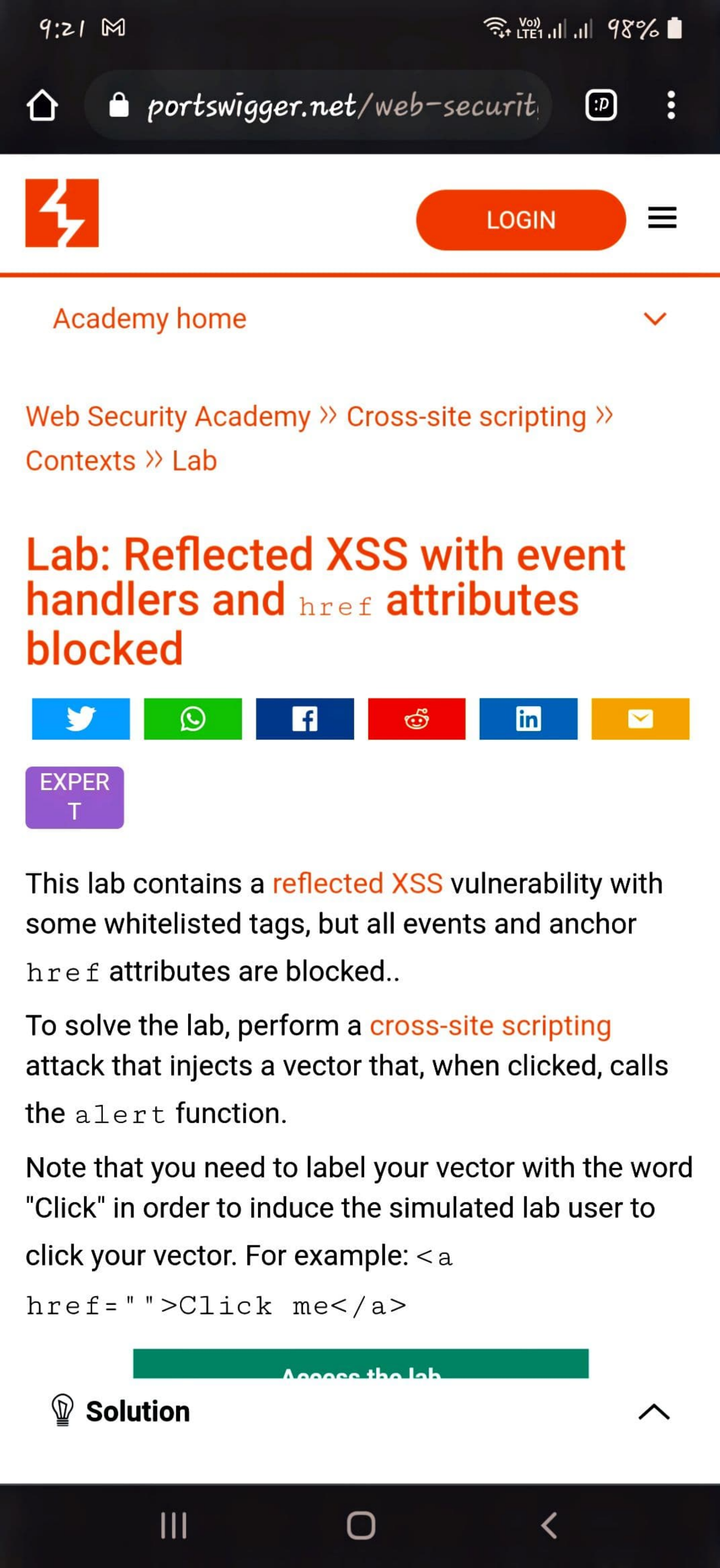


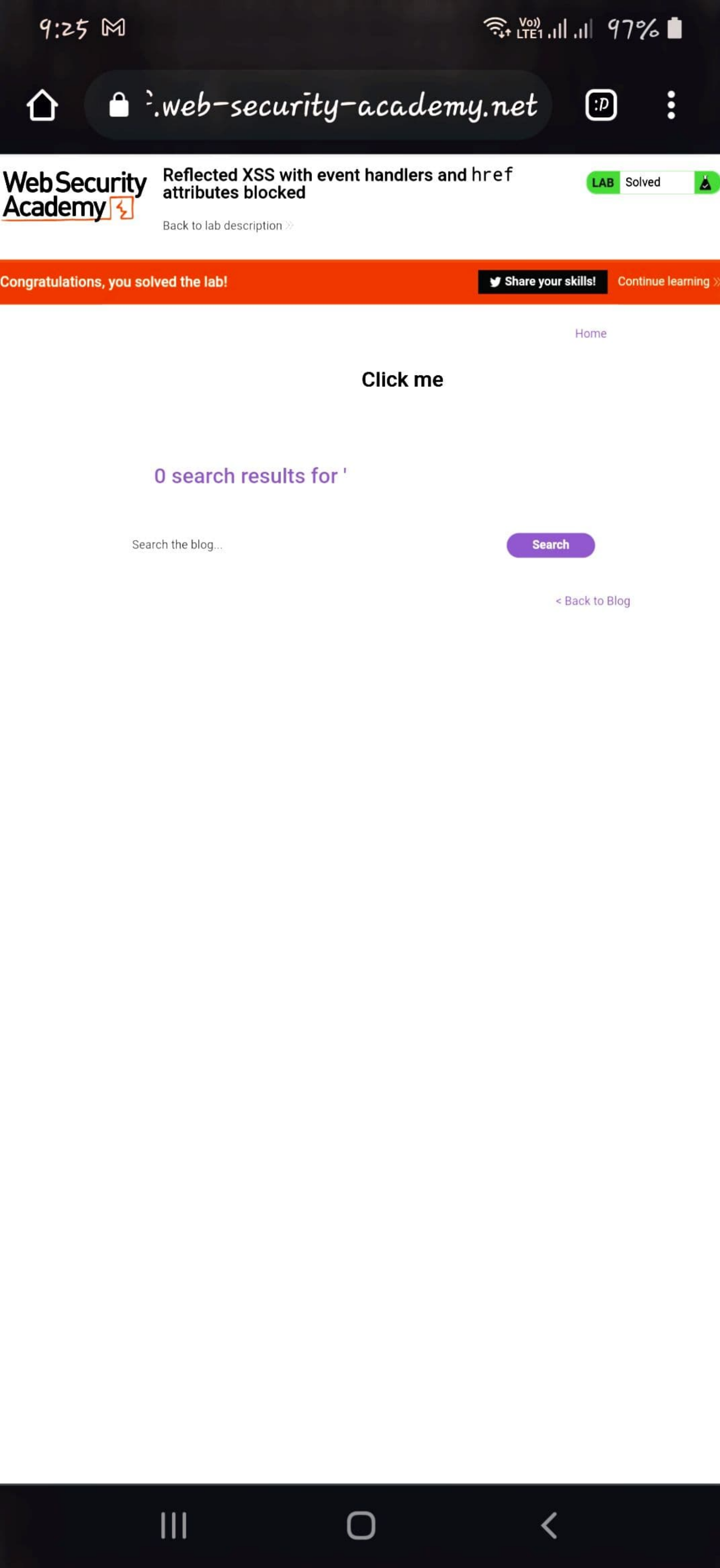
Web Security Academy » Cross-site scripting » Contexts » Lab

Lab: Reflected XSS with event handlers and `href` attributes blocked

This lab contains a reflected XSS vulnerability with some whitelisted tags, but all events and anchor `href` attributes are blocked..

To solve the lab, perform a cross-site scripting attack that injects a vector that, when clicked, calls the `alert` function.

Note that you need to label your vector with the word "Click" in order to induce the simulated lab user to click your vector. For example: `<a href="">Click me</a>`



WebSecurity Academy

Reflected XSS with event handlers and `href` attributes blocked

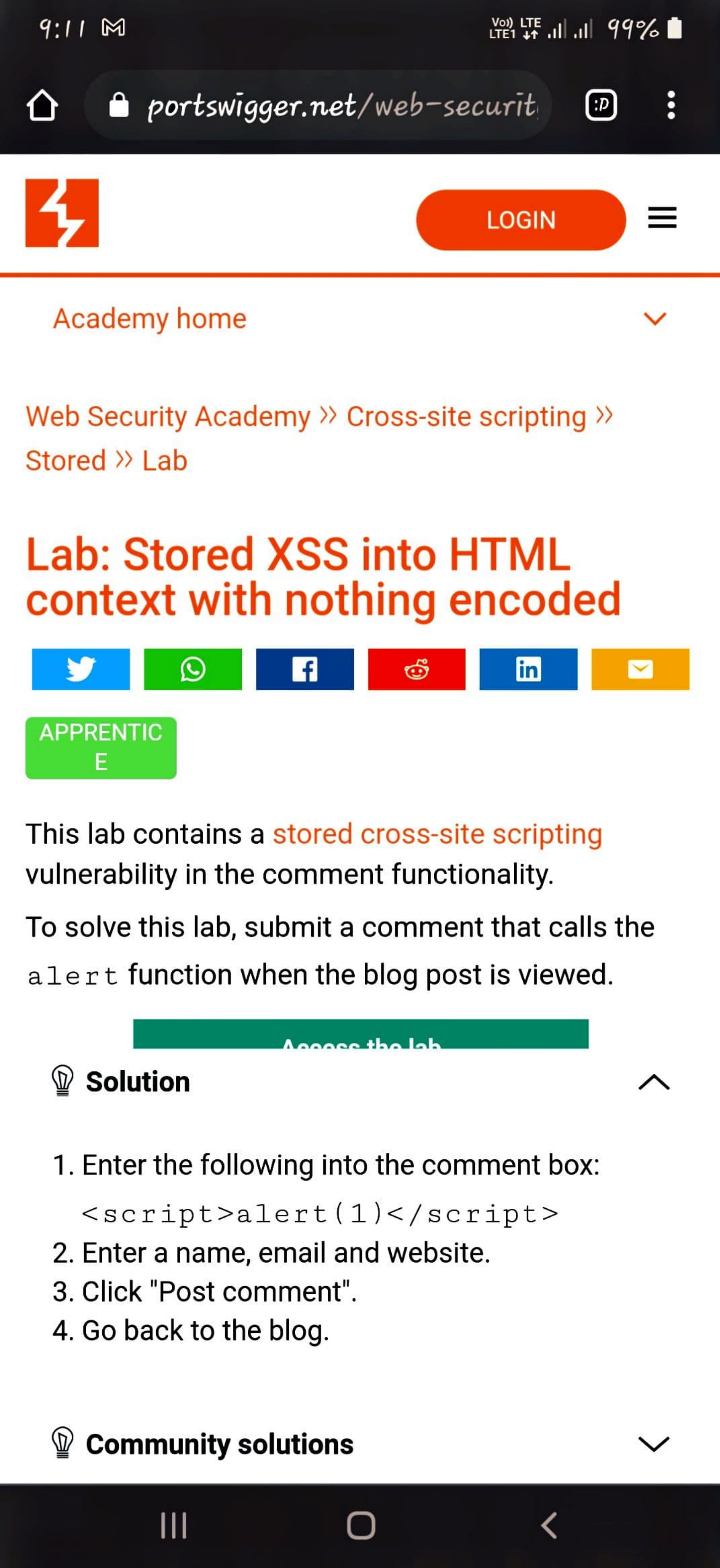
Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Click me

0 search results for '



Web Security Academy » Cross-site scripting » Stored » Lab

Lab: Stored XSS into HTML context with nothing encoded

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

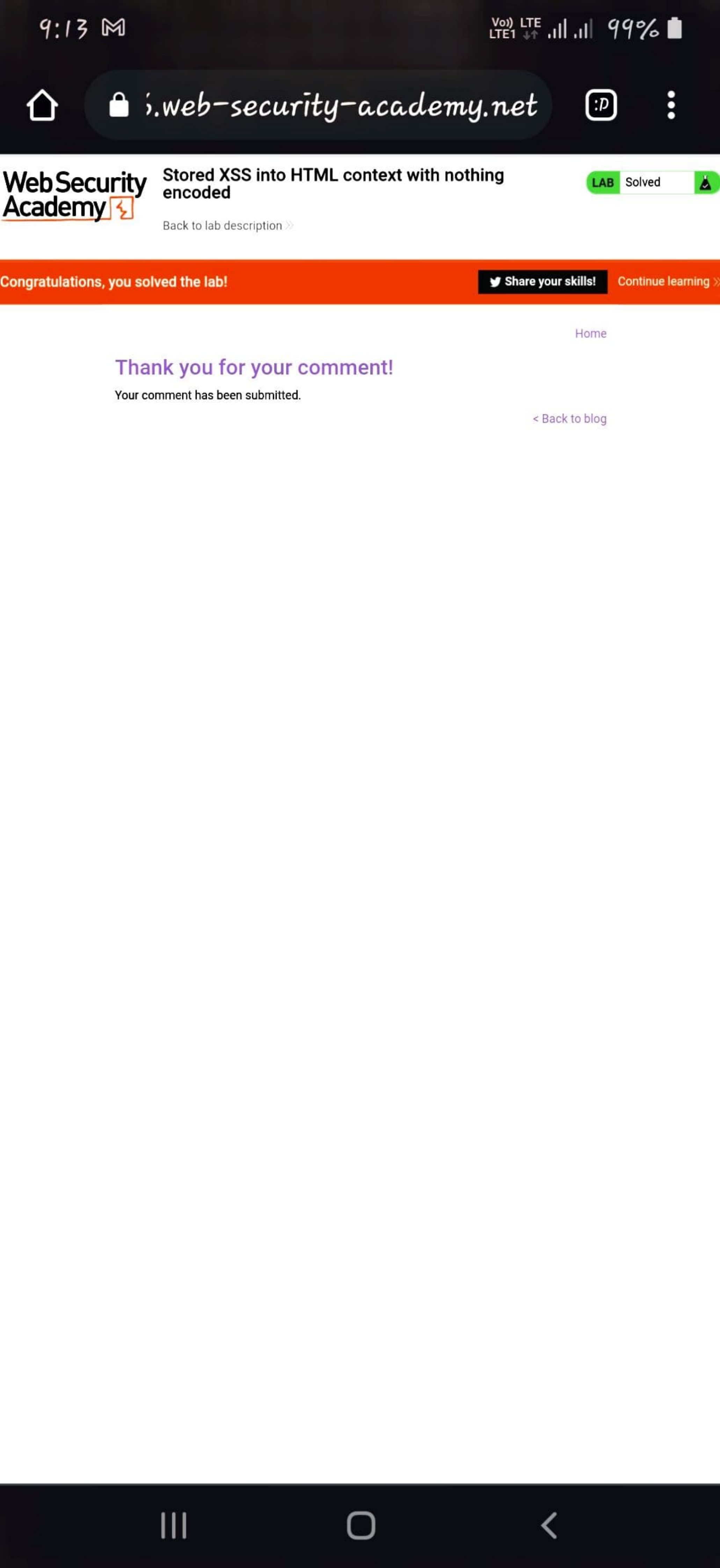
To solve this lab, submit a comment that calls the `alert` function when the blog post is viewed.

Solution

1. Enter the following into the comment box:

   ```
   <script>alert(1)</script>
   ```
2. Enter a name, email and website.
3. Click "Post comment".
4. Go back to the blog.

Community solutions



Stored XSS into HTML context with nothing encoded

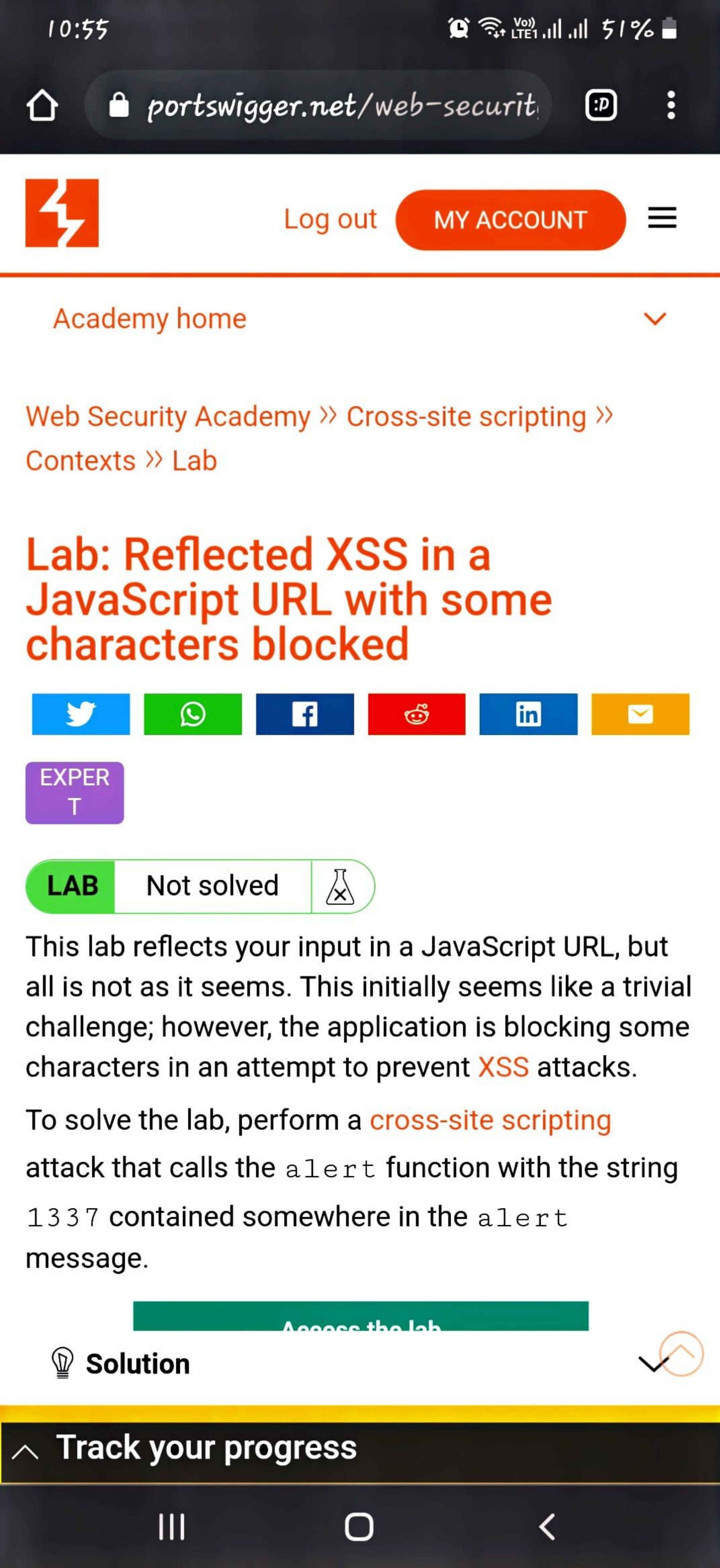
Back to lab description

Congratulations, you solved the lab!

Thank you for your comment!

Your comment has been submitted.

< Back to blog

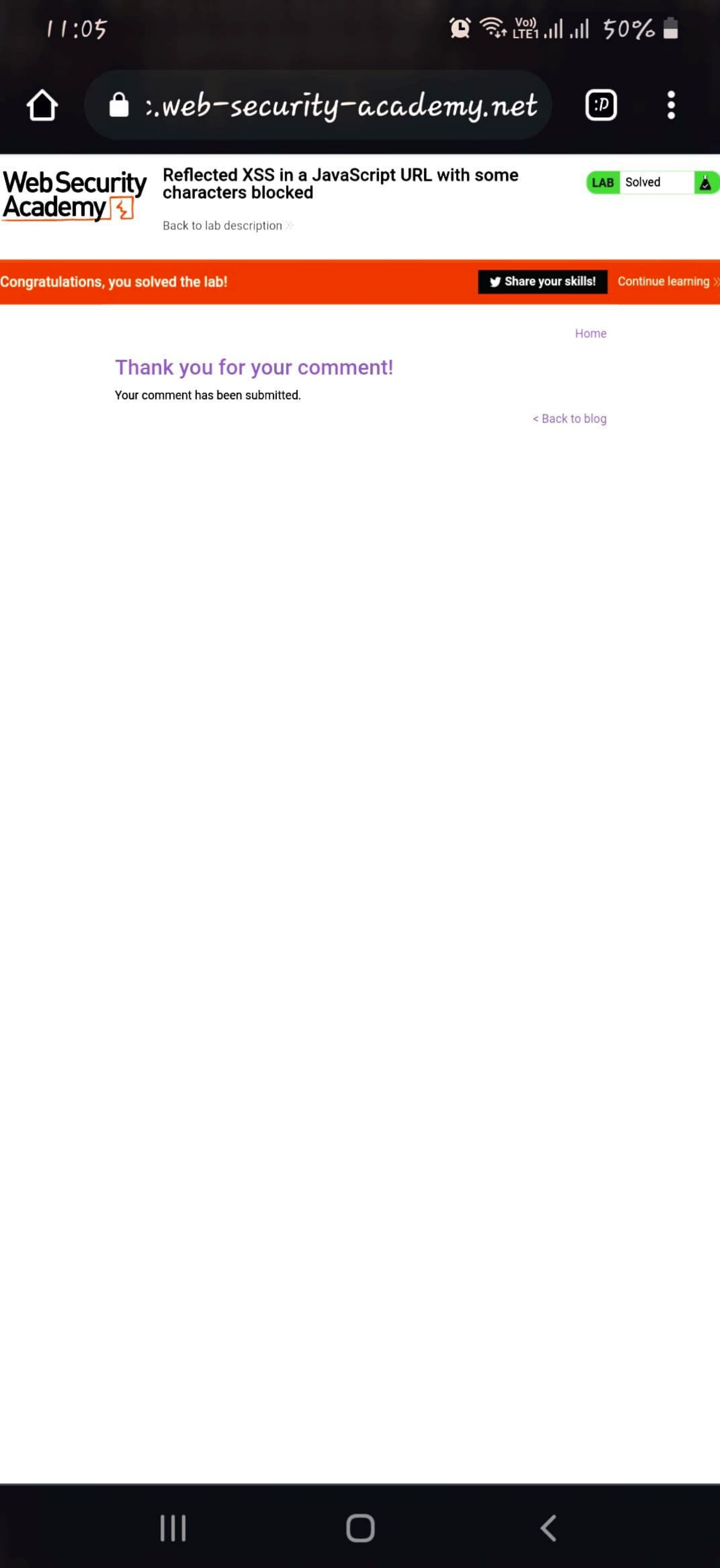


Web Security Academy » Cross-site scripting » Contexts » Lab

Lab: Reflected XSS in a JavaScript URL with some characters blocked

This lab reflects your input in a JavaScript URL, but all is not as it seems. This initially seems like a trivial challenge; however, the application is blocking some characters in an attempt to prevent XSS attacks.

To solve the lab, perform a cross-site scripting attack that calls the `alert` function with the string `1337` contained somewhere in the `alert` message.



Reflected XSS in a JavaScript URL with some characters blocked

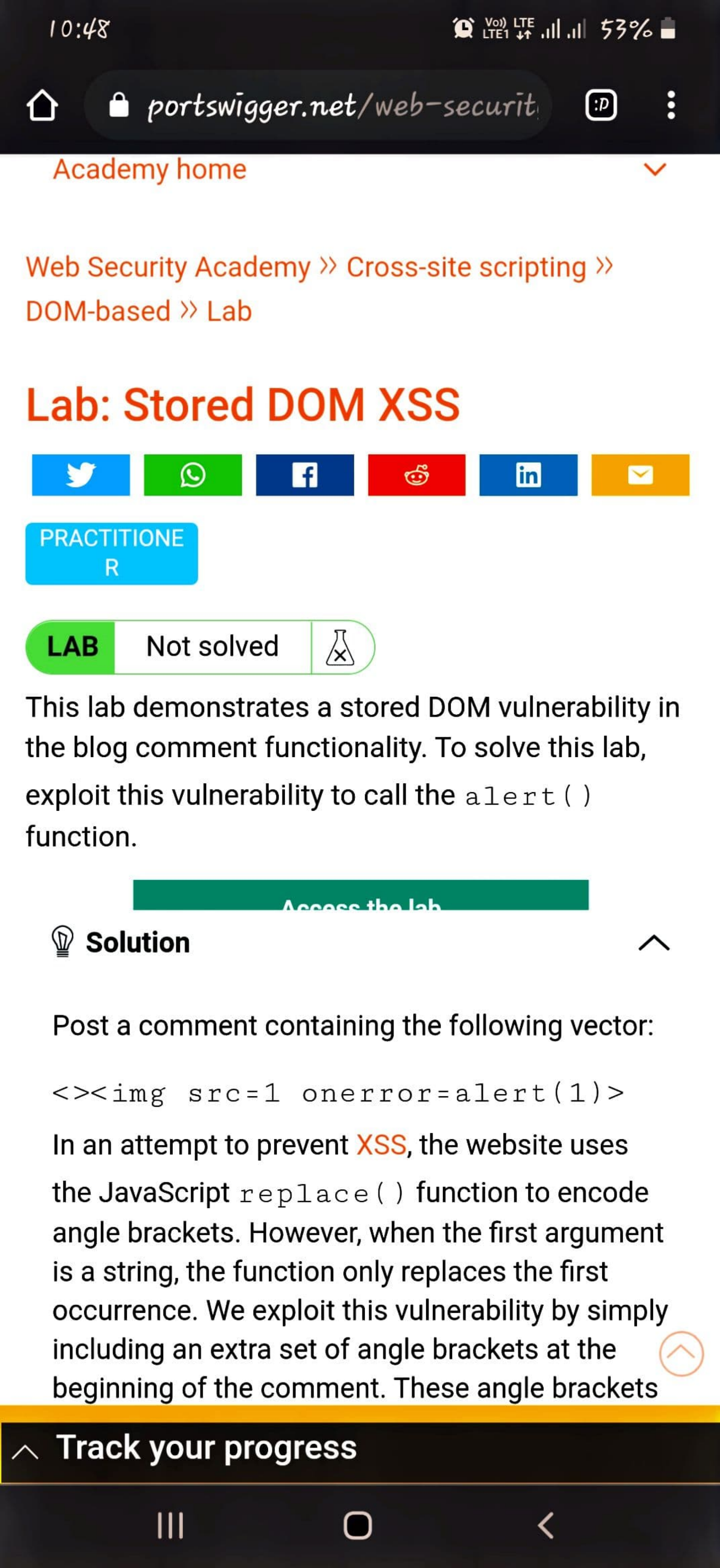
Back to lab description

Congratulations, you solved the lab!

Thank you for your comment!

Your comment has been submitted.

< Back to blog



Academy home

Web Security Academy » Cross-site scripting » DOM-based » Lab

Lab: Stored DOM XSS

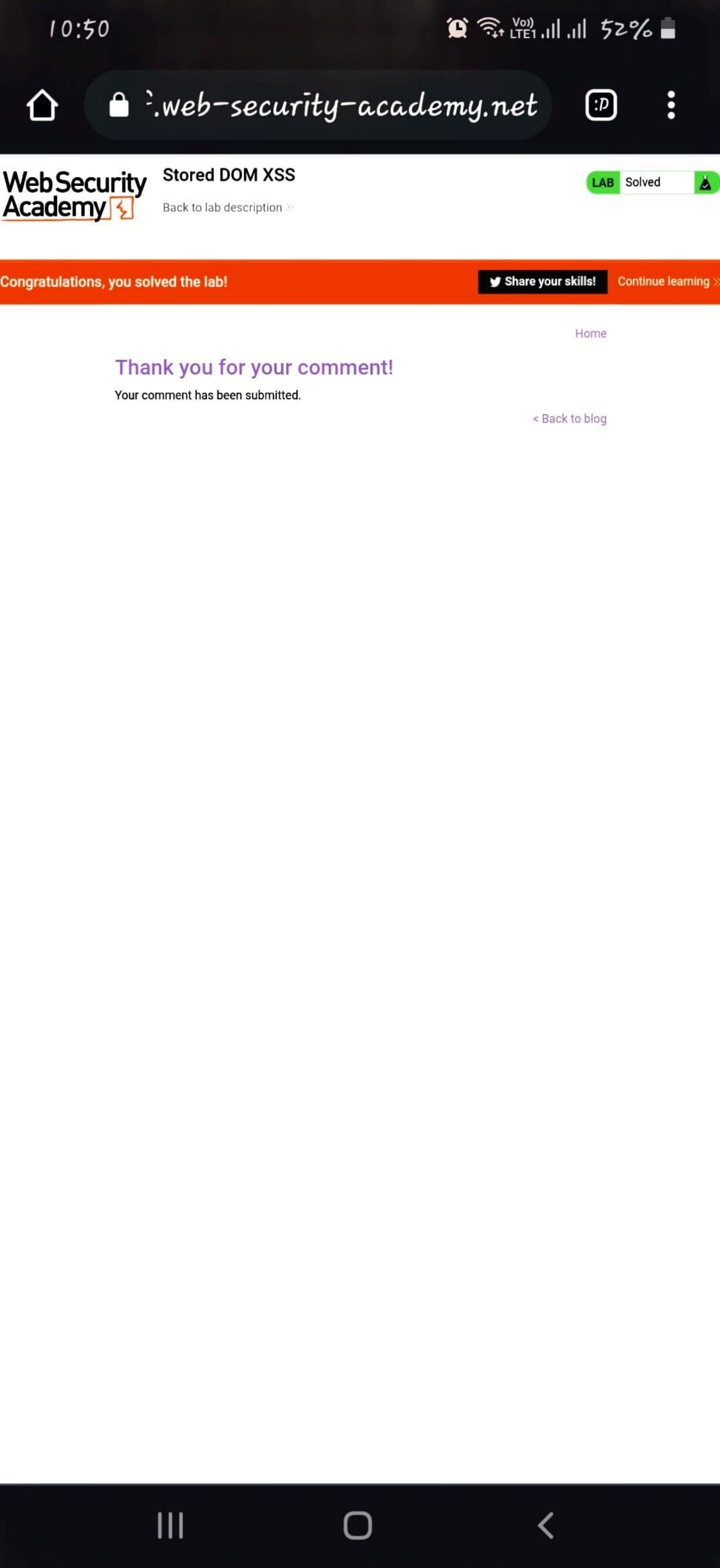
This lab demonstrates a stored DOM vulnerability in the blog comment functionality. To solve this lab, exploit this vulnerability to call the `alert()` function.

Solution

Post a comment containing the following vector:

```
<><img src=1 onerror=alert(1)>
```

In an attempt to prevent XSS, the website uses the JavaScript `replace()` function to encode angle brackets. However, when the first argument is a string, the function only replaces the first occurrence. We exploit this vulnerability by simply including an extra set of angle brackets at the beginning of the comment. These angle brackets



Stored DOM XSS

Back to lab description

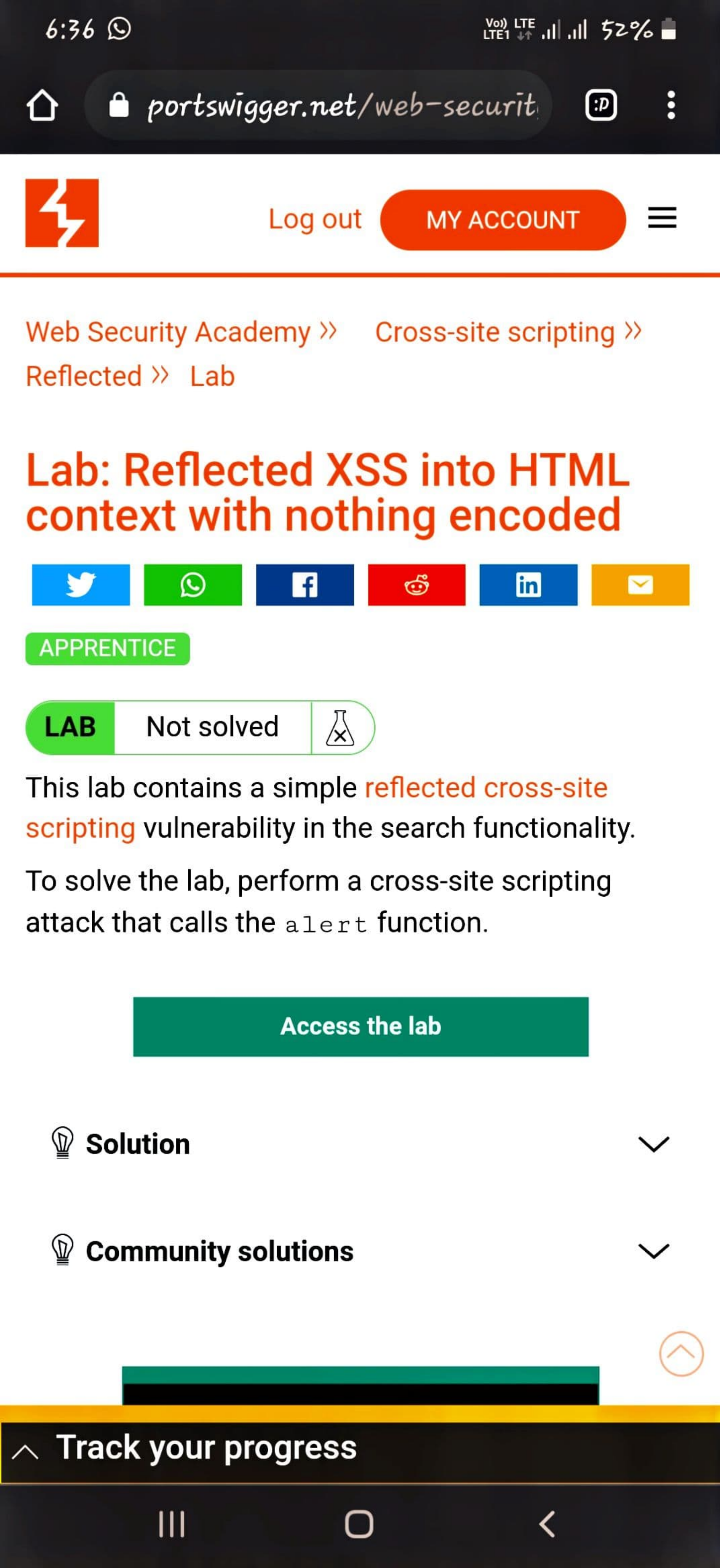
Congratulations, you solved the lab!

Home

Thank you for your comment!

Your comment has been submitted.

< Back to blog



6:36

portswigger.net/web-securit

Log out MY ACCOUNT

Web Security Academy » Cross-site scripting » Reflected » Lab

Lab: Reflected XSS into HTML context with nothing encoded

APPRENTICE

LAB Not solved

This lab contains a simple reflected cross-site scripting vulnerability in the search functionality.

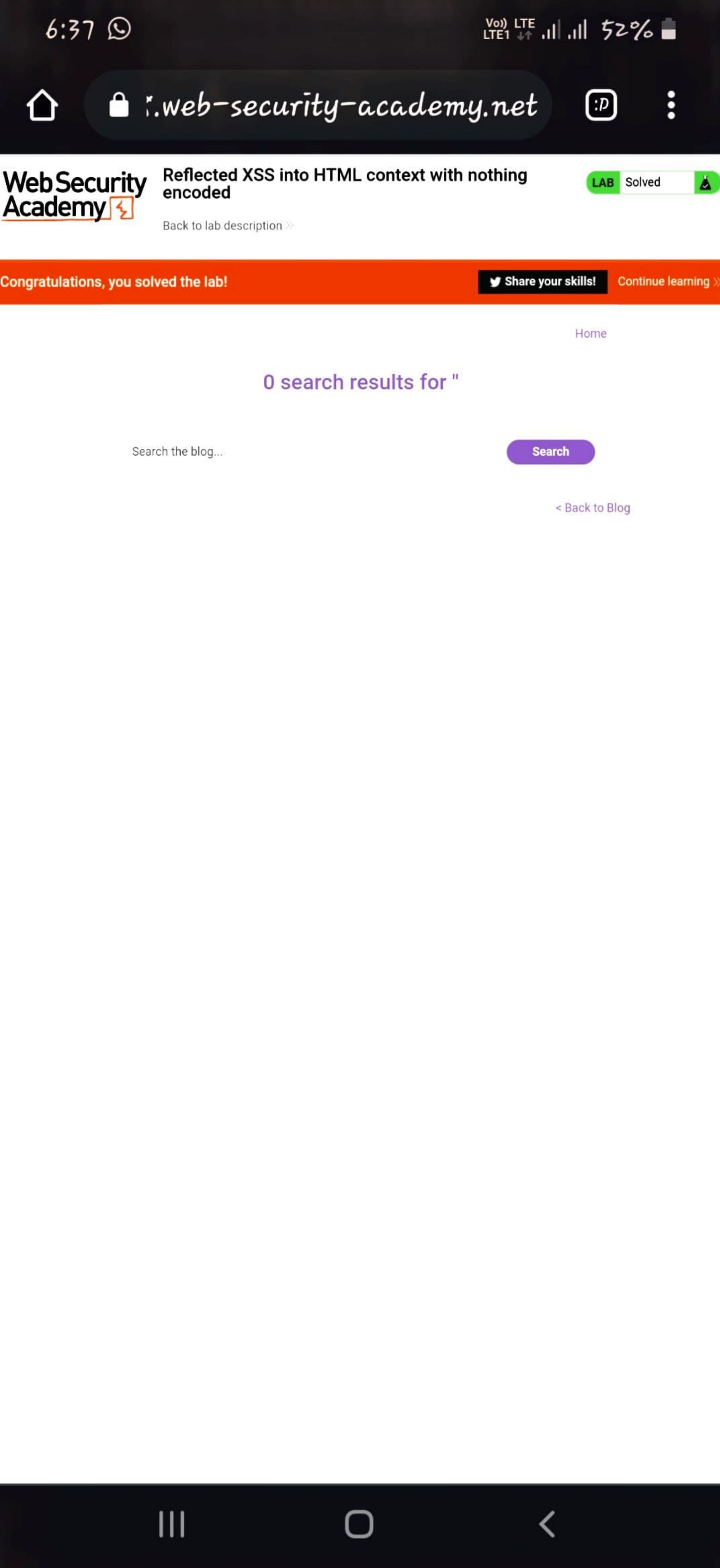
To solve the lab, perform a cross-site scripting attack that calls the `alert` function.

Access the lab

Solution

Community solutions

Track your progress



WebSecurity Academy

Reflected XSS into HTML context with nothing encoded

LAB Solved

Back to lab description »

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Home

0 search results for ''

Search the blog...

Search

< Back to Blog