

## PROBLEM\_STATEMENT

## TASK-1:

Task 1: In Session 22 we introduced you to portswigger labs. Portswigger is a website which has so many vulnerable labs which helps you to learn about other vulnerabilities in real life. You can visit Portswigger labs at <https://portswigger.net/> So the exact task for you now is there are several XSS labs on this website <https://portswigger.net/web-security/all-labs>. You can just choose any 5 of them and solve it. We are leaving the choice up to you. Every lab on the website has a hint section which you can use to solve the labs if you are stuck somewhere. Watch me solve one lab to give you a demo. After solving you should see something like “Solved Status” on the top of the lab. That status is necessary to pass the task out. If you need any more help solving labs, you can use Google to find out a solution video available on Youtube.

## SOLUTION:

The screenshot displays the PortSwigger website interface. The browser's address bar shows the URL: <https://portswigger.net/web-security/cross-site-scripting/contexts/lab-javascript-string-angle-brackets-html-encoded>. The PortSwigger logo is at the top left, with navigation links for Products, Solutions, Research, Academy, Daily Swig, and Support. The main content area features the lab title "Lab: Reflected XSS into a JavaScript string with angle brackets HTML encoded" in orange. Below the title, it indicates the lab is "Solved" and "APPRENTICE" level. A description states: "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." A green button labeled "Access the lab" is visible. A "Solution" dropdown menu is open at the bottom. On the right, a "Track your progress" sidebar shows learning materials at 0%, vulnerability labs at 3%, and level progress for Apprentice (3 of 47), Practitioner (2 of 123), and Expert (1 of 27). The Windows taskbar at the bottom shows the time as 17:53 on 09-07-2021.

# PROJECT\_SUBBMISSION \_INTERNSHIP\_STUDIO

Lab: Reflected XSS in canonical

https://portswigger.net/web-security/cross-site-scripting/contexts/lab-canonical-link-tag

Apps Gmail YouTube Maps Inheritance in Java... Two vessels contain... DTW2 - Google Drive CoSpaces Edu: Mak... Vulforia Developer... Freshmen Engineer... Java StringBuilder c... Reading list

PortSwigger

Log out MY ACCOUNT

Products Solutions Research Academy Daily Swig Support

Academy Home Learning Path Latest Topics All Labs Hall of Fame Getting Started Guide

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

Lab: Reflected XSS in canonical link tag

PRACTITIONER

LAB Solved

This lab reflects user input in a canonical link tag and escapes angle brackets.

To solve the lab, perform a **cross-site scripting** attack on the home page that injects an attribute that calls the `alert` function.

To assist with your exploit, you can assume that the simulated user will press the following key combinations:

- ALT+SHIFT+X
- CTRL+ALT+X
- Alt+X

Please note that the intended solution to this lab is only possible in Chrome.

Track your progress

Learning materials: 0% [View all](#)

Vulnerability labs: 3% [View all](#)

Level progress:

3 of 47

2 of 123

1 of 27

Apprentice Practitioner Expert

Type here to search

Lab: Reflected XSS into attribute

https://portswigger.net/web-security/cross-site-scripting/contexts/lab-attribute-angle-brackets-html-encoded

Apps Gmail YouTube Maps Inheritance in Java... Two vessels contain... DTW2 - Google Drive CoSpaces Edu: Mak... Vulforia Developer... Freshmen Engineer... Java StringBuilder c... Reading list

PortSwigger

Log out MY ACCOUNT

Products Solutions Research Academy Daily Swig Support

Academy Home Learning Path Latest Topics All Labs Hall of Fame Getting Started Guide

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

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

Track your progress

Learning materials: 0% [View all](#)

Vulnerability labs: 3% [View all](#)

Level progress:

3 of 47

2 of 123

1 of 27

Apprentice Practitioner Expert

Type here to search

# PROJECT\_SUBBMISSION \_INTERNSHIP\_STUDIO

Lab: Reflected XSS with event han...

https://portswigger.net/web-security/cross-site-scripting/contexts/lab-event-handlers-and-href-attributes-blocked

Apps Gmail YouTube Maps OG Inheritance in Java... Two vessels contain... DTW2 - Google Drive CoSpaces Edu: Mak... Vuloria Developer... Freshmen Engineer... Java StringBuilder c... Reading list

PortSwigger

Log out MY ACCOUNT

Products Solutions Research Academy Daily Swig Support

Academy Home Learning Path Latest Topics All Labs Hall of Fame Getting Started Guide

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

Lab: Reflected XSS with event handlers and href attributes blocked

EXPERT

LAB Solved

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>`

Access the lab

Track your progress

Learning materials: View all 0%

Vulnerability labs: View all 3%

Level progress:

3 of 47 Apprentice 2 of 123 Practitioner 1 of 27 Expert

Type here to search

Lab: Reflected XSS into HTML con...

https://portswigger.net/web-security/cross-site-scripting/contexts/lab-html-context-with-all-standard-tags-blocked

Apps Gmail YouTube Maps OG Inheritance in Java... Two vessels contain... DTW2 - Google Drive CoSpaces Edu: Mak... Vuloria Developer... Freshmen Engineer... Java StringBuilder c... Reading list

PortSwigger

Log out MY ACCOUNT

Products Solutions Research Academy Daily Swig Support

Academy Home Learning Path Latest Topics All Labs Hall of Fame Getting Started Guide

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

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

Track your progress

Learning materials: View all 0%

Vulnerability labs: View all 3%

Level progress:

3 of 47 Apprentice 2 of 123 Practitioner 1 of 27 Expert

Type here to search

# PROJECT\_SUBBMISSION \_INTERNSHIP\_STUDIO

The screenshot shows the PortSwigger Web Security Academy interface. The browser's address bar displays the URL: `https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded`. The PortSwigger logo is in the top left, with 'Log out' and 'MY ACCOUNT' links in the top right. A navigation menu includes 'Products', 'Solutions', 'Research', 'Academy', 'Daily Swig', and 'Support'. Below this, a secondary menu lists 'Academy Home', 'Learning Path', 'Latest Topics', 'All Labs', 'Hall of Fame', and 'Getting Started Guide'.

The main content area is titled 'Lab: Reflected XSS into HTML context with nothing encoded'. It is categorized under 'Web Security Academy » Cross-site scripting » Reflected » Lab'. The lab is marked as 'Solved' and is part of the 'APPRENTICE' level. A description states: '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.' A green 'Access the lab' button is visible.

On the right side, a 'Track your progress' sidebar shows: 'Learning materials: 0%' (with a 'View all' button), 'Vulnerability labs: 3%' (with a 'View all' button), and 'Level progress' for three levels: 'Apprentice' (3 of 47), 'Practitioner' (2 of 123), and 'Expert' (1 of 27).

The bottom of the image shows a Windows taskbar with the search bar and various application icons. The system clock in the bottom right corner indicates the time is 17:54 on 09-07-2021.