Task 1

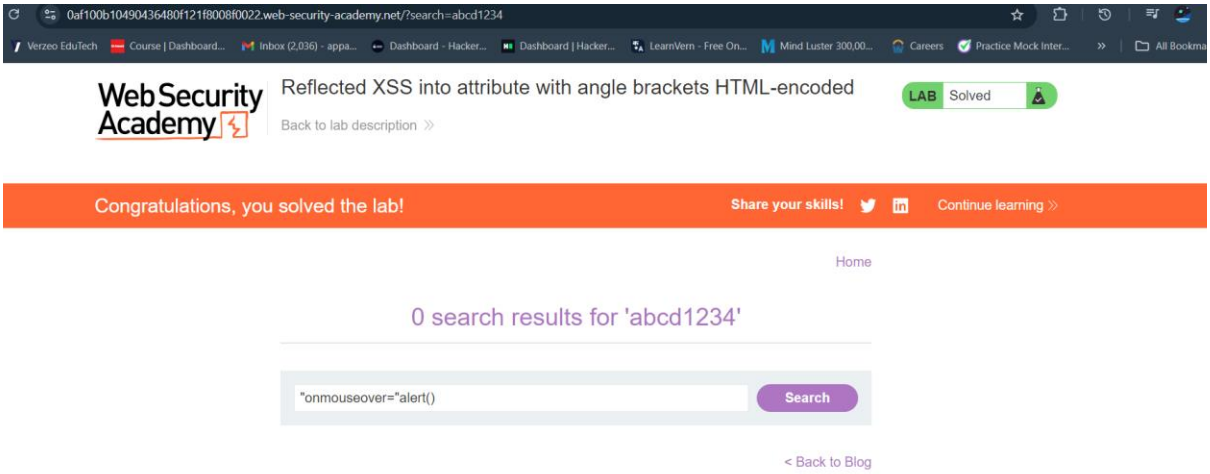
https://portswigger.net/web-security/all-labs.

Answers Screenshots

Lab 1

This lab contains a reflected cross-site scripting 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



0af100b10490436480f121f8008f0022.web-security-academy.net/?search=abcd1234

Reflected XSS into attribute with angle brackets HTML-encoded

Congratulations, you solved the lab!

0 search results for 'abcd1234'

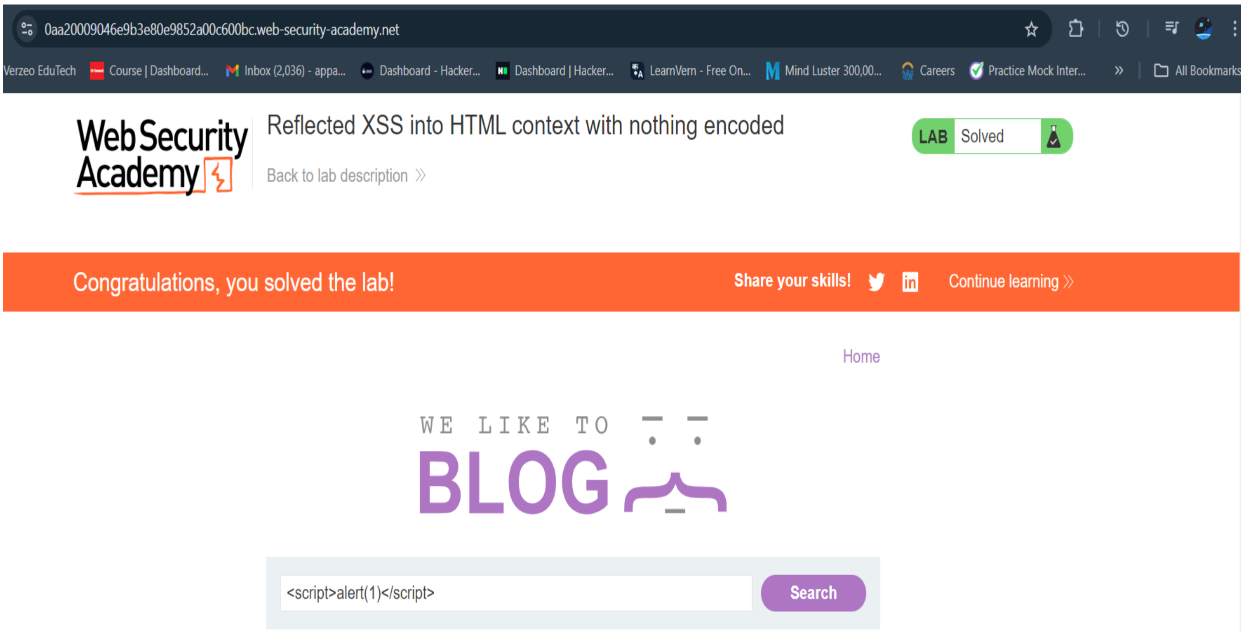
"onmouseover="alert()

Lab 2

This lab contains a simple reflected cross-site scripting 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



Reflected XSS into HTML context with nothing encoded

Back to lab description

Congratulations, you solved the lab!

<script>alert(1)</script>

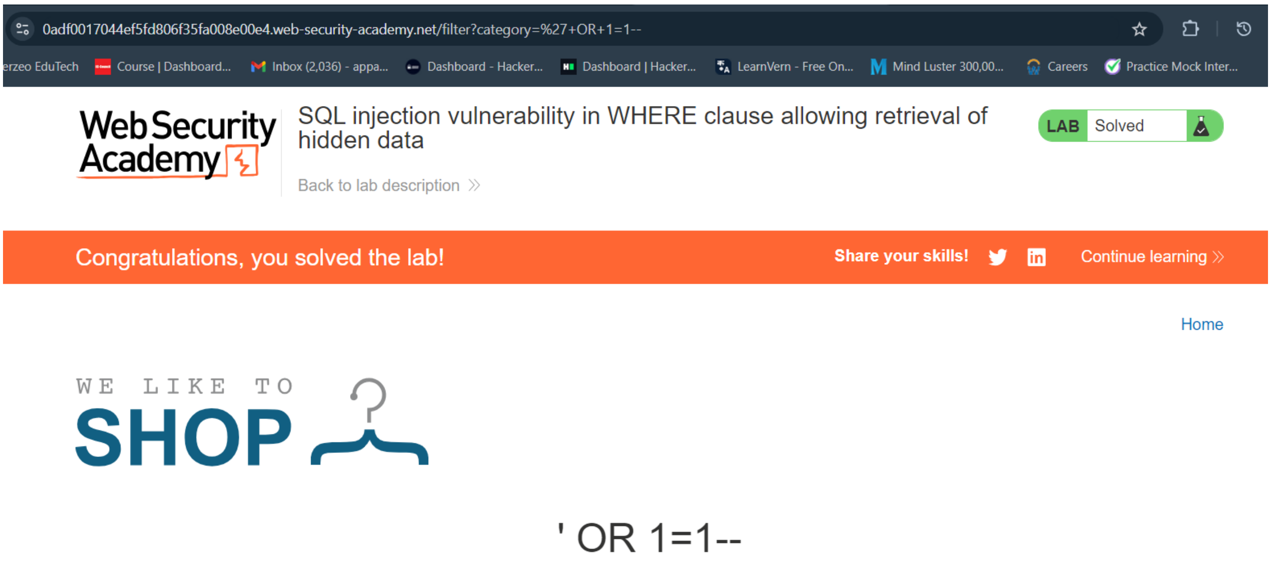
Lab3:

This lab contains a 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



0adf0017044ef5fd806f35fa008e00e4.web-security-academy.net/filter?category=%27+OR+1=1--

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

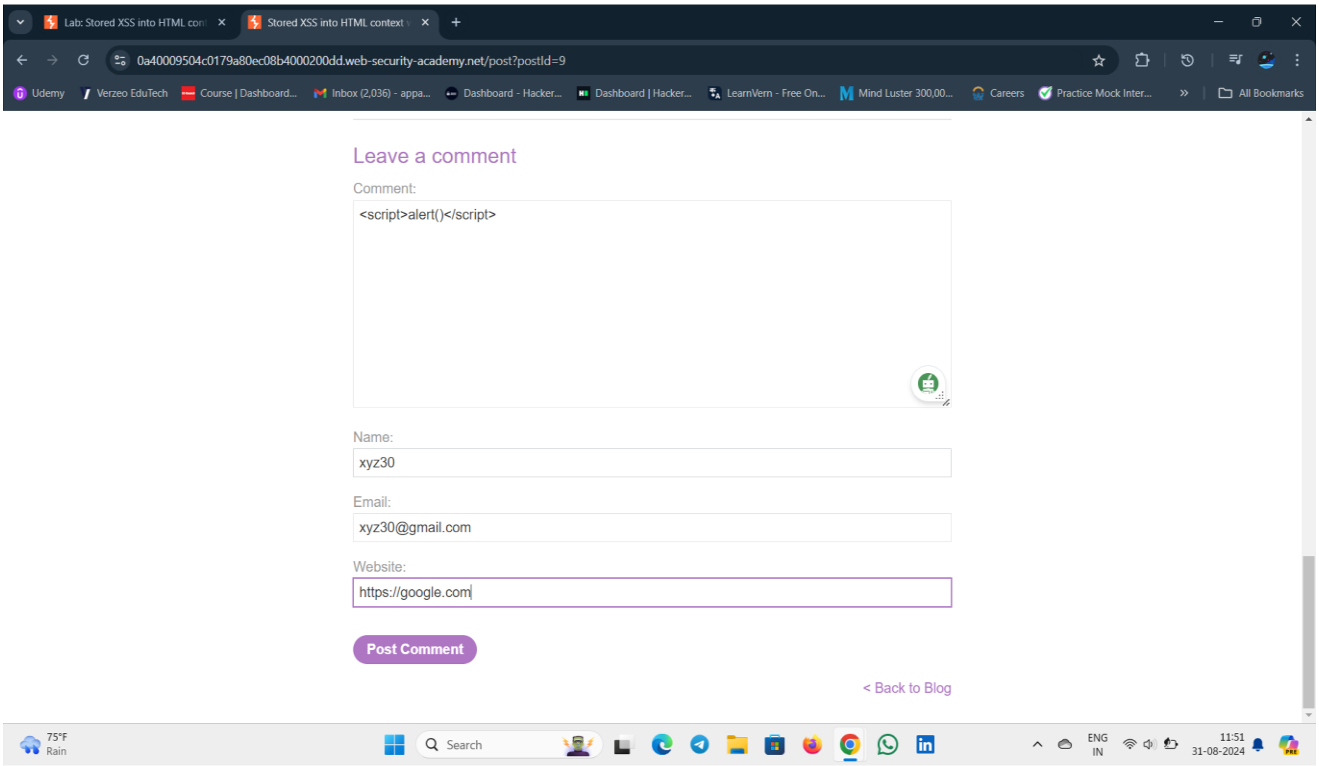
Congratulations, you solved the lab!

' OR 1=1--

Lab 4:

This lab contains a stored cross-site scripting vulnerability in the comment functionality.

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



Lab: Stored XSS into HTML con… | Stored XSS into HTML context…

0a40009504c0179a80ec08b4000200dd.web-security-academy.net/post?postId=9

Leave a comment

Comment:

<script>alert()</script>

Name:

xyz30

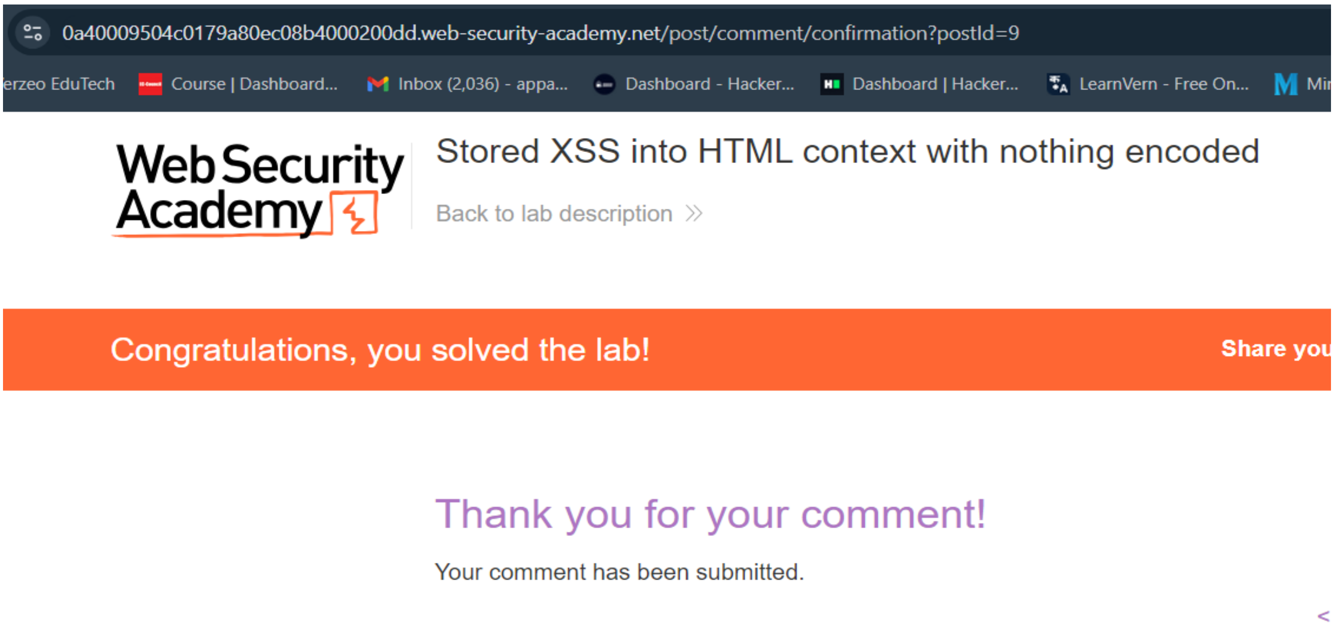
Email:

xyz30@gmail.com

Website:

https://google.com

Stored XSS into HTML context with nothing encoded



0a40009504c0179a80ec08b4000200dd.web-security-academy.net/post/comment/confirmation?postId=9

Stored XSS into HTML context with nothing encoded

Back to lab description »

Congratulations, you solved the lab!

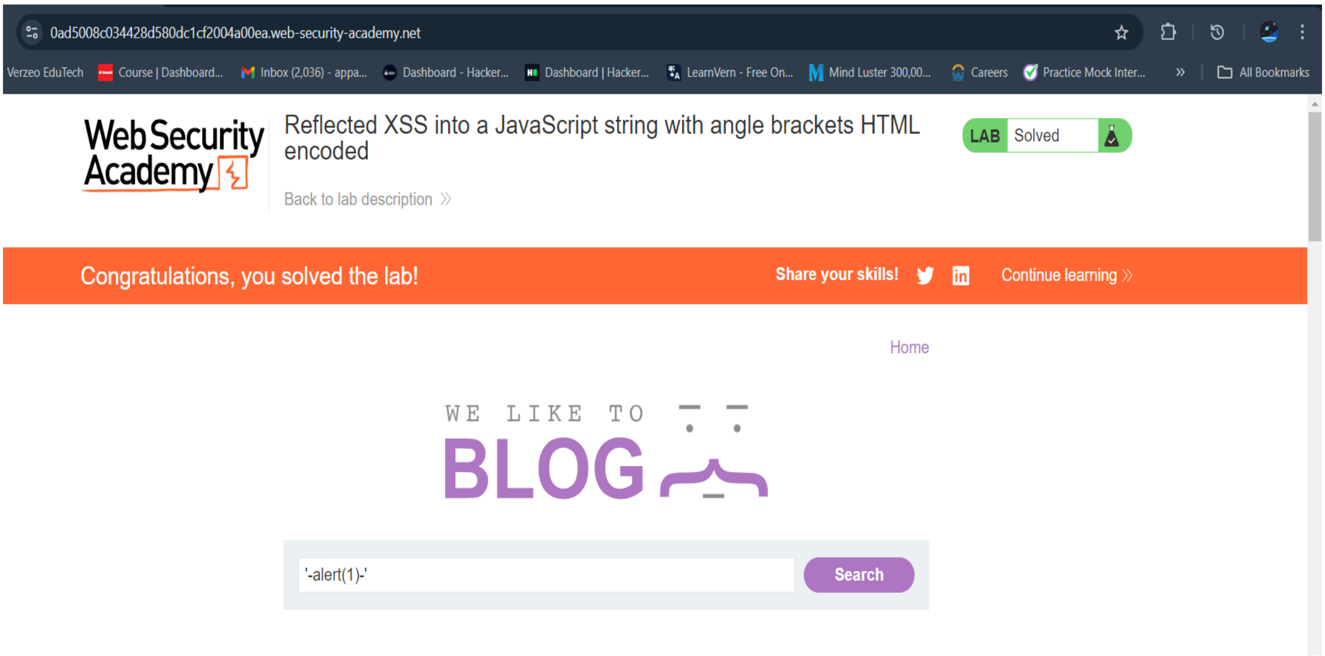
Thank you for your comment!

Your comment has been submitted.

Lab 5:

This lab contains a reflected cross-site scripting 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



0ad5008c034428d580dc1cf2004a00ea.web-security-academy.net

Reflected XSS into a JavaScript string with angle brackets HTML encoded

Congratulations, you solved the lab!

'-alert(1)-'