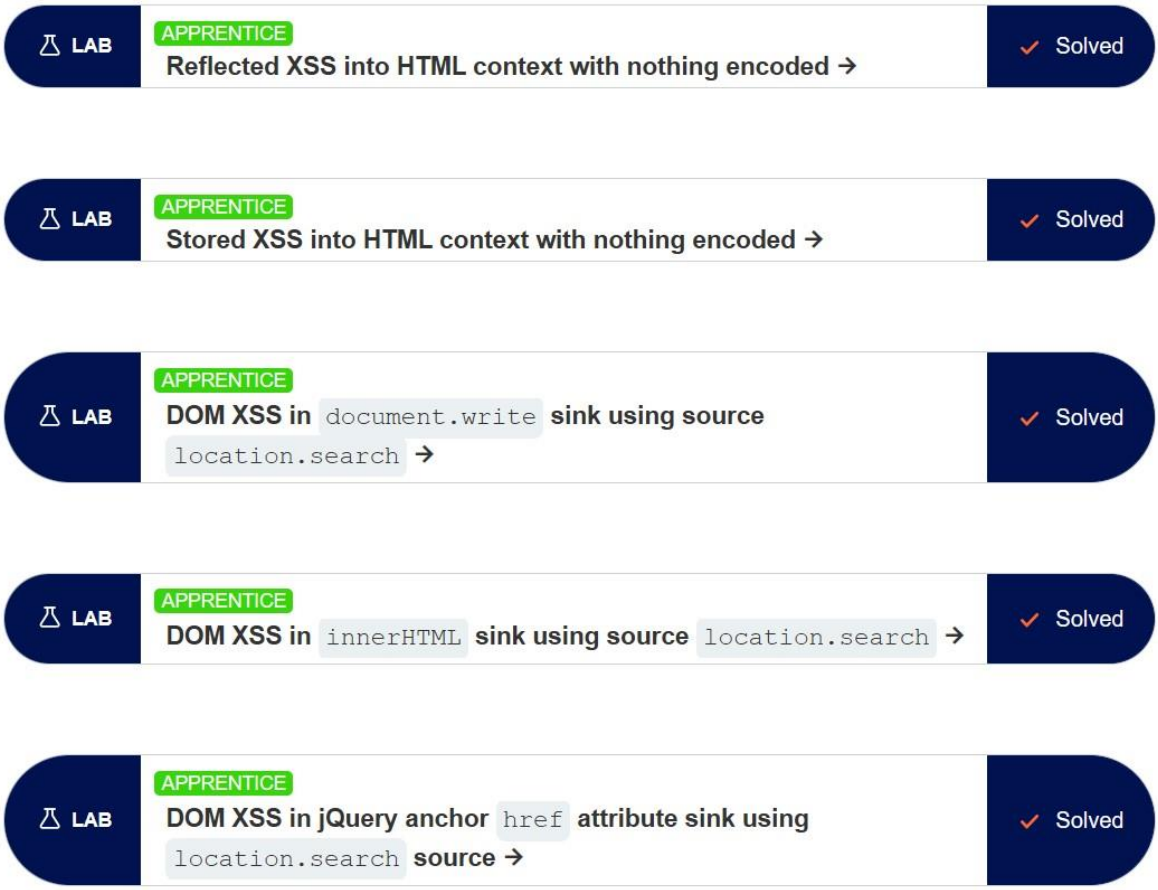
TASK -1

To find vulnerabilities in postswigger labs


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
APPRENTICE
DOM XSS in jQuery anchor href attribute sink using location.search source →
Solved

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.

ACCESS THE LAB

Solution

Community solutions

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

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

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

APPRENTICE

LAB ✓ Solved

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.

ACCESS THE LAB

Solution

Community solutions

Lab: DOM XSS in jQuery anchor `href` attribute sink using `location.search` source

APPRENTICE

LAB ✓ Solved

This lab contains a DOM-based cross-site scripting vulnerability in the submit feedback page. It uses the jQuery library's `$` selector function to find an anchor element, and changes its `href` attribute using data from `location.search`.

To solve this lab, make the "back" link alert `document.cookie`.

ACCESS THE LAB

Solution

Community solutions