Task 1

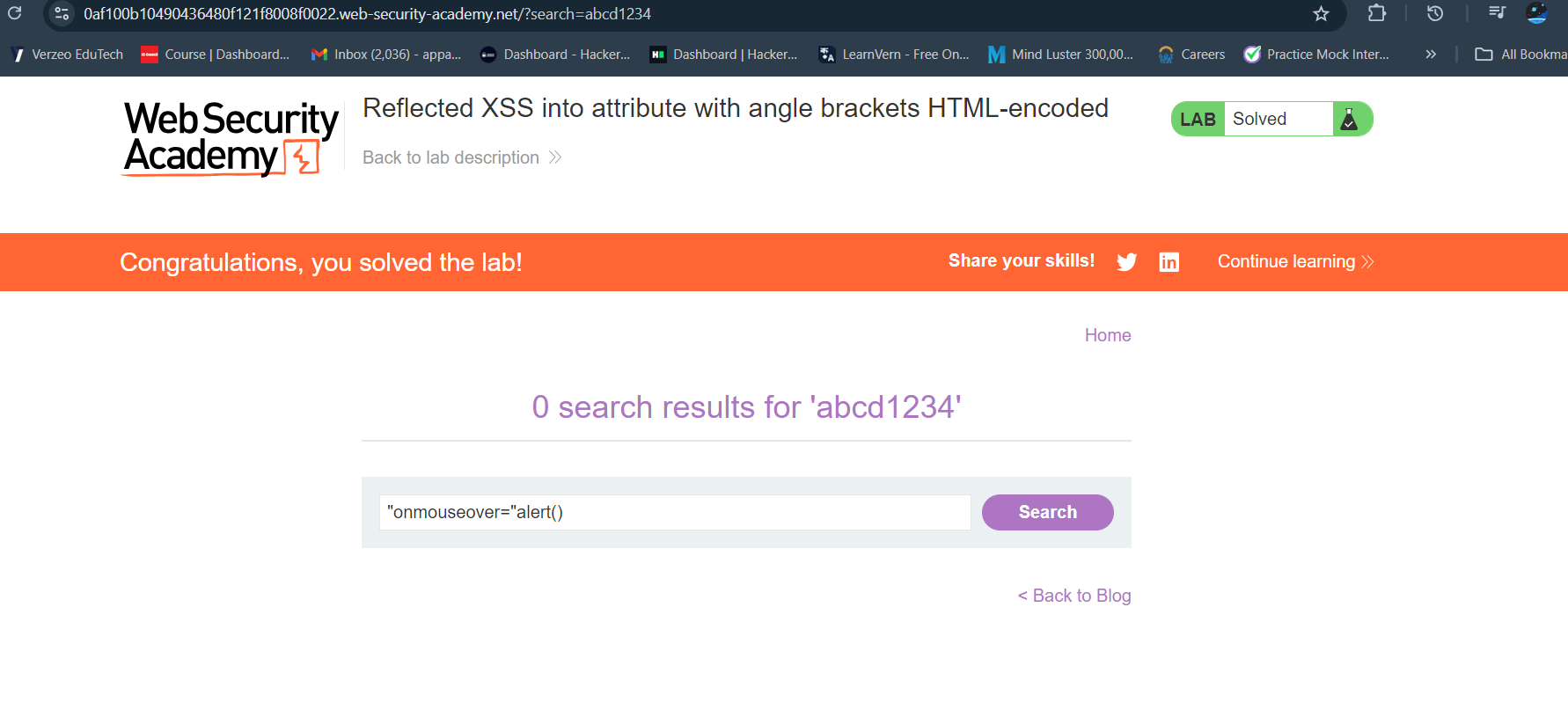
<https://portswigger.net/web-security/all-labs>.

Answers Screenshots

Lab 1

This lab contains a [reflected cross-site scripting](https://portswigger.net/web-security/cross-site-scripting/reflected) vulnerability in the search query tracking functionality where angle brackets are encoded. The reflection occurs inside a JavaScript string. To solve this lab, perform a cross-site scripting attack that breaks out of the JavaScript string and calls the alert function.

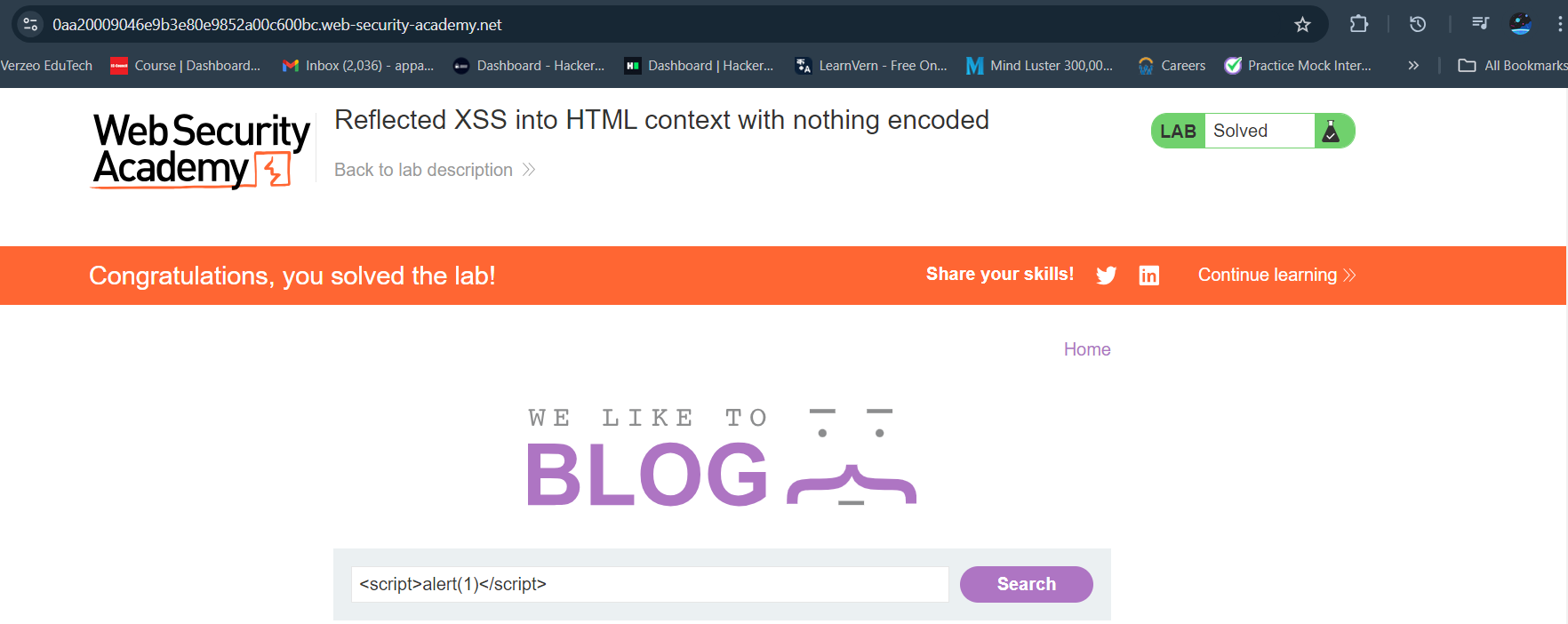
Reflected XSS into attribute with angle brackets HTML-encoded



Lab 2

This lab contains a simple [reflected cross-site scripting](https://portswigger.net/web-security/cross-site-scripting/reflected) vulnerability in the search functionality.

To solve the lab, perform a cross-site scripting attack that calls the alert function.

Reflected XSS into HTML context with nothing encoded

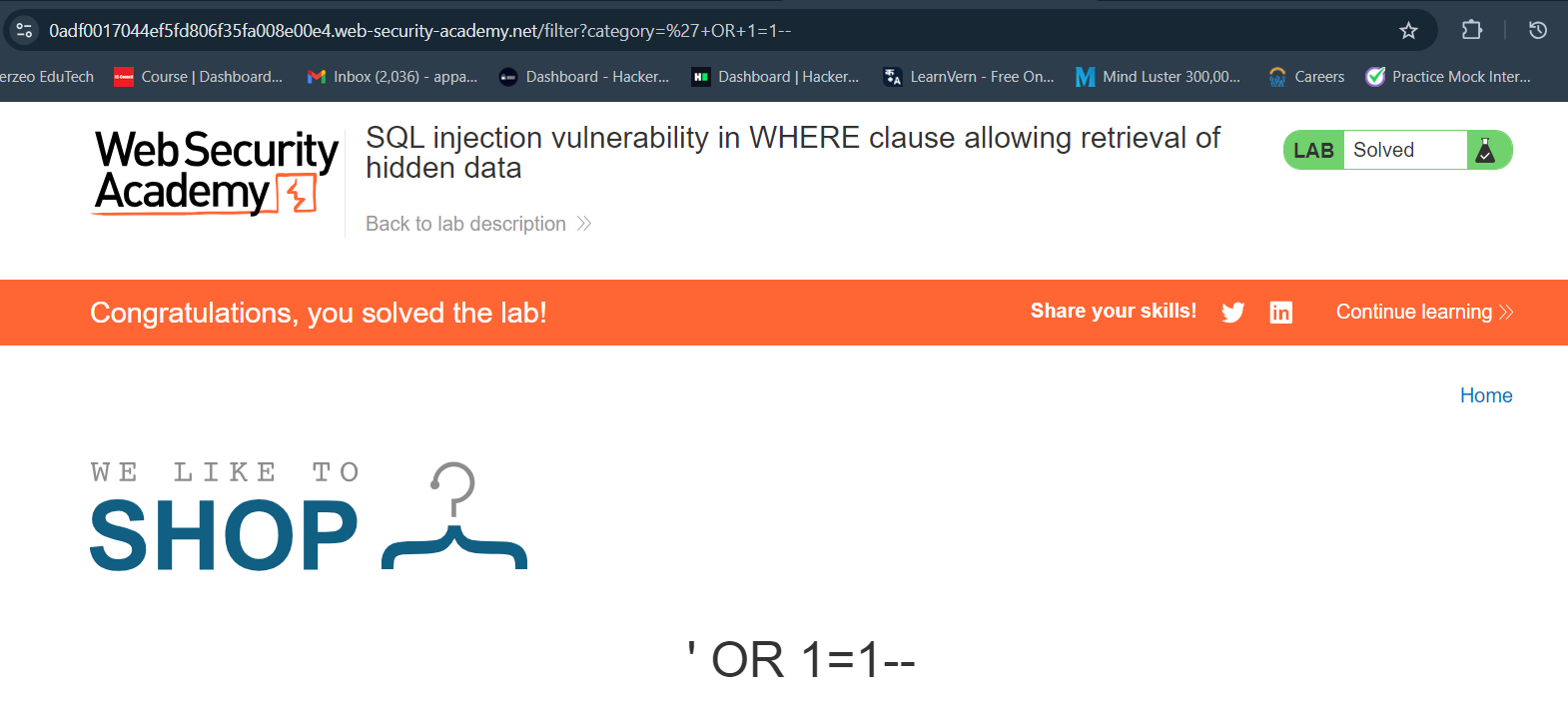
Lab3:

This lab contains a [SQL injection](https://portswigger.net/web-security/sql-injection) vulnerability in the product category filter. When the user selects a category, the application carries out a SQL query like the following:

SELECT \* FROM products WHERE category = 'Gifts' AND released = 1

To solve the lab, perform a SQL injection attack that causes the application to display one or more unreleased products.

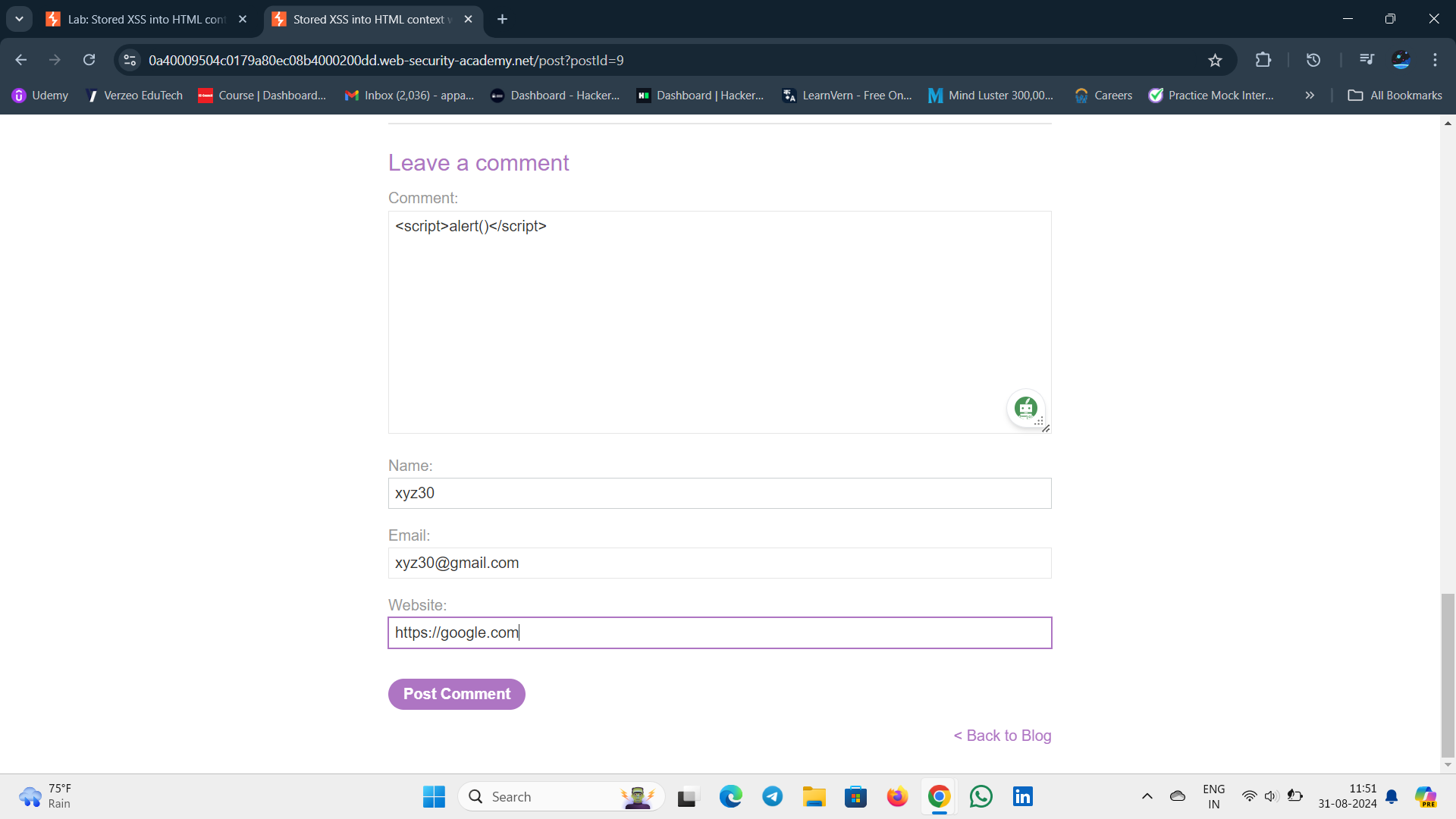
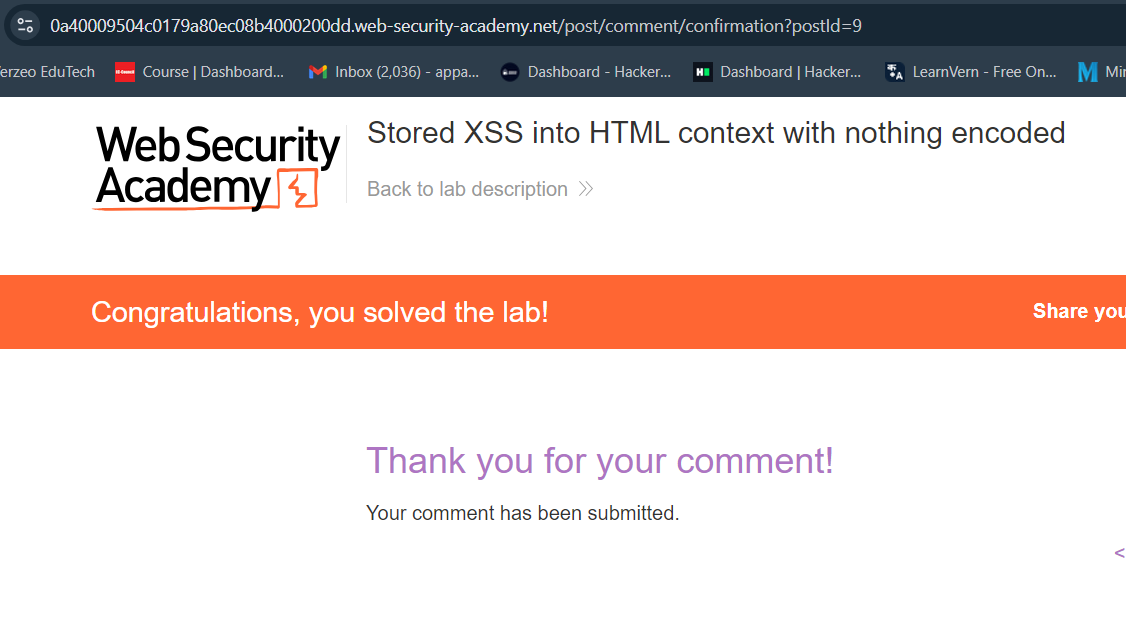
SQL injection vulnerability in WHERE clause allowing retrieval of hidden data



Lab 4:

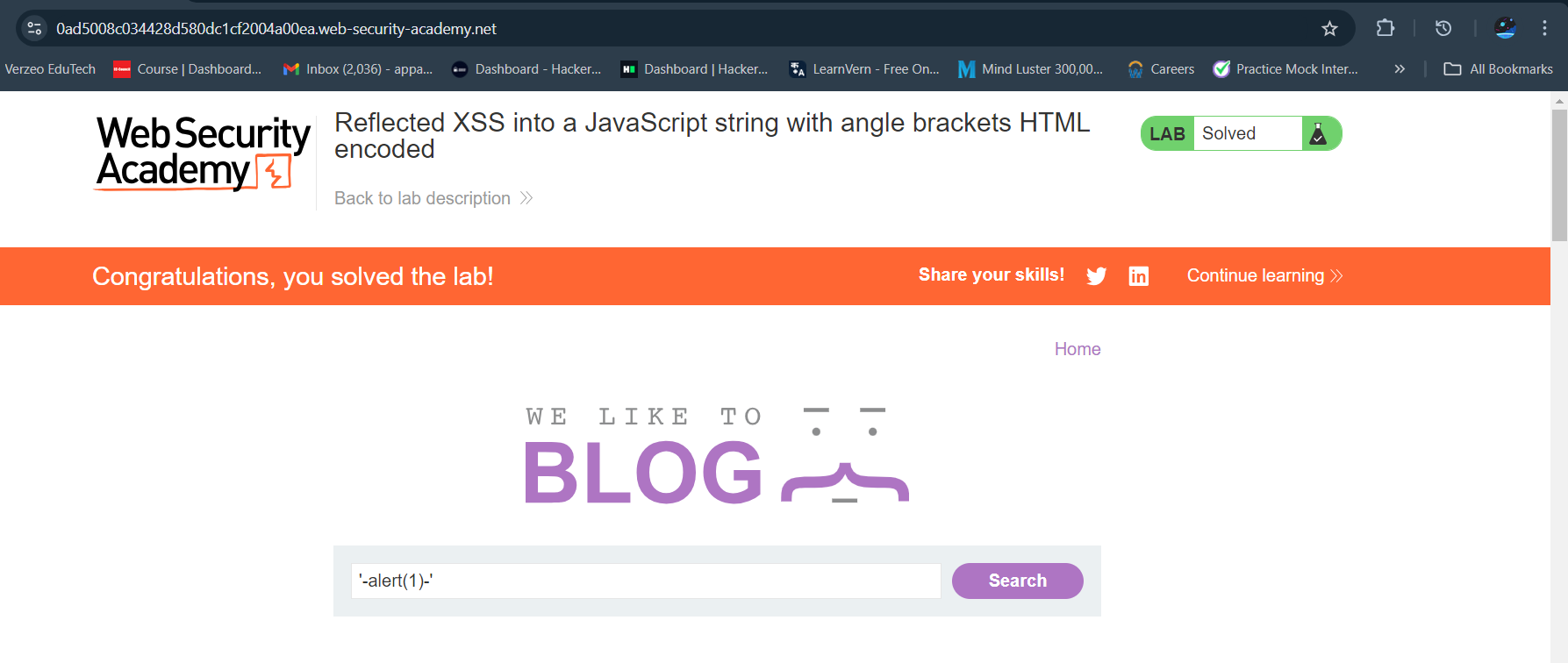
This lab contains a [stored cross-site scripting](https://portswigger.net/web-security/cross-site-scripting/stored) vulnerability in the comment functionality.

To solve this lab, submit a comment that calls the alert function when the blog post is viewed.

Stored XSS into HTML context with nothing encoded

Lab 5:

This lab contains a [reflected cross-site scripting](https://portswigger.net/web-security/cross-site-scripting/reflected) vulnerability in the search query tracking functionality where angle brackets are encoded. The reflection occurs inside a JavaScript string. To solve this lab, perform a cross-site scripting attack that breaks out of the JavaScript string and calls the alert function.

Reflected XSS into a JavaScript string with angle brackets HTML encoded