


Task 1


All 5 Screenshots of portswigger task.

Cross-site scripting


LAB Reflected XSS into HTML context with nothing encoded »

 Solved

LAB Reflected XSS into HTML context with most tags and attributes blocked »

 Solved

LAB Reflected XSS into HTML context with all tags blocked except custom ones »

 Solved

LAB Reflected XSS into attribute with angle brackets HTML-encoded »

 Solved

LAB Stored XSS into HTML context with nothing encoded »

 Solved

Lab :1

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



Track your progress

Learning materials: [View all](#)

0%

Vulnerability labs: [View all](#)

2%

Level progress:

3 of 47

2 of 123

0 of 27

Apprentice Practitioner Expert

Your level:

Ne

NEWBIE

Solve 44 more labs to become an apprentice.

Lab 2:

Lab: Reflected XSS into HTML context with most tags and attributes blocked

PRACTITIONER

LAB Solved

This lab contains a **reflected XSS** vulnerability in the search functionality but uses a web application firewall (WAF) to protect against common XSS vectors.

To solve the lab, perform a **cross-site scripting** attack that bypasses the WAF and calls the `print()` function.

Note

Your solution must not require any user interaction. Manually causing `print()` to be called in your own browser will not solve the lab.

Access the lab

Solution

Community solutions



Lab 3:

Lab: Reflected XSS into HTML context with all tags blocked except custom ones



PRACTITIONER

LAB


Solved




This lab blocks all HTML tags except custom ones.

To solve the lab, perform a **cross-site scripting** attack that injects a custom tag and automatically alerts `document.cookie`.

Access the lab

 Solution



 Community solutions



Lab 4:

Lab: Reflected XSS into attribute with angle brackets HTML-encoded



APPRENTICE


LAB

Solved




This lab contains a **reflected cross-site scripting** vulnerability in the search blog functionality where angle brackets are HTML-encoded. To solve this lab, perform a cross-site scripting attack that injects an attribute and calls the `alert` function.

Access the lab

 Solution



 Community solutions



Lab 5:

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

