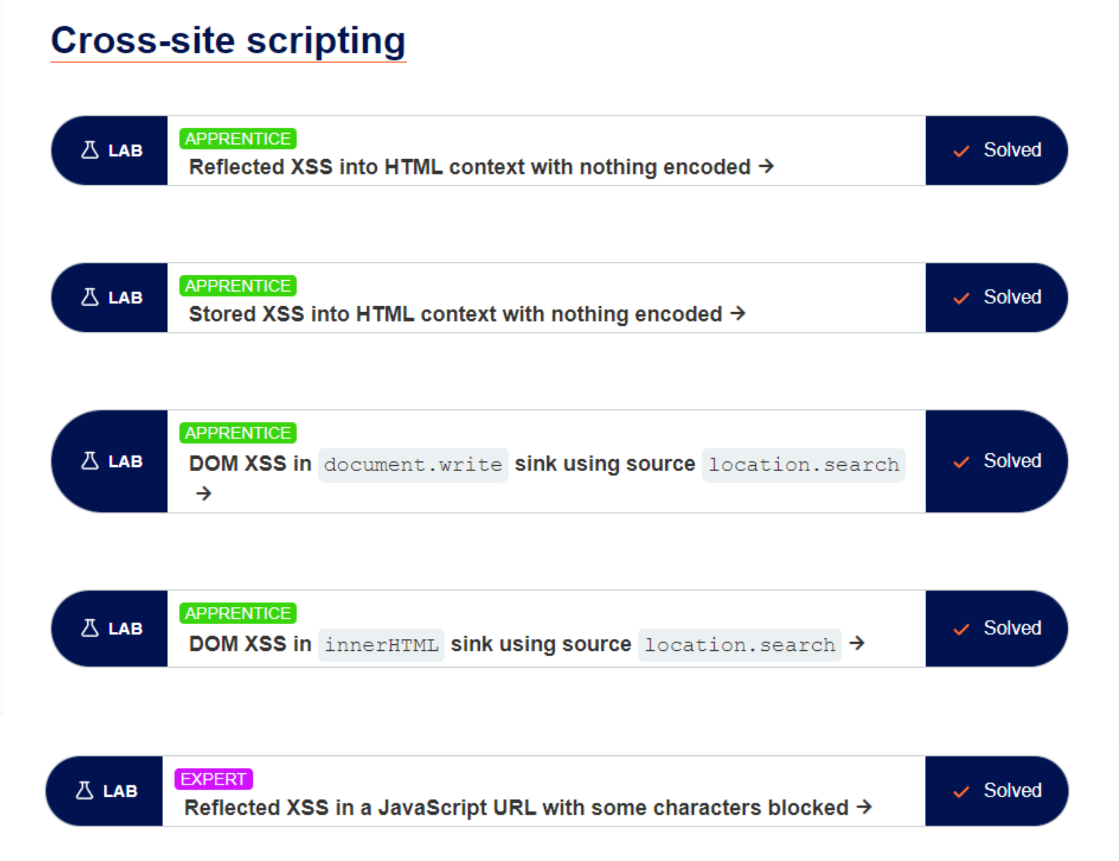
Solved Cross-site scripting Labs



Cross-site scripting

LAB | APPRENTICE Reflected XSS into HTML context with nothing encoded → | ✓ Solved

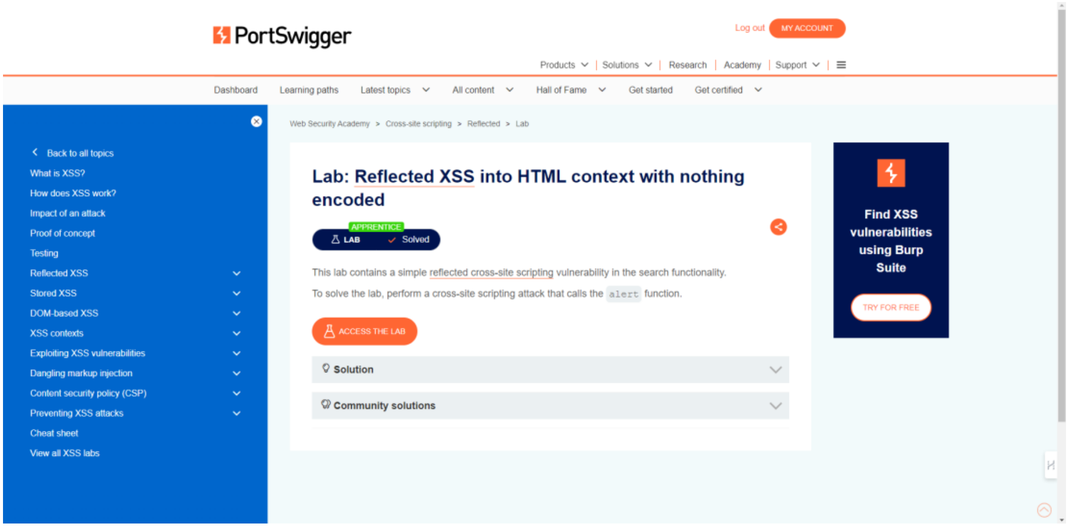
LAB | APPRENTICE Stored XSS into HTML context with nothing encoded → | ✓ Solved

LAB | APPRENTICE DOM XSS in `document.write` sink using source `location.search` → | ✓ Solved

LAB | APPRENTICE DOM XSS in `innerHTML` sink using source `location.search` → | ✓ Solved

LAB | EXPERT Reflected XSS in a JavaScript URL with some characters blocked → | ✓ Solved

1. Lab: Reflected XSS into HTML context with nothing encoded



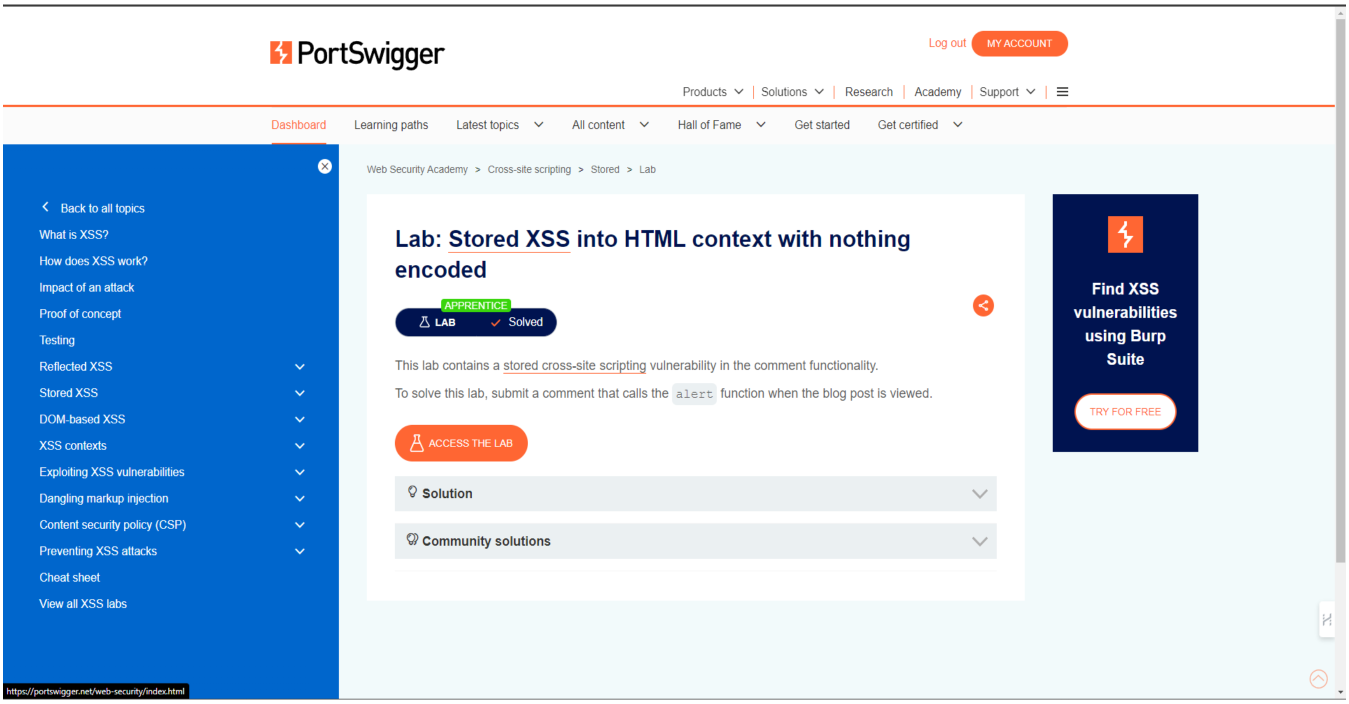
Lab: Reflected XSS into HTML context with nothing encoded

APPRENTICE LAB ✓ 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.

2. Lab: Stored XSS into HTML context with nothing encode



Lab: Stored XSS into HTML context with nothing encoded

APPRENTICE LAB ✓ Solved

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

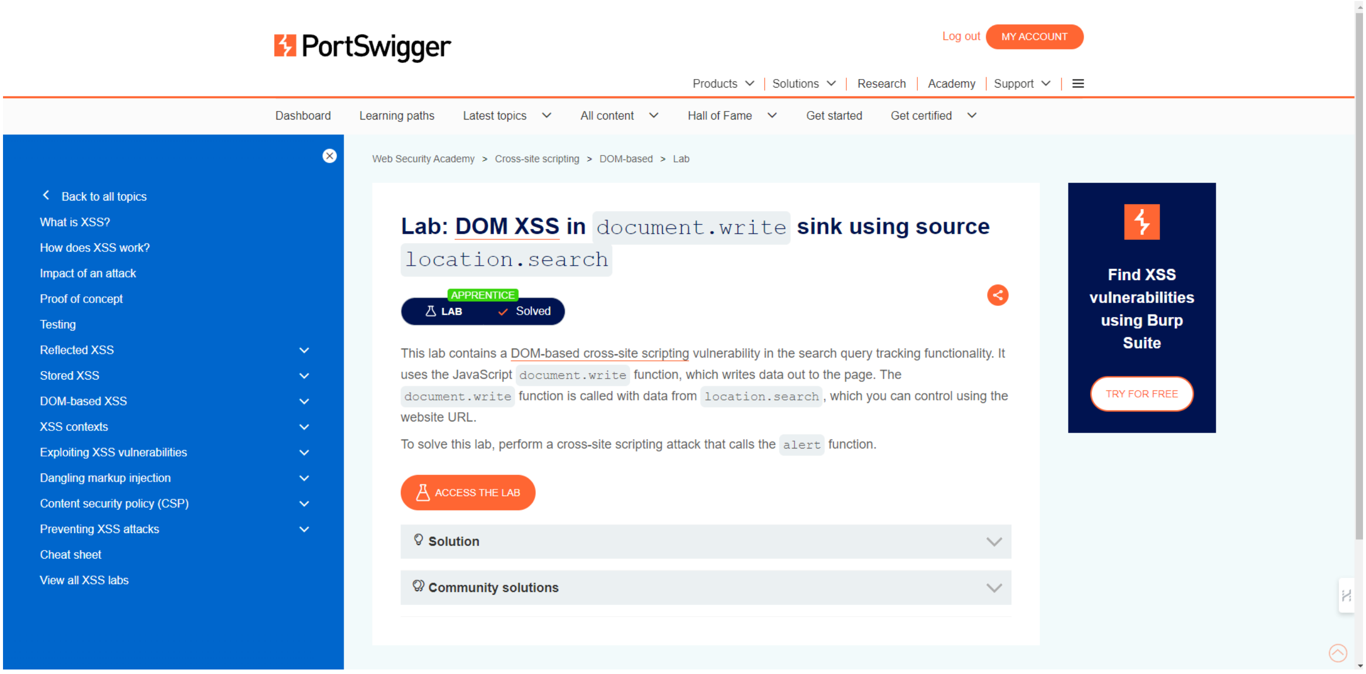
To solve this lab, submit a comment that calls the `alert` function when the blog post is viewed.

ACCESS THE LAB

Solution

Community solutions

3. Lab: DOM XSS in `document.write` sink using source `location.search`



Lab: DOM XSS in `document.write` sink using source `location.search`

APPRENTICE LAB ✓ Solved

This lab contains a DOM-based cross-site scripting vulnerability in the search query tracking functionality. It uses the JavaScript `document.write` function, which writes data out to the page. The `document.write` function is called with data from `location.search`, which you can control using the website URL.

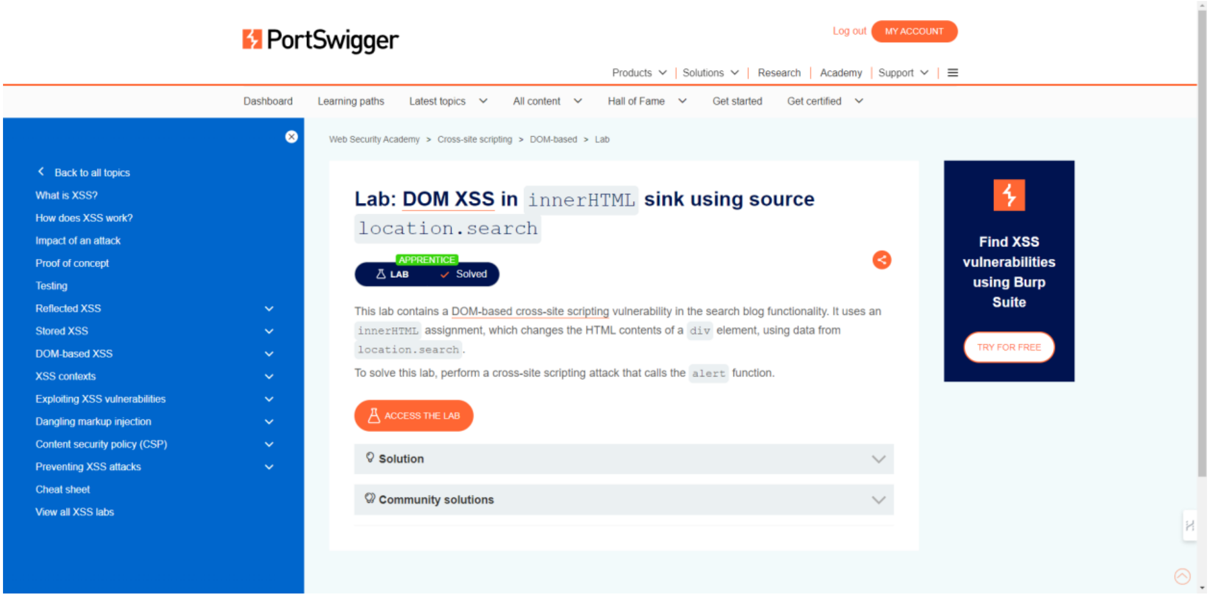
To solve this lab, perform a cross-site scripting attack that calls the `alert` function.

ACCESS THE LAB

Solution

Community solutions

4. Lab: DOM XSS in `innerHTML` sink using source `location.search`

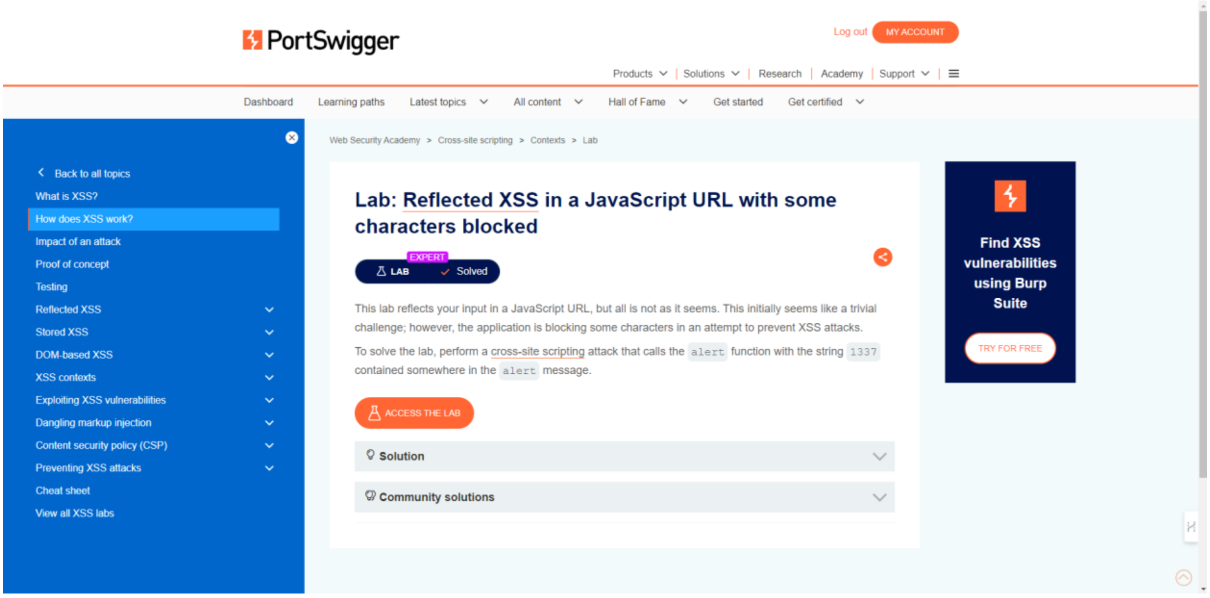


Lab: DOM XSS in `innerHTML` sink using source `location.search`

This lab contains a DOM-based cross-site scripting vulnerability in the search blog functionality. It uses an `innerHTML` assignment, which changes the HTML contents of a `div` element, using data from `location.search`.

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

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



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.