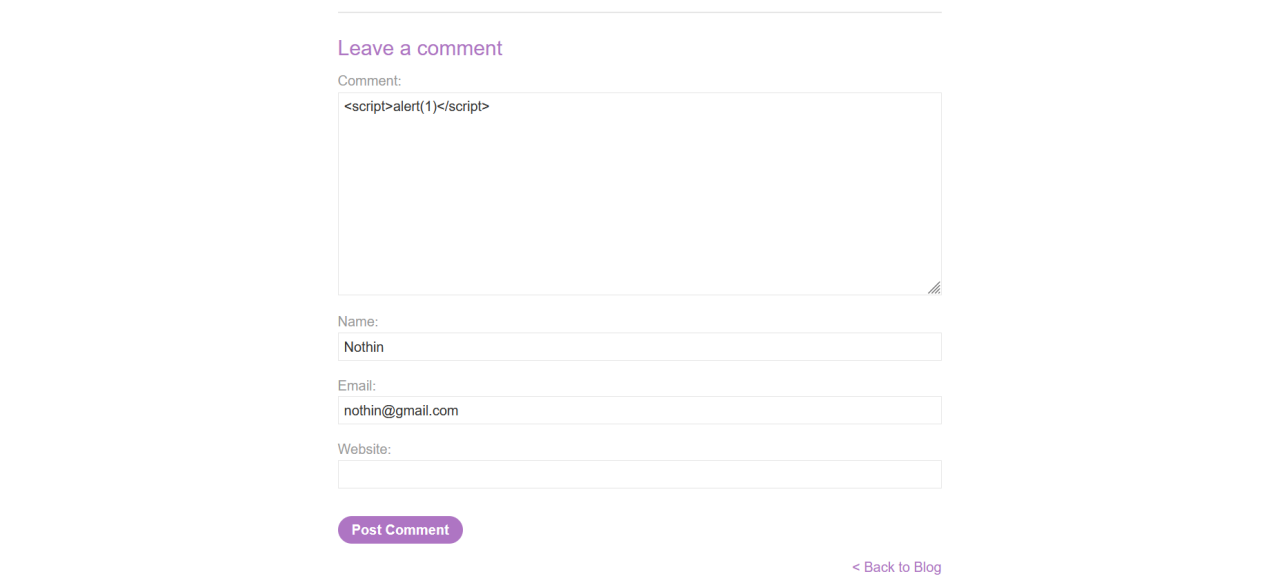
Navigate to a blog post.



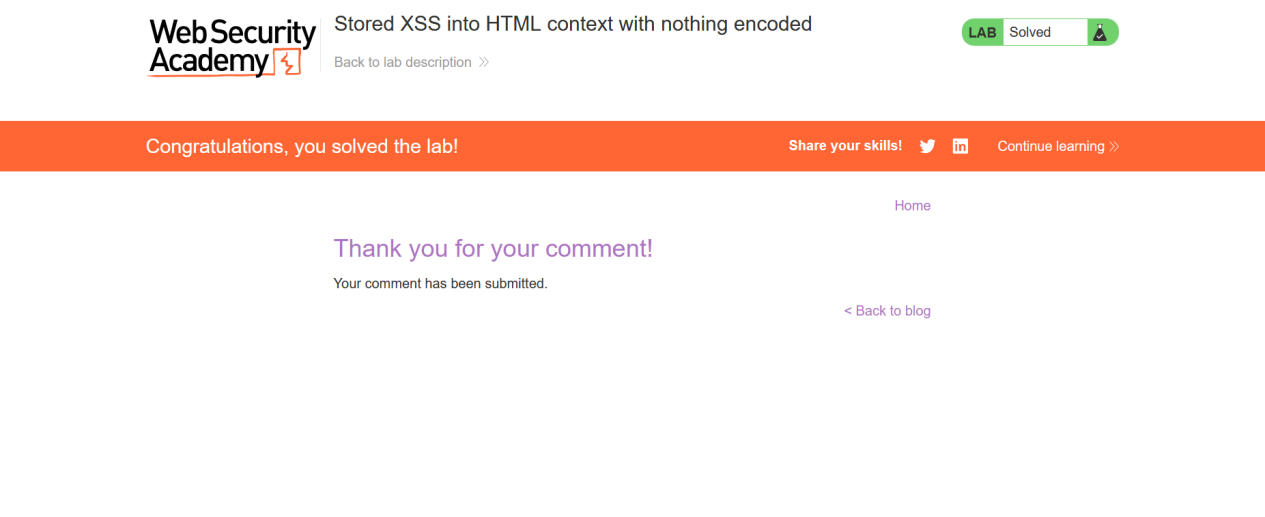
Scroll down to the comment section.



Submit the payload in the comment field.



Reload the blog post page.



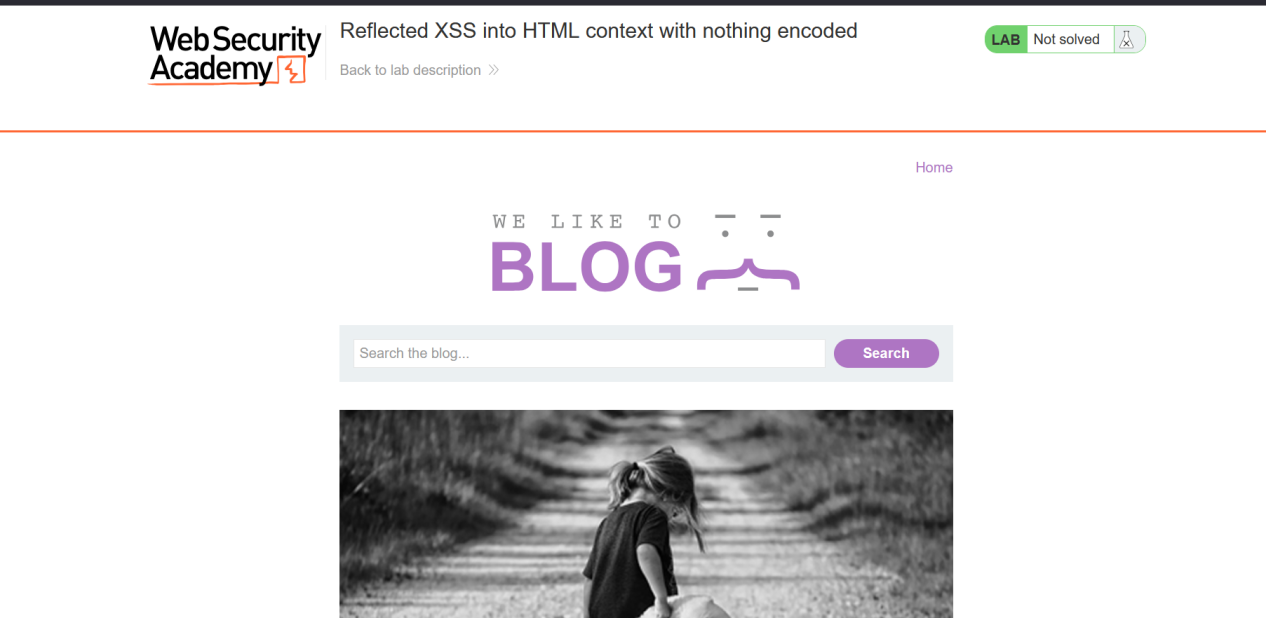
## Reflected XSS PoC

**Payload Used:**

<script>alert(1)</script>

**Steps to Reproduce:**

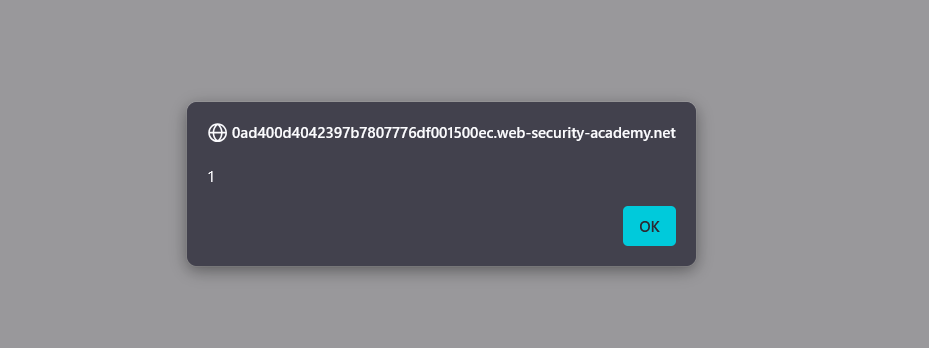
Enter the payload in the search box.

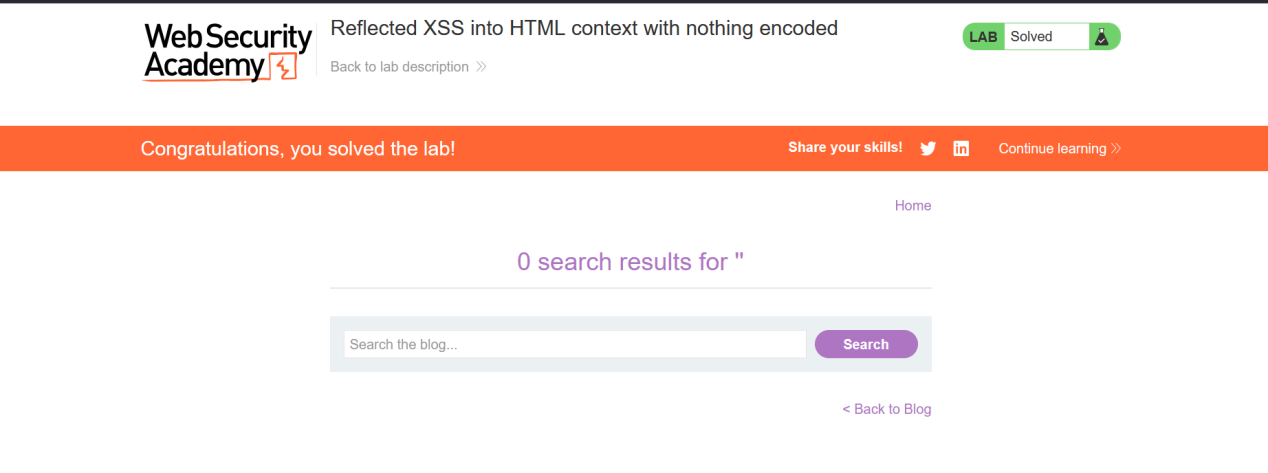


Submit the search.



The script executes immediately and displays the alert message.





## Impact & Mitigation

**Impact:**

An attacker could inject arbitrary JavaScript into web pages viewed by other users.

This could lead to credential theft, session hijacking, or malicious redirects.

Stored XSS persists across sessions and affects multiple users, while reflected XSS can be exploited via crafted URLs.

**Mitigation:**

Properly sanitize and encode user input before rendering into HTML.

Implement Content Security Policy (CSP) headers to reduce the risk of script execution.

Use frameworks and libraries with built-in XSS protection.

Perform regular security testing and input validation.