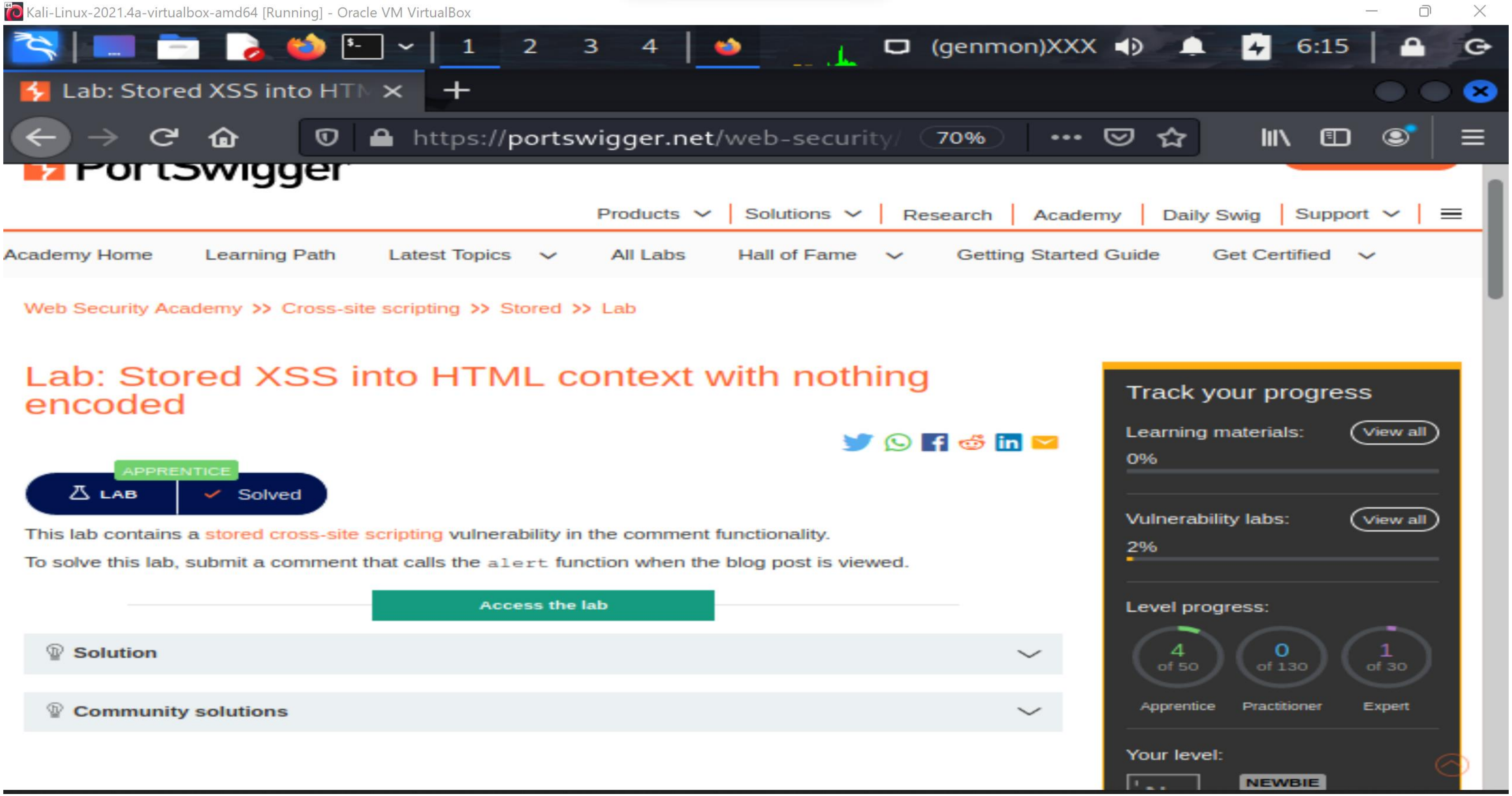
Task 1: SOLVING THE VULNERABILITIES OF XSS LABS AT P0RTSWIGGER

GOWTHAM B H



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.

Track your progress

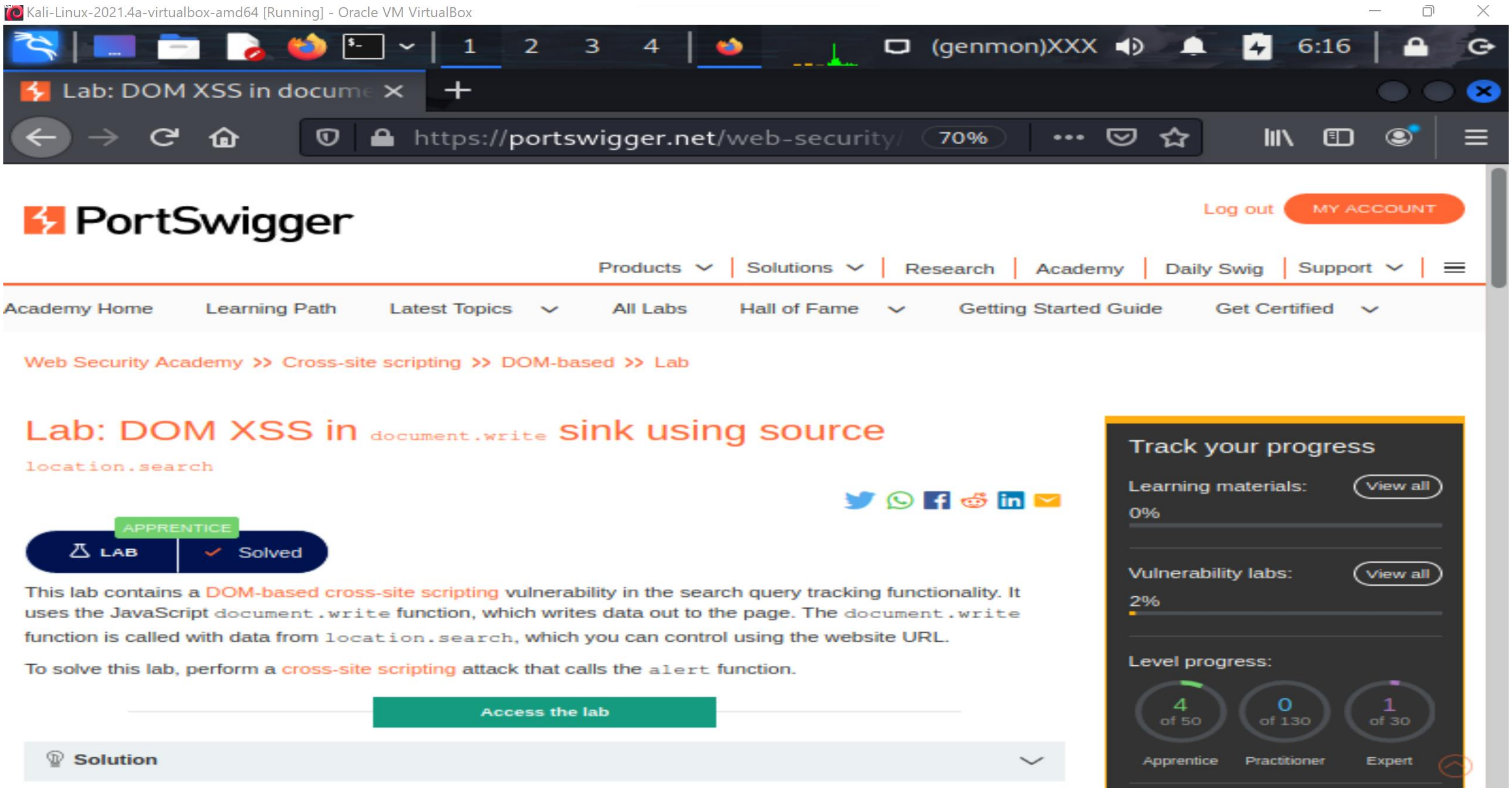
Learning materials: View all
0%

Vulnerability labs: View all
2%

Level progress:

4	0	1
of 50	of 130	of 30
Apprentice	Practitioner	Expert

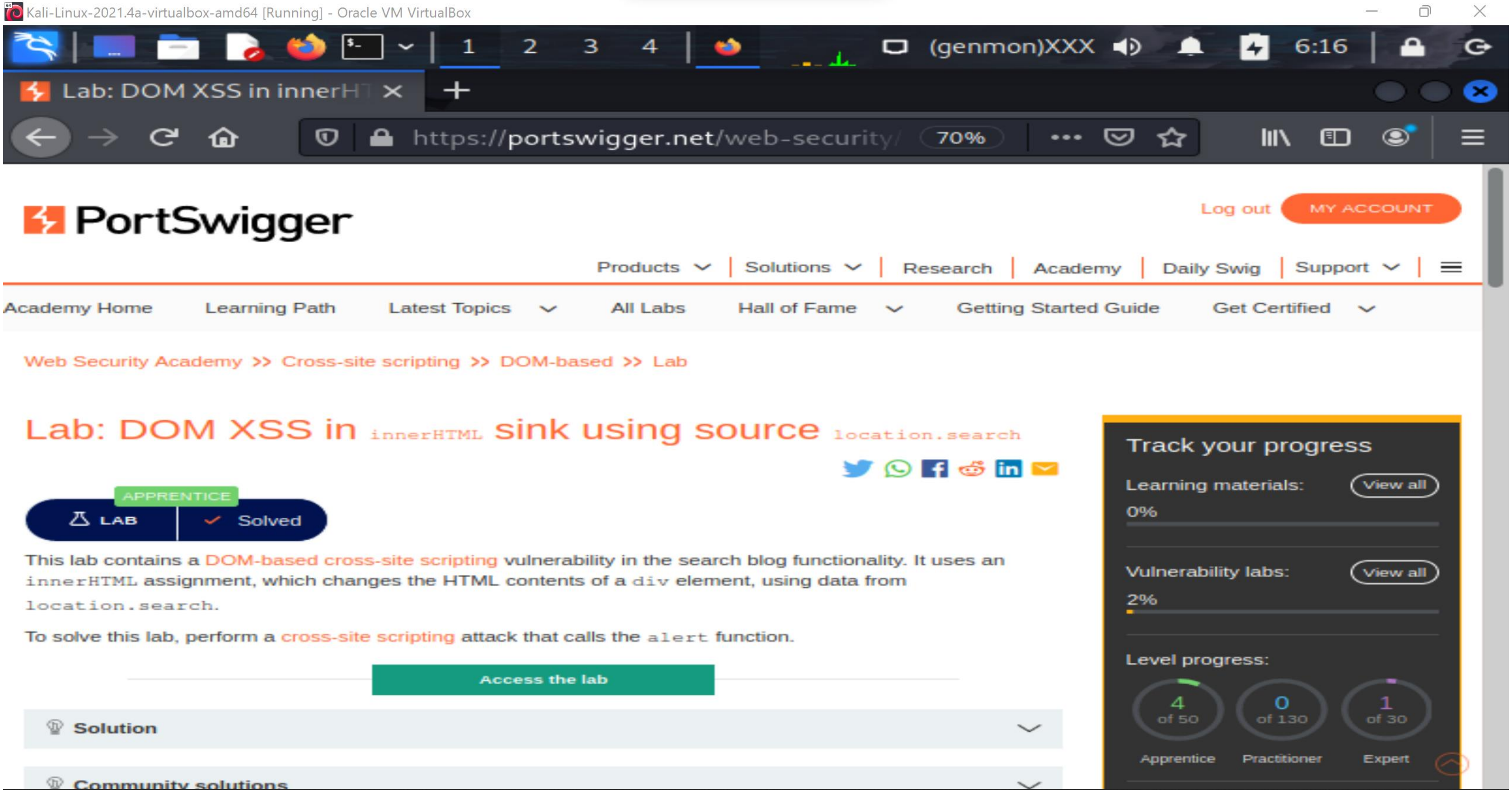
Your level: NEWBIE



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.



Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
1
2
3
4
(genmon)XXX
6:16
Lab: DOM XSS in innerH
https://portswigger.net/web-security/
70%

PortSwigger

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.

Track your progress

Learning materials: View all

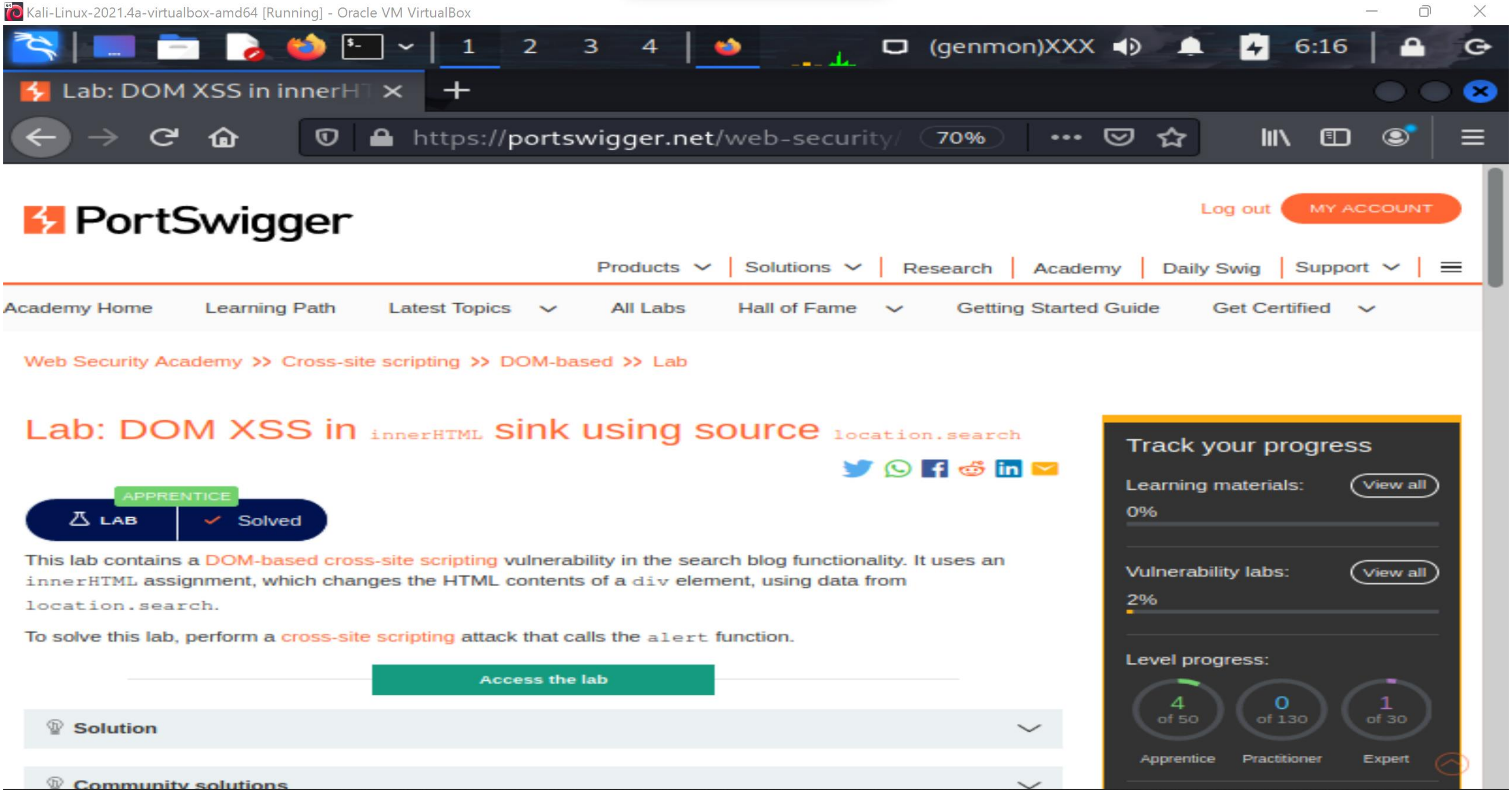
0%

Vulnerability labs: View all

2%

Level progress:

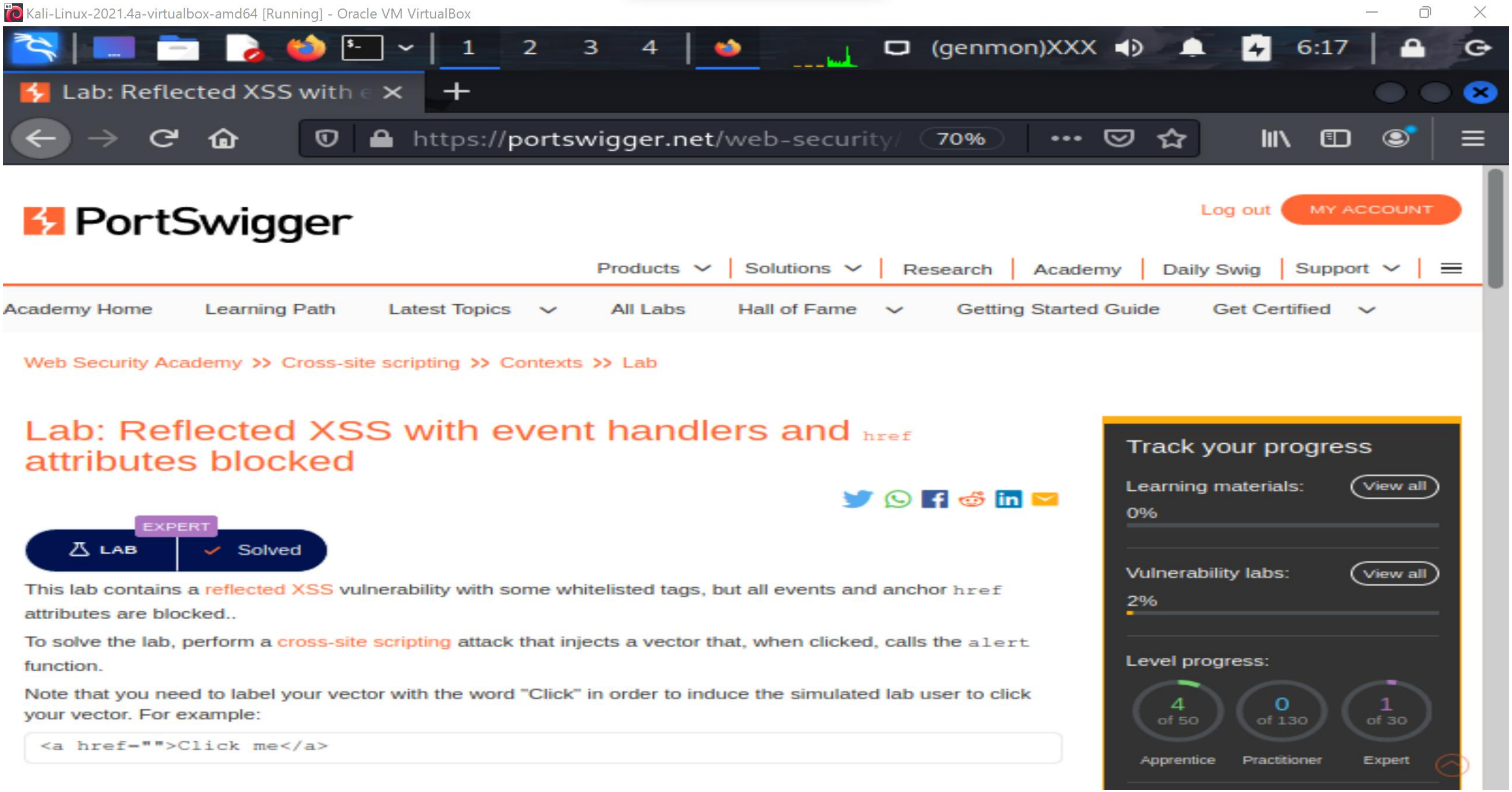
4 of 50	0 of 130	1 of 30
Apprentice	Practitioner	Expert



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.


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
1
2
3
4
(genmon)XXX
6:17
Lab: Reflected XSS with e
https://portswigger.net/web-security/
70%

PortSwigger

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

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>
```

Track your progress

Learning materials: View all
0%

Vulnerability labs: View all
2%

Level progress:

4 of 50	0 of 130	1 of 30
Apprentice	Practitioner	Expert