

INTERNSHIP STUDIO PROJECT SUBMISSION

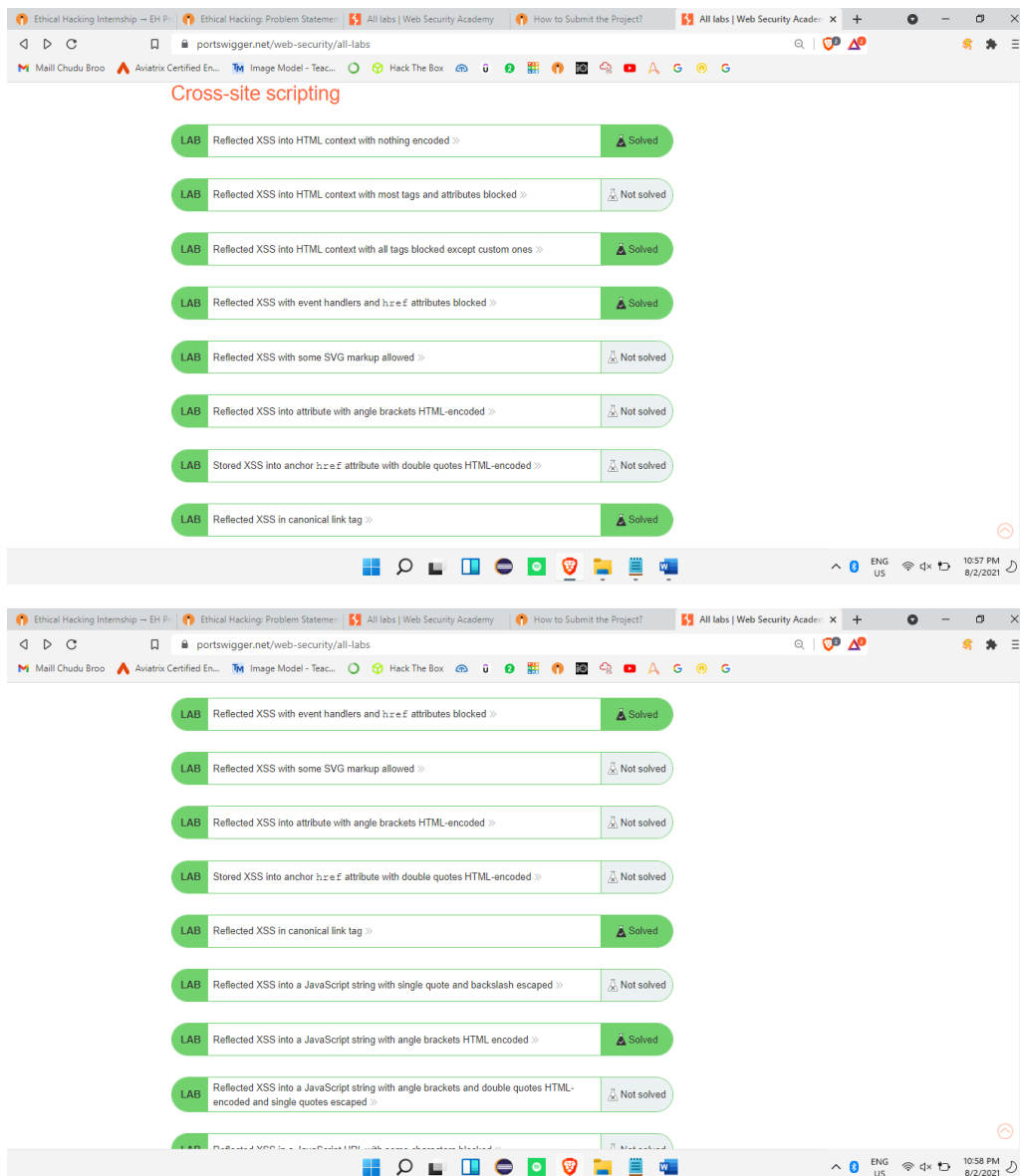
Problem Statement

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

---As told in the task-1

The following labs were done in the portswigger labs.



INTERNSHIP STUDIO PROJECT SUBMISSION

Lab: Reflected XSS into HTML context with nothing encoded

The screenshot shows the PortSwigger Web Security Academy interface. The browser's address bar displays the URL: `portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded`. The page title is "Lab: Reflected XSS into HTML context with nothing encoded". The lab is categorized as "APPRENTICE" and "LAB Solved". The 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 button labeled "Access the lab" is visible. On the right, a "Track your progress" sidebar shows learning materials at 0%, vulnerability labs at 2%, and level progress for Apprentice (2 of 47), Practitioner (2 of 123), and Expert (1 of 27). The user's level is "NEWBIE". The bottom of the page shows the Windows taskbar with various application icons and the system clock indicating 10:59 PM on 8/2/2021.

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

The screenshot shows the PortSwigger Web Security Academy interface for a different lab. The browser's address bar displays the URL: `portswigger.net/web-security/cross-site-scripting/contexts/lab-html-context-with-all-standard-tags-blocked`. The page title is "Lab: Reflected XSS into HTML context with all tags blocked except custom ones". The lab is categorized as "PRACTITIONER" and "LAB Solved". The description states: "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`." A green button labeled "Access the lab" is visible. On the right, a "Track your progress" sidebar shows learning materials at 0%, vulnerability labs at 2%, and level progress for Apprentice (2 of 47), Practitioner (2 of 123), and Expert (1 of 27). The user's level is "NEWBIE". The bottom of the page shows the Windows taskbar with various application icons and the system clock indicating 10:59 PM on 8/2/2021.

Lab: Reflected XSS with event handlers and href attributes blocked

Ethical Hacking Internship -> Ethical Hacking Problem Solving | All labs | Web Security Academy | How to Submit the Project? | All labs | Web Security Academy | Lab: Reflected XSS with event handlers and href attributes blocked

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

Mail Chudu BrooAvatrix Certified En...Image Model - Teac...Hack The Box

PortSwigger

Log outMY ACCOUNT

ProductsSolutionsResearchAcademyDaily SwigSupport

Academy HomeLearning PathLatest TopicsAll LabsHall of FameGetting Started GuideGet Certified

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

Lab: Reflected XSS with event handlers and href attributes blocked

EXPERTLAB 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: Click me

Access the lab

Solution

Track your progress

Learning materials: 0% View all

Vulnerability labs: 2% View all

Level progress:

2 of 47 Apprentice2 of 123 Practitioner1 of 27 Expert

Your level: NEWBIE

Lab: Reflected XSS in canonical link tag

The screenshot displays the PortSwigger Web Security Academy interface. At the top, there's a navigation bar with links for Products, Solutions, Research, Academy, Daily Swig, and Support. Below this is a breadcrumb trail: Web Security Academy » Cross-site scripting » Contexts » Lab. The main heading is 'Lab: Reflected XSS in canonical link tag'. To the left of the heading is a 'PRACTITIONER' badge, and below it is a 'LAB Solved' indicator. The lab description states: '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, and Alt+X. Please note that the intended solution to this lab is only possible in Chrome.' A green button labeled 'Access the lab' is at the bottom. On the right, a sidebar titled 'Track your progress' shows learning materials (0%), vulnerability labs (2%), and level progress (2 of 47 for Apprentice, 2 of 123 for Practitioner, 1 of 27 for Expert). The bottom of the page shows a Windows taskbar with various icons and the system clock.

INTERNSHIP STUDIO PROJECT SUBMISSION

Lab: Reflected XSS into a JavaScript string with angle brackets HTML encoded

The screenshot shows the PortSwigger web security academy interface. The browser's address bar displays the URL: `portswigger.net/web-security/cross-site-scripting/contexts/lab-javascript-string-angle-brackets-html-encoded`. The PortSwigger logo is at the top left, with a 'Log out' button and a 'MY ACCOUNT' button at the top right. A navigation menu includes 'Products', 'Solutions', 'Research', 'Academy', 'Daily Swig', and 'Support'. Below this, a sub-menu shows 'Academy Home', 'Learning Path', 'Latest Topics', 'All Labs', 'Hall of Fame', 'Getting Started Guide', and 'Get Certified'. The main content area is titled 'Web Security Academy >> Cross-site scripting >> Contexts >> Lab'. The lab title is 'Lab: Reflected XSS into a JavaScript string with angle brackets HTML encoded'. It is categorized as 'APPRENTICE' and 'LAB' and is marked as 'Solved'. The 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.' There is an 'Access the lab' button. Below the description are sections for 'Solution' and 'Community solutions'. On the right, a 'Track your progress' sidebar shows 'Learning materials: 0%', 'Vulnerability labs: 2%', and 'Level progress: 2 of 47 for Apprentice, 2 of 123 for Practitioner, 1 of 27 for Expert'. The user's level is 'NEWBIE'. The Windows taskbar at the bottom shows the time as 11:03 PM on 8/2/2021.

In the task-1 we had did the labs on XSS. Using portswigger .