TASK1

AIM:- **SOLVING THE VULNERABILITIES OF XSS LABS AT P0RTSWIGGER..**

DOMAIN:- **P0RTSWIGGER**

LABS:- l.Reflected XSS into HTML context with nothing encoded.

2. Stored XSS into HTML context with nothing encoded.
3. DOM XSS in document.write sink using source location.search.
4. DOM XSS in inner HTML sink using source location.search
5. Stored DOM XSS

STEPS:-

STEPS TO BE FOLLOWED:

STEP 1: OPEN VIRTUAL BOX AND LOGIN TO KALI LINUX .

STEP 2: OPEN FIREFOX IN LINUX AND SEARCH PORTSWIGGER.

STEP 3: SIGN UP TO PORT SWIGGER AFTER SIGNING UP SIGN IN TO THE WEBSITE.

STEP 4: OPEN YOUR PROFILE THEN OPEN THE VULNERABILITIES LIST .

STEP 5:NOW CHECK WHETHER THE XSS LAB VULNERABILITIES ARE AVAILABLE OR NOT.

STEP 6: NOW START SOLVING THE VULNERABILITIES OF XSS LABS BY USING PAYLOADS.

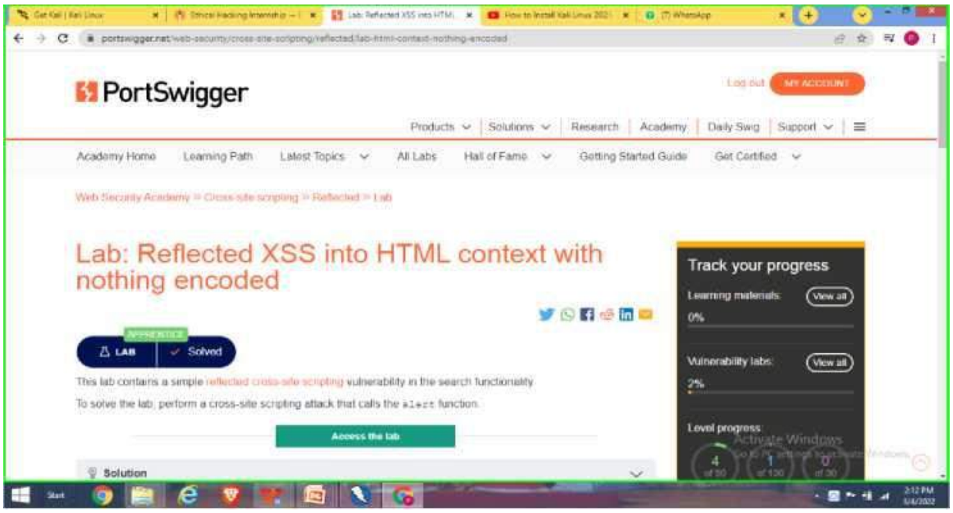
STEP 7: PAYLOADS CAN BE DOWNLOADED FROM GITHUB.

STEP 8: SOLVE ANY 5 OF THE GIVEN VULNERABILITIES,THE TASK IS FINISHED.

LAB1

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.



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

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

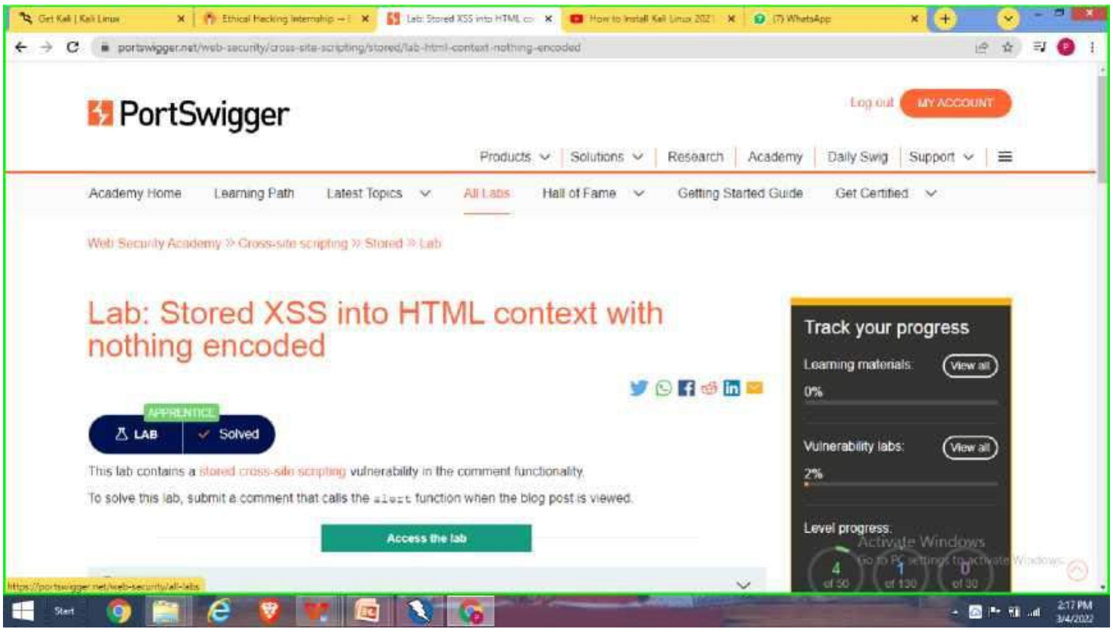
Lab: Reflected XSS into HTML context with nothing encoded

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.

LAB2

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.



Get Kali | Kali Linux
Ethical Hacking Internship – I
Lab: Stored XSS into HTML co
How to Install Kali Linux 2021
(7) WhatsApp
portswigger.net/web-security/cross-site-scripting/stored/lab-html-context-nothing-encoded
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
Get Certified
Web Security Academy » Cross-site scripting » Stored » Lab

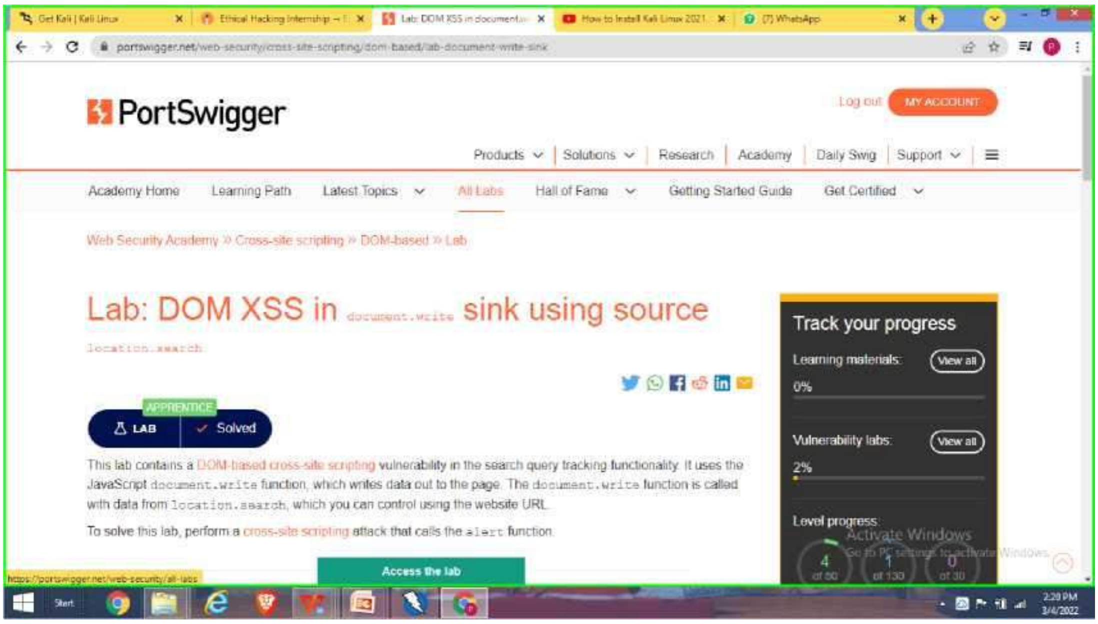
Lab: Stored XSS into HTML context with nothing encoded

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.

LAB3

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.



Get Kali | Kali Linux
Ethical Hacking Internship – I
Lab: DOM XSS in document.w
How to Install Kali Linux 2021
(7) WhatsApp
portswigger.net/web-security/cross-site-scripting/dom-based/lab-document-write-sink
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
Get Certified
Web Security Academy » Cross-site scripting » DOM-based » Lab

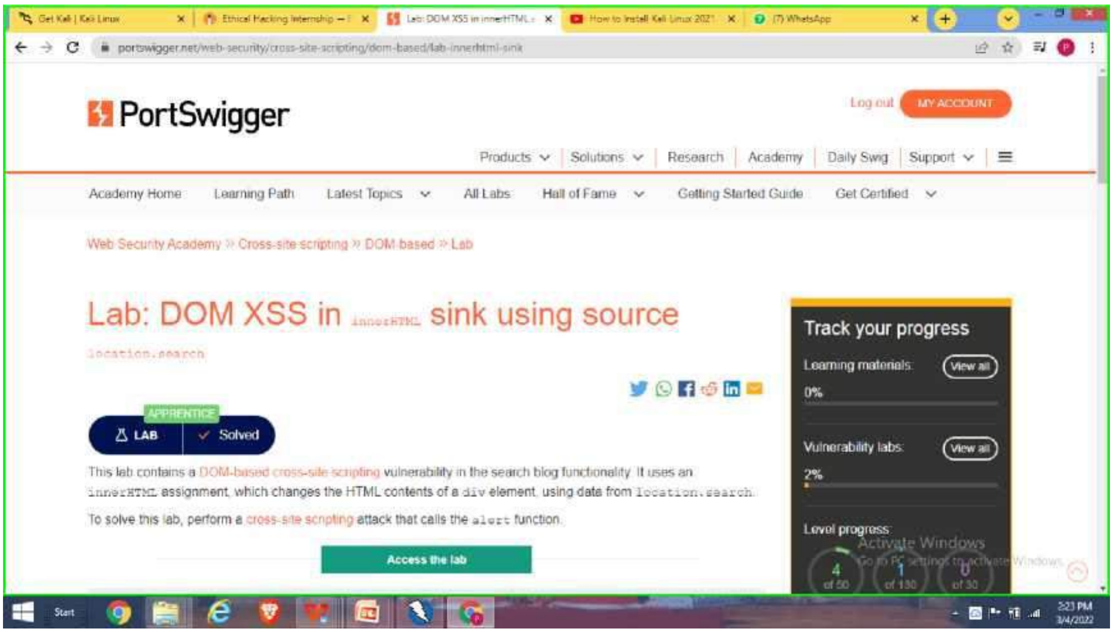
Lab: DOM XSS in `document.write` sink using source `location.search`

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.

LAB4

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.



Get Kali | Kali Linux
Ethical Hacking Internship – I
Lab: DOM XSS in innerHTML s
How to Install Kali Linux 2021
(7) WhatsApp
portswigger.net/web-security/cross-site-scripting/dom-based/lab-innerhtml-sink
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
Get Certified
Web Security Academy » Cross-site scripting » DOM-based » Lab

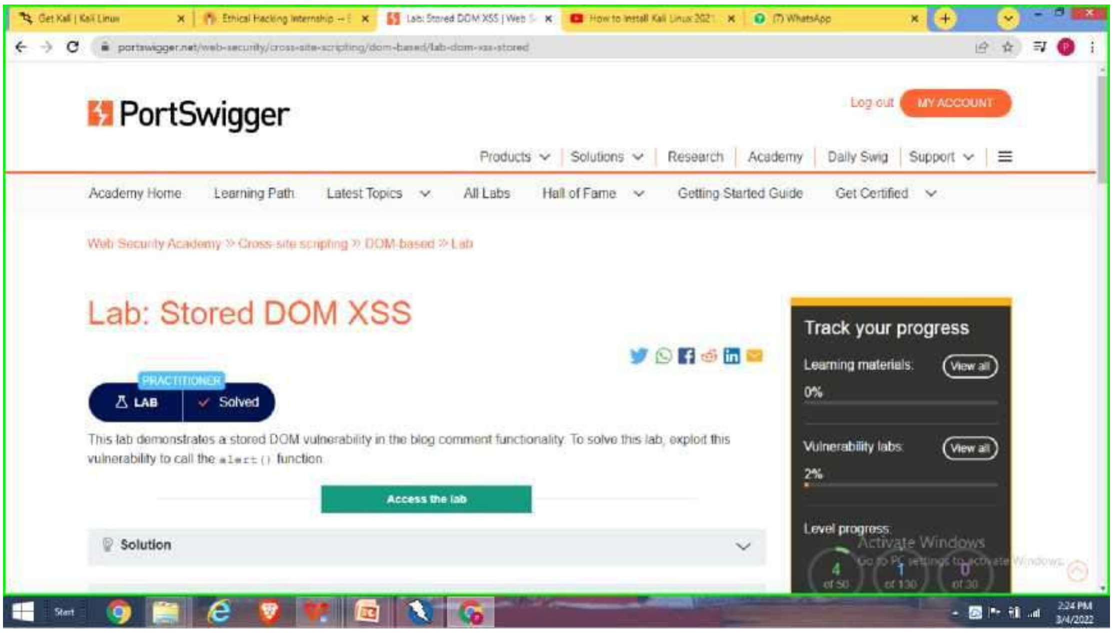
Lab: DOM XSS in innerHTML sink using source location.search

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.

LAB5

This lab demonstrates a stored DOM vulnerability in the blog comment functionality. To solve this lab, exploit this vulnerability to call the `alert()` function



Get Kali | Kali Linux
Ethical Hacking Internship – I
Lab: Stored DOM XSS | Web S
How to Install Kali Linux 2021
(7) WhatsApp
portswigger.net/web-security/cross-site-scripting/dom-based/lab-dom-xss-stored
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
Get Certified
Web Security Academy » Cross-site scripting » DOM-based » Lab

Lab: Stored DOM XSS

This lab demonstrates a stored DOM vulnerability in the blog comment functionality. To solve this lab, exploit this vulnerability to call the alert() function.

VIDEO:-

INTERNSHIP STUDIO
TASK 1

ALL THE LABS

CONCLUSION:-

Using Diffrent techniques to find VULNERABILITIES using XSS lab.