INTERNSHIP STUDIO
PROJECT SUBMISSION

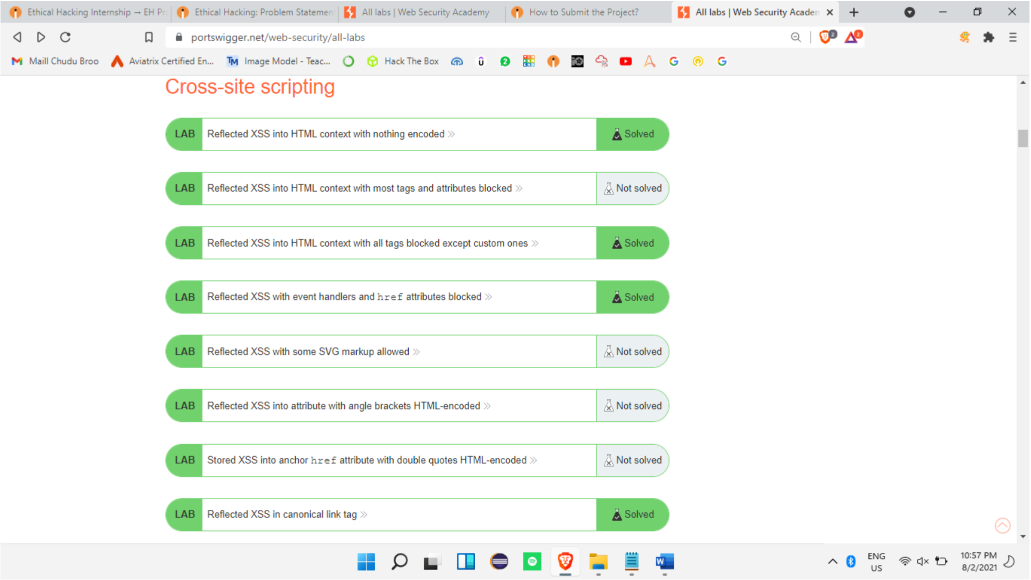
Problem Statement

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

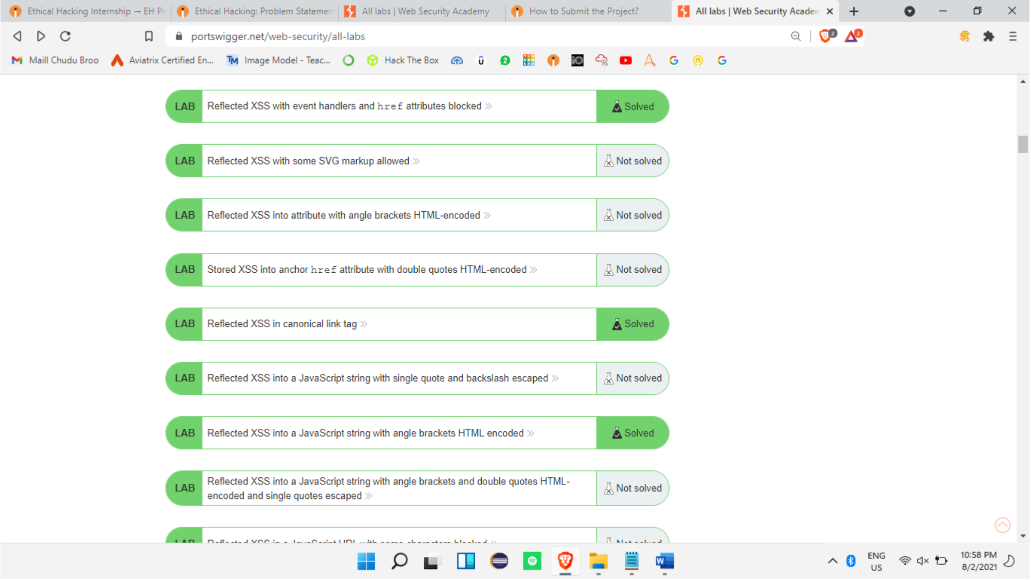
---As told in the task-1

The following labs were done in the portswigger labs.


Ethical Hacking Internship – EH P
Ethical Hacking: Problem Statemen
All labs | Web Security Academy
How to Submit the Project?
All labs | Web Security Academ
portswigger.net/web-security/all-labs
Maill Chudu Broo
Aviatrix Certified En...
Image Model - Teac...
Hack The Box
ENG US
10:57 PM
8/2/2021

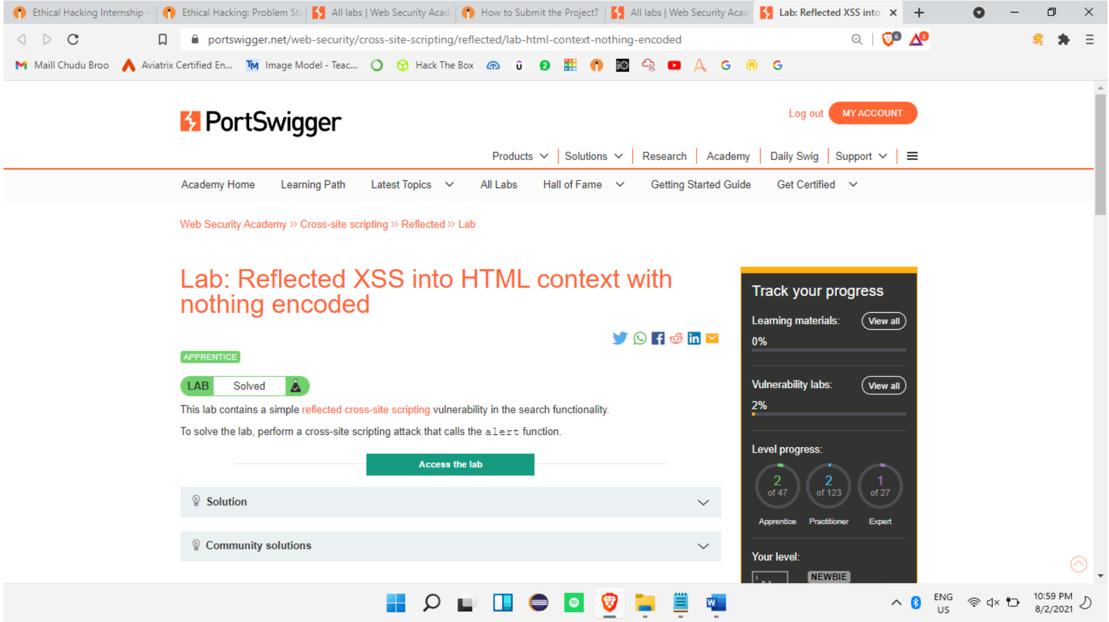
Cross-site scripting

LAB	Reflected XSS into HTML context with nothing encoded »	Solved
LAB	Reflected XSS into HTML context with most tags and attributes blocked »	Not solved
LAB	Reflected XSS into HTML context with all tags blocked except custom ones »	Solved
LAB	Reflected XSS with event handlers and `href` attributes blocked »	Solved
LAB	Reflected XSS with some SVG markup allowed »	Not solved
LAB	Reflected XSS into attribute with angle brackets HTML-encoded »	Not solved
LAB	Stored XSS into anchor `href` attribute with double quotes HTML-encoded »	Not solved
LAB	Reflected XSS in canonical link tag »	Solved


Ethical Hacking Internship – EH P
Ethical Hacking: Problem Statemen
All labs | Web Security Academy
How to Submit the Project?
All labs | Web Security Academ
portswigger.net/web-security/all-labs
Maill Chudu Broo
Aviatrix Certified En...
Image Model - Teac...
Hack The Box
ENG US
10:58 PM
8/2/2021

LAB	Reflected XSS with event handlers and `href` attributes blocked »	Solved
LAB	Reflected XSS with some SVG markup allowed »	Not solved
LAB	Reflected XSS into attribute with angle brackets HTML-encoded »	Not solved
LAB	Stored XSS into anchor `href` attribute with double quotes HTML-encoded »	Not solved
LAB	Reflected XSS in canonical link tag »	Solved
LAB	Reflected XSS into a JavaScript string with single quote and backslash escaped »	Not solved
LAB	Reflected XSS into a JavaScript string with angle brackets HTML encoded »	Solved
LAB	Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped »	Not solved
LAB	Reflected XSS in a JavaScript URL with some characters blocked	Not solved

Lab: Reflected XSS into HTML context with nothing encoded



portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded

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

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.

Track your progress

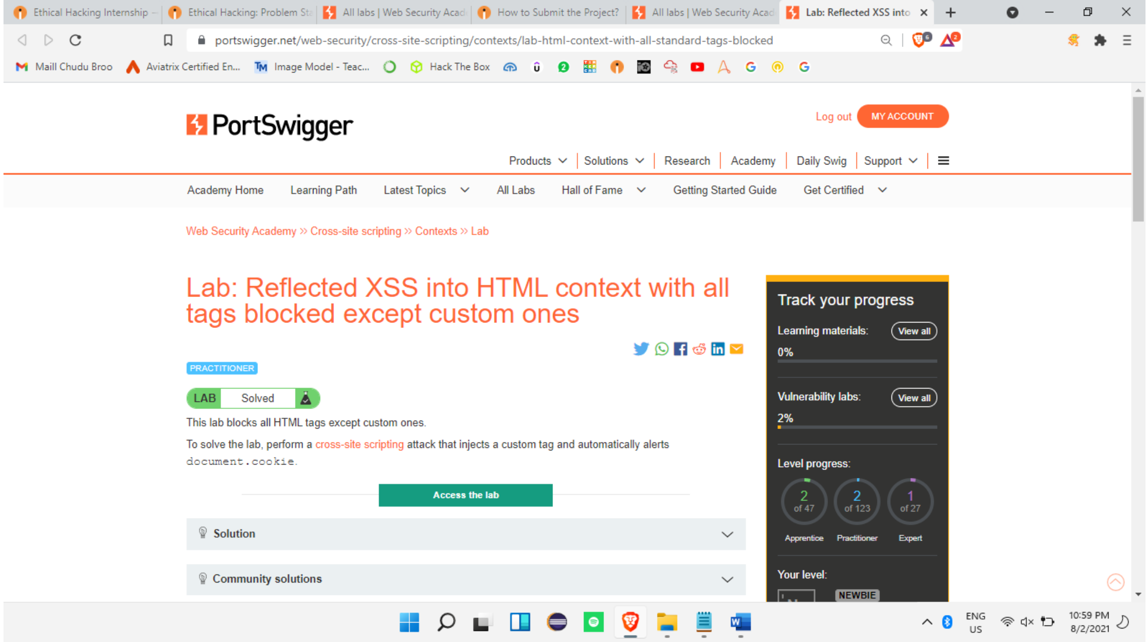
Learning materials: 0%

Vulnerability labs: 2%

Level progress: 2 of 47 Apprentice, 2 of 123 Practitioner, 1 of 27 Expert

Your level: NEWBIE

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



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

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`.

Track your progress

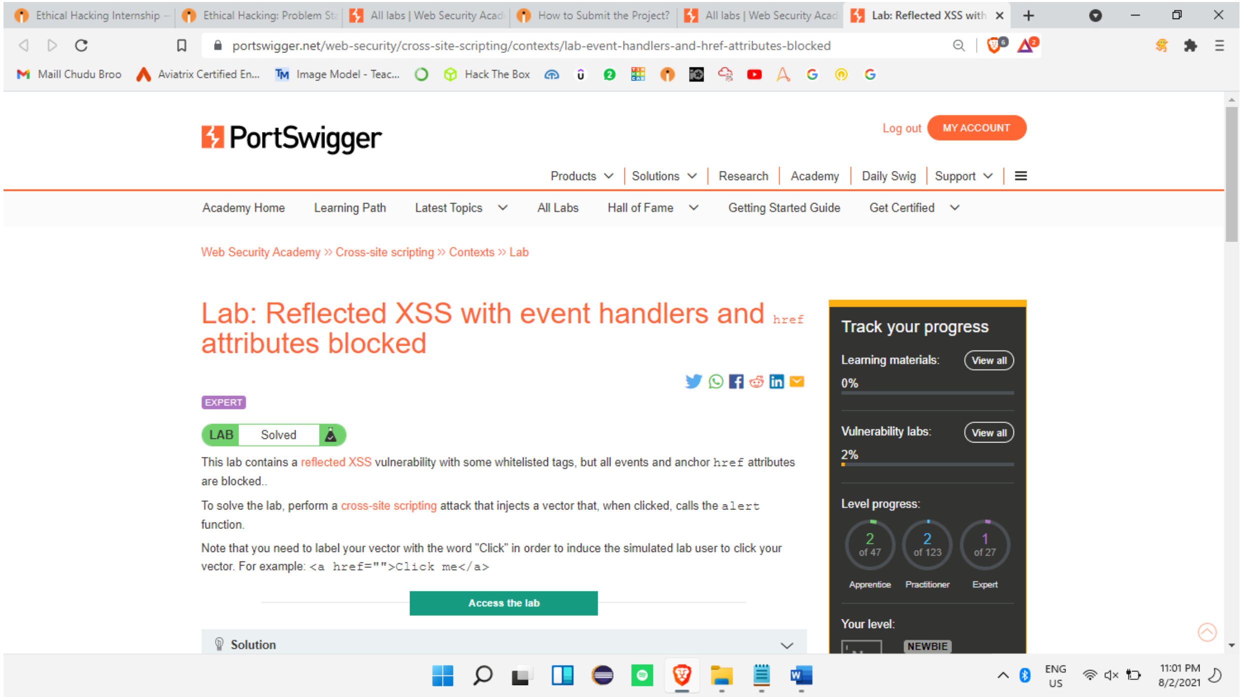
Learning materials: 0%

Vulnerability labs: 2%

Level progress: 2 of 47 Apprentice, 2 of 123 Practitioner, 1 of 27 Expert

Your level: NEWBIE

Lab: Reflected XSS with event handlers and `href` attributes blocked



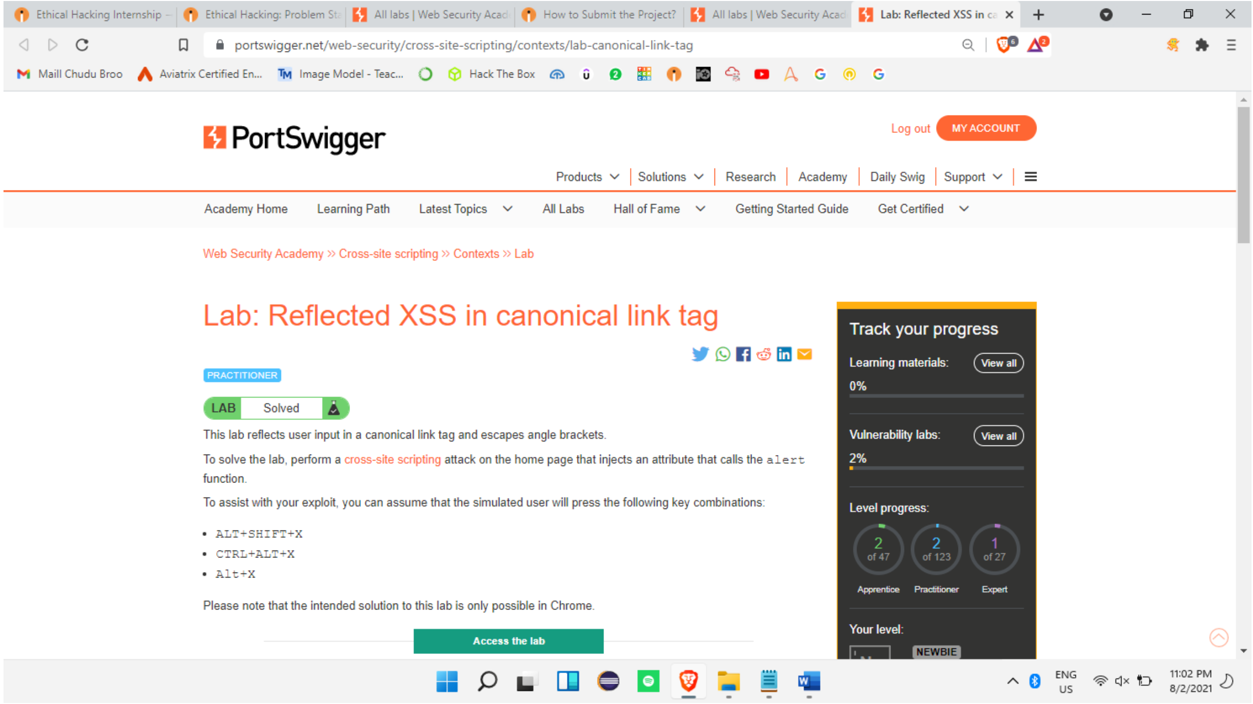
Lab: Reflected XSS with event handlers and `href` attributes blocked

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>`

Lab: Reflected XSS in canonical link tag



Lab: Reflected XSS in canonical link tag

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

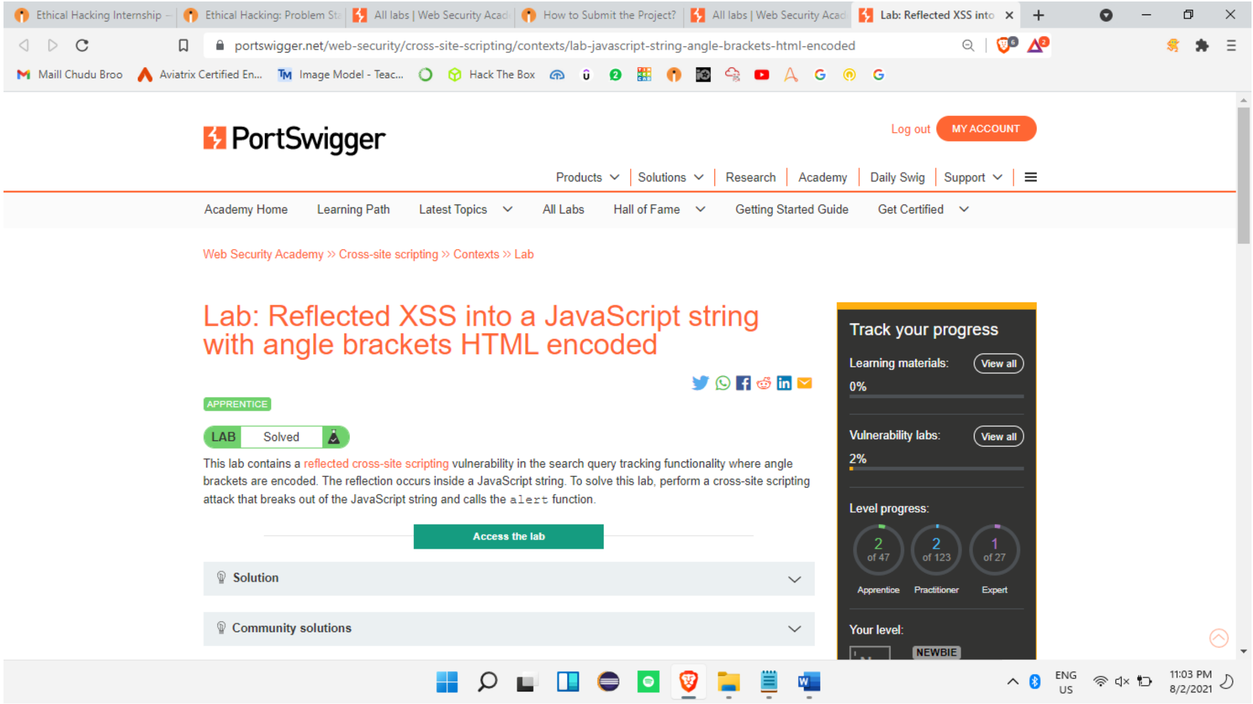
To solve the lab, perform a cross-site scripting attack on the home page that injects an attribute that calls the `alert` function.

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.

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



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

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

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.

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