internship
studio

ETHICAL HACKING INTERNSHIP

Name: Kalyani Gajanan Lonkar

Institutional Affiliation: Internship Studio

Email: kalyanilonkar5@gmail.com

Task : 1

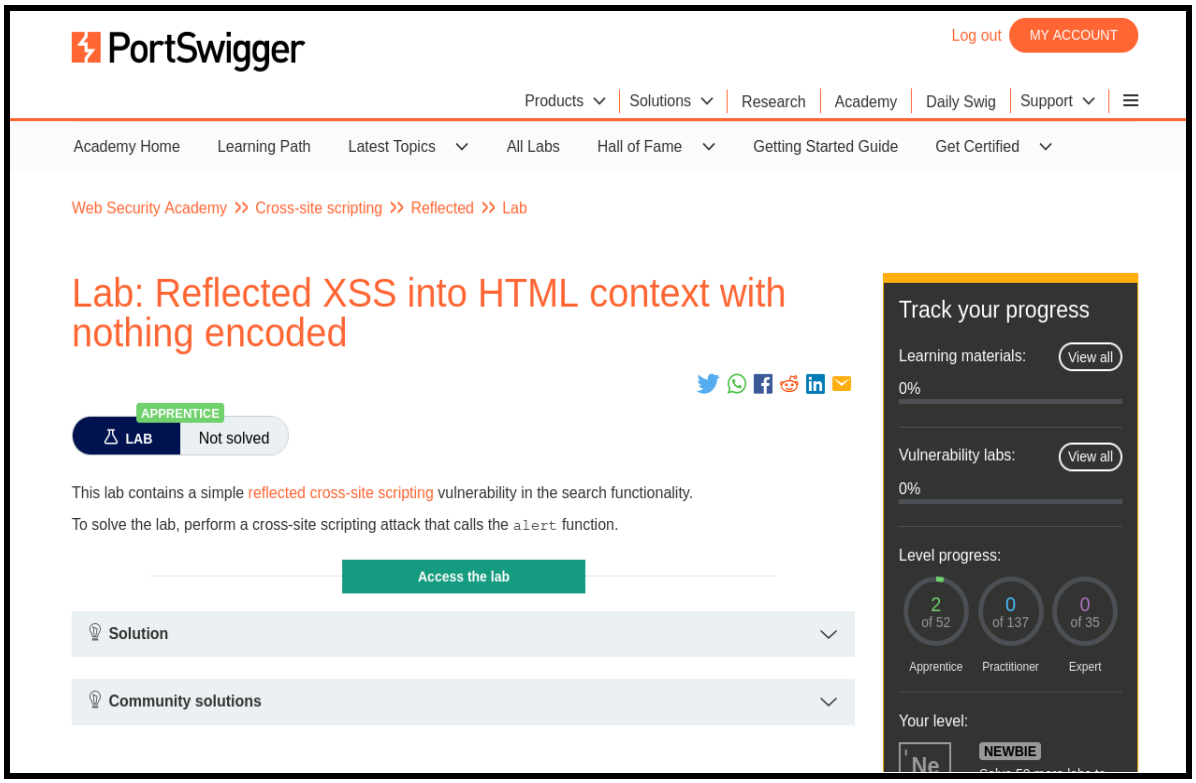
Portswigger Vulnerability Labs

https://portswigger.net/web-security/all-labs

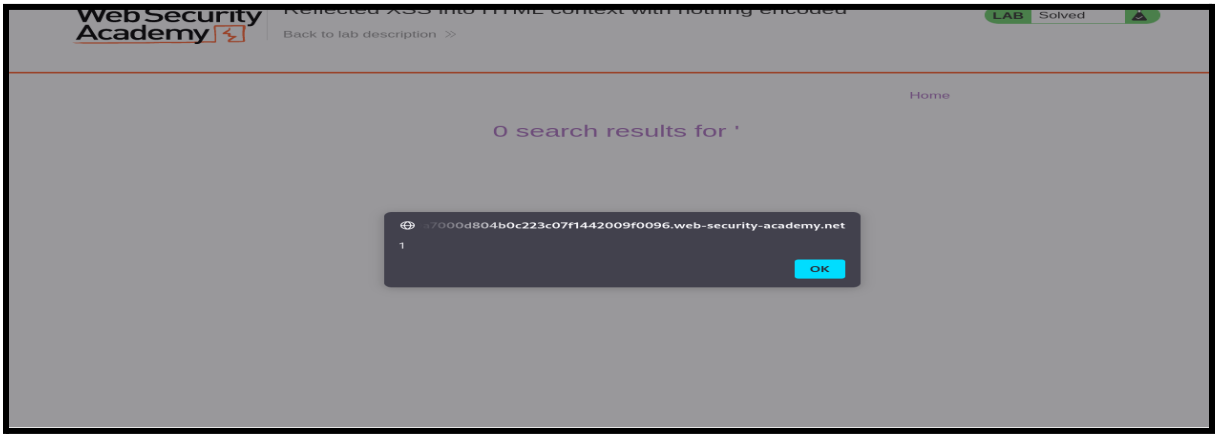
Cross-site scripting

Lab 1: Reflected XSS into HTML context with nothing encoded.

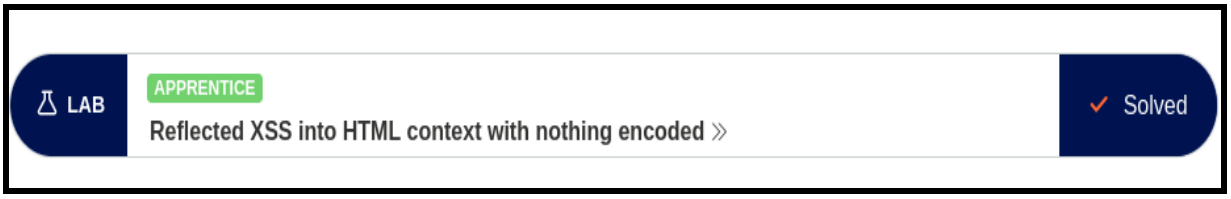
This lab contains a simple *reflected cross-site scripting* vulnerability in the search functionality.
To solve the lab,perform a *cross-site scripting* attack that calls the **alert** function.



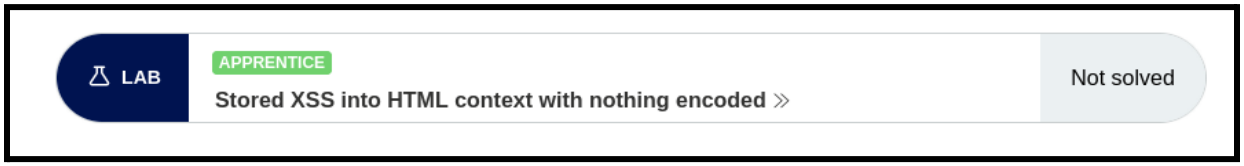
Using the script <script>alert(1)</script> we got a pop up.



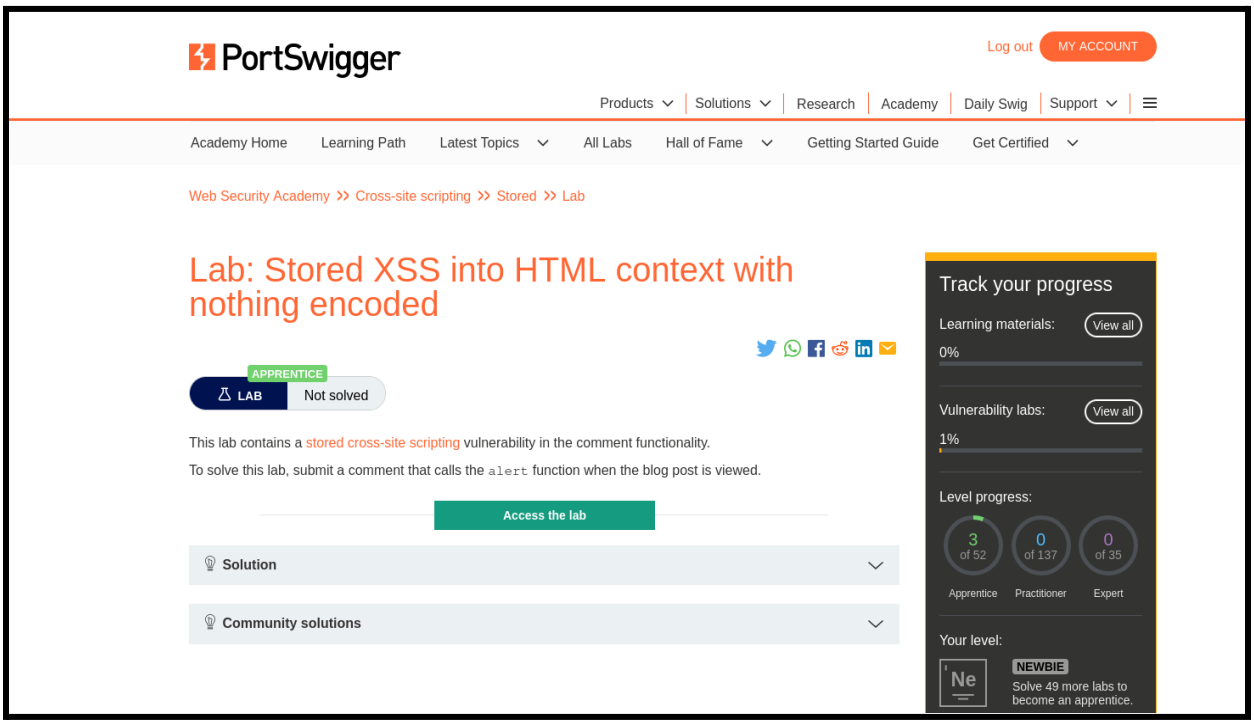
And so we have found the reflected cross-site scripting vulnerability. And hence we have completed the Lab.



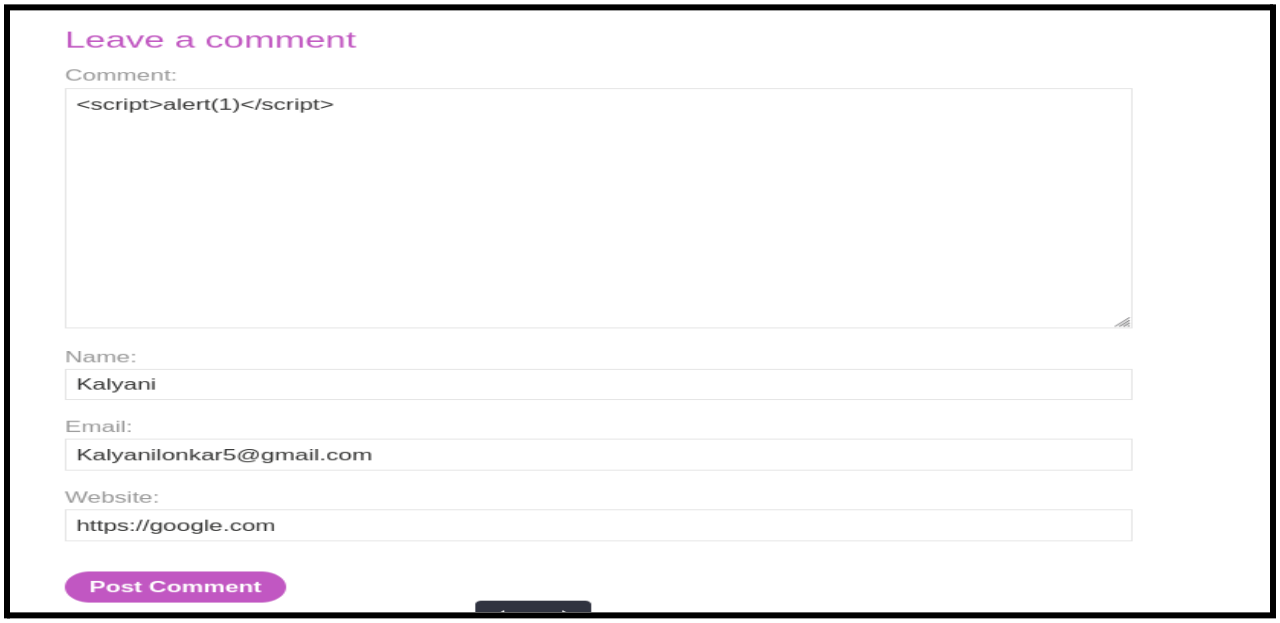
Lab 2: Stored XSS into HTML context with nothing encoded.



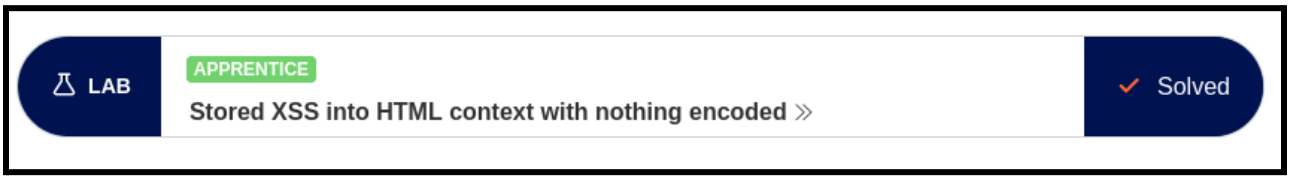
This lab contains a *stored cross-site scripting* vulnerability in the comment functionality.
To solve this lab, submit a comment that calls the **alert** function when the blog post is viewed.



After Viewing this Post. Put the <script>alert(1)</script> in the comment section and post it.



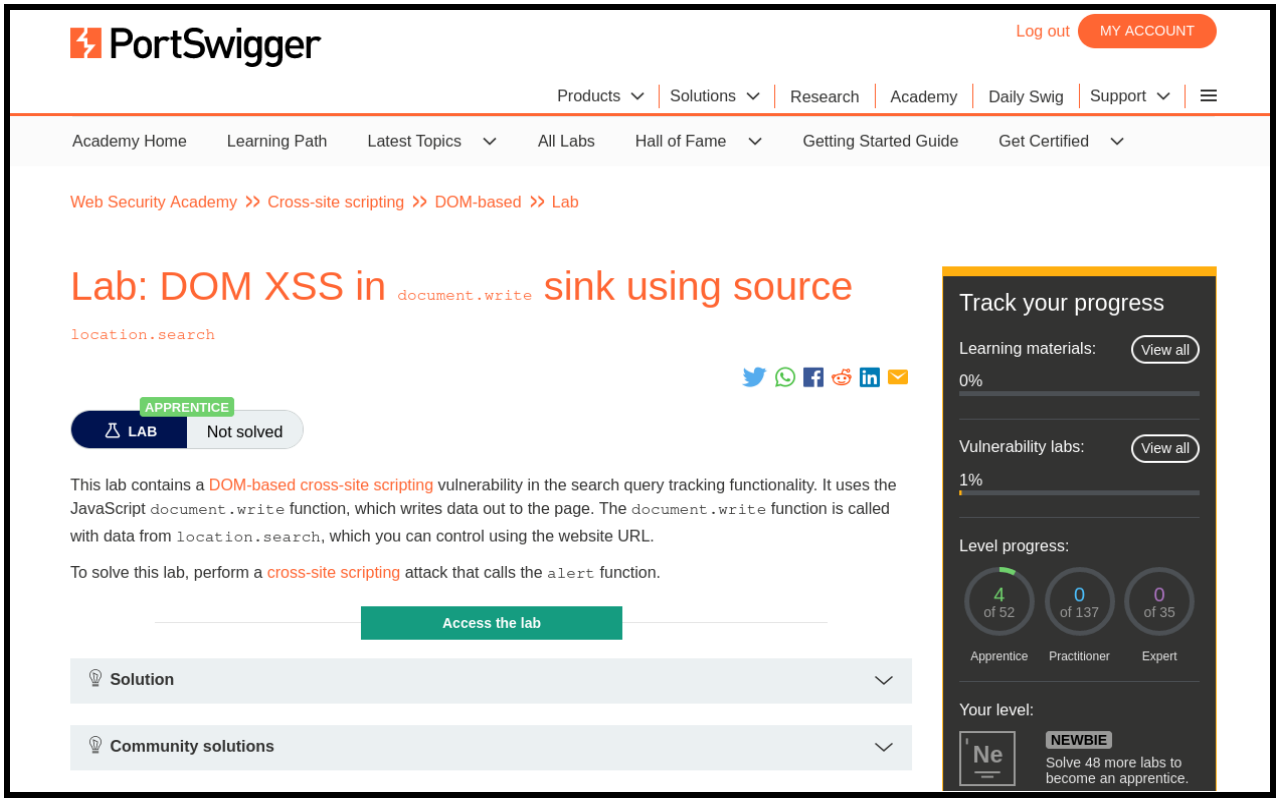
Hence we have completed the Lab.



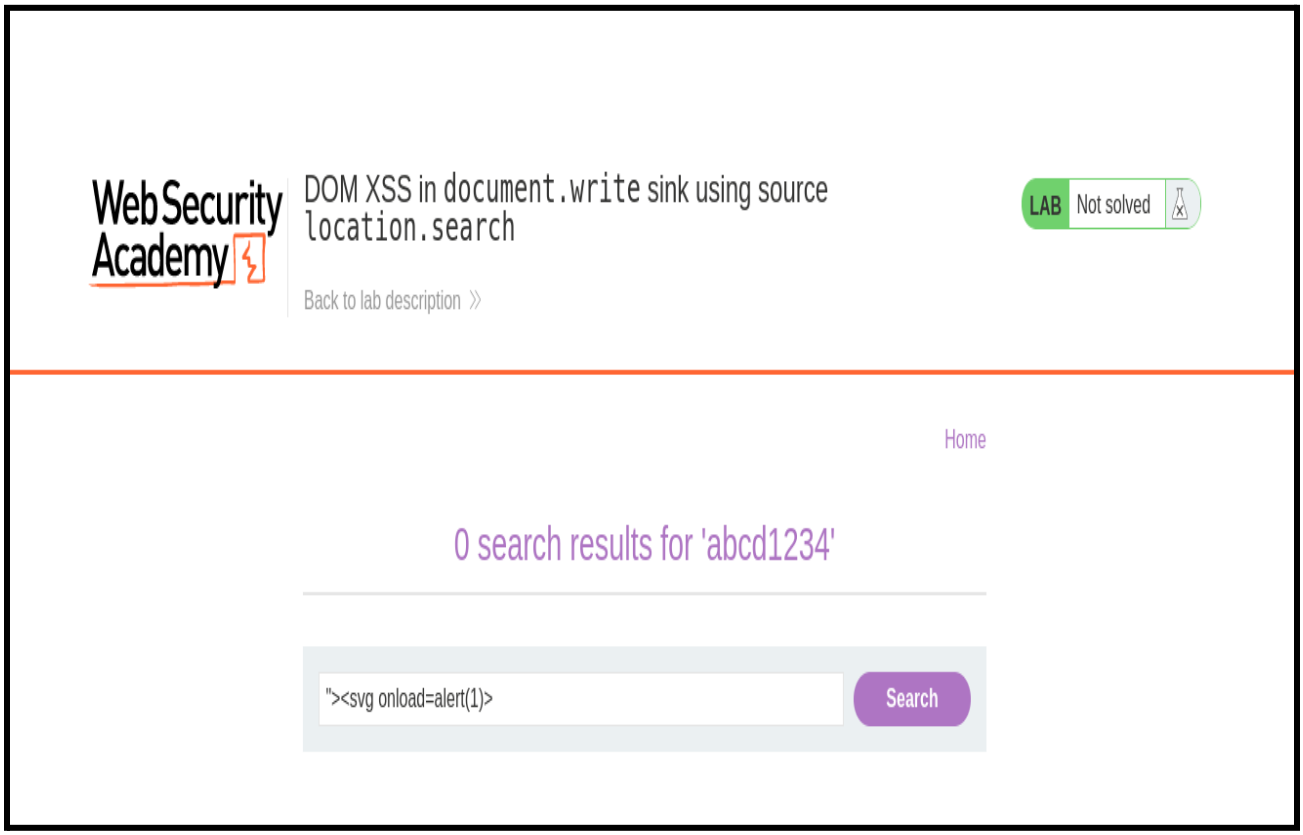
internship studio

Lab 3: DOM XSS 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.



Performing a cross-site scripting attack that calls the alert function.

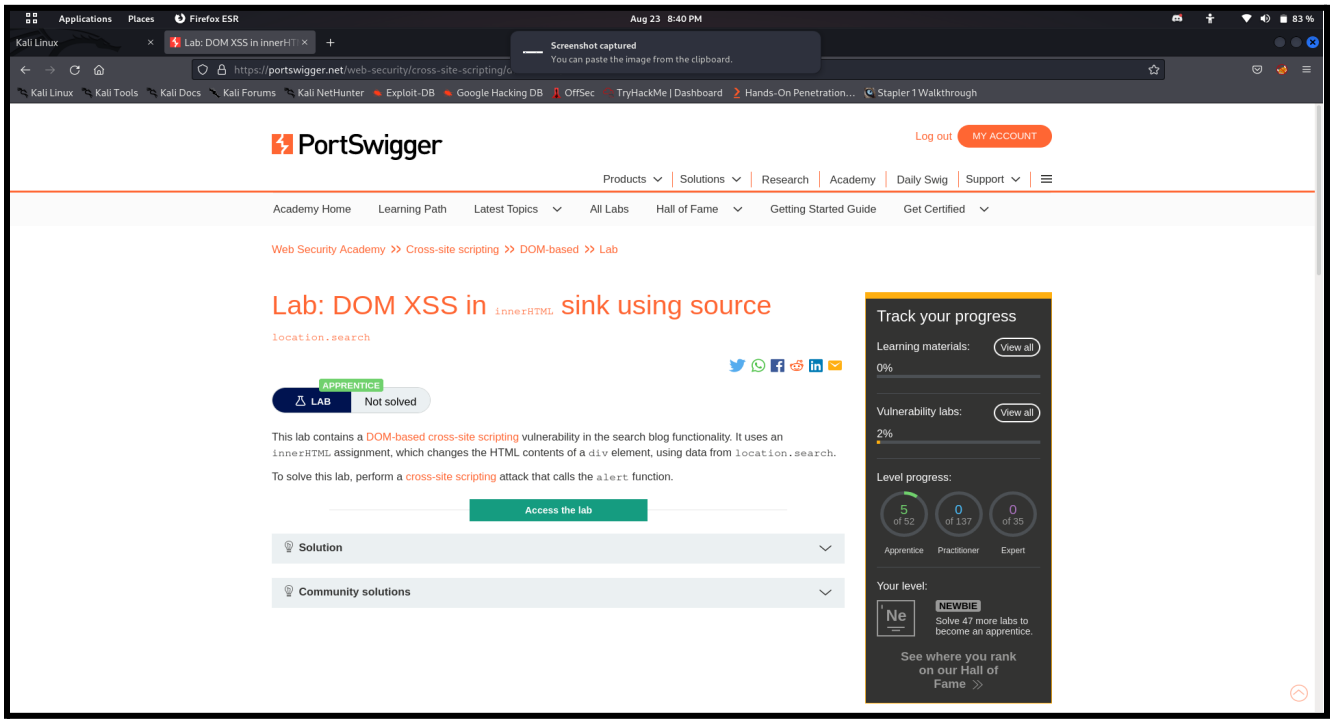


Using the script “><svg onload=alert(1)> we got the vulnerability. Hence we have completed the lab.

internship studio

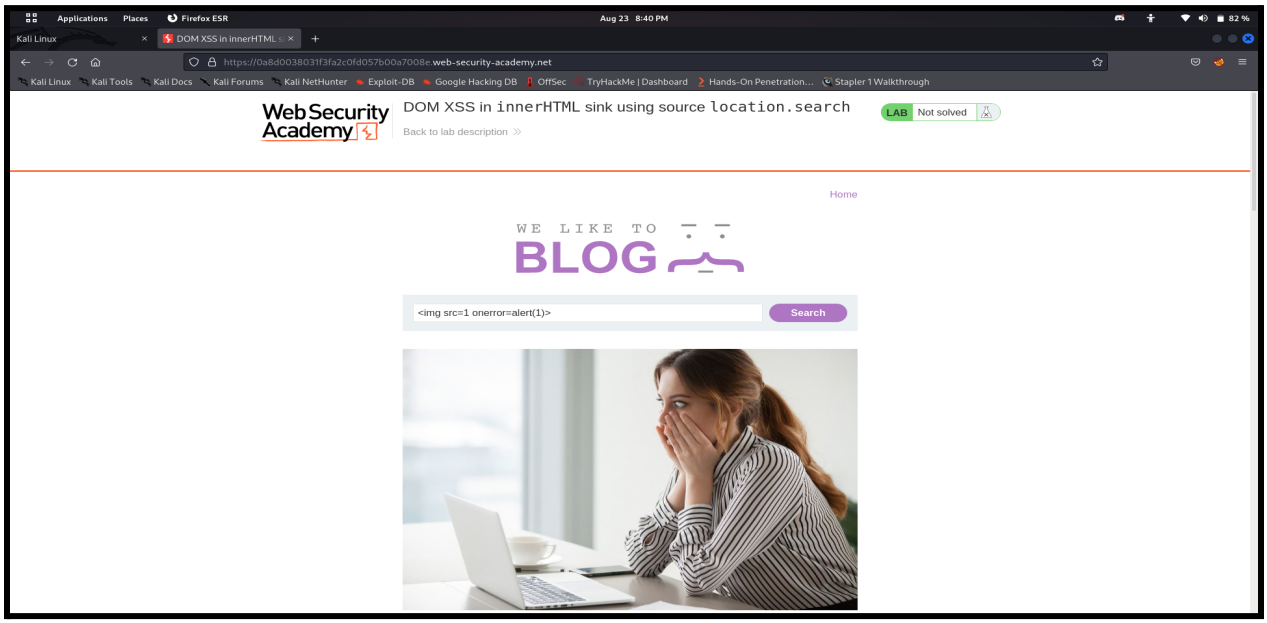
Lab 4: DOM XSS in innerHTML sink using source location.search

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.

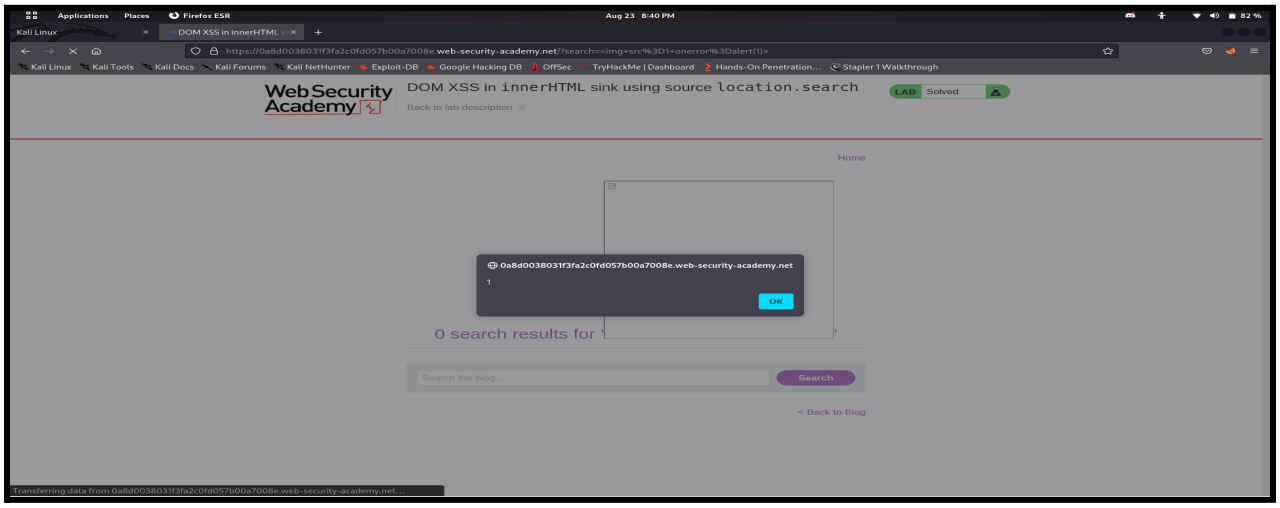


internship studio

Using the Script <img src=1 onerror=alert(1)>



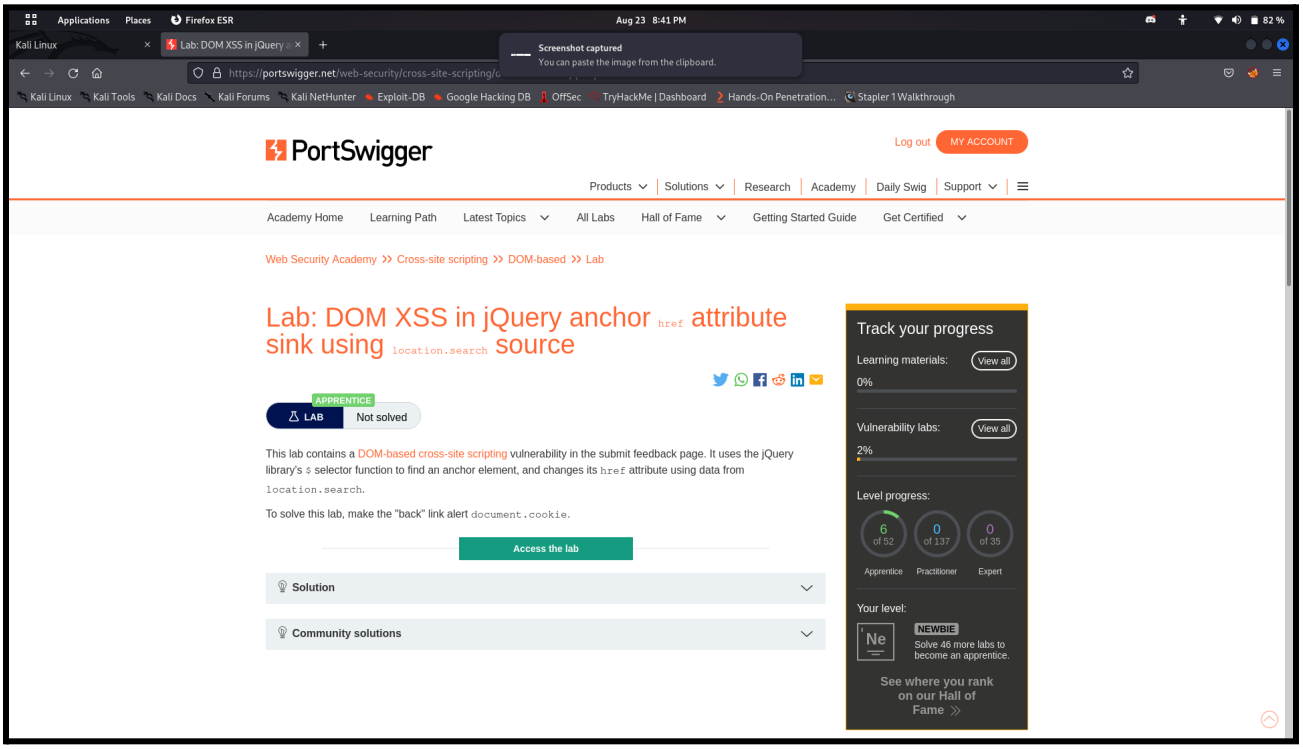
Hence after the pop up arrives the lab is completed



internship studio

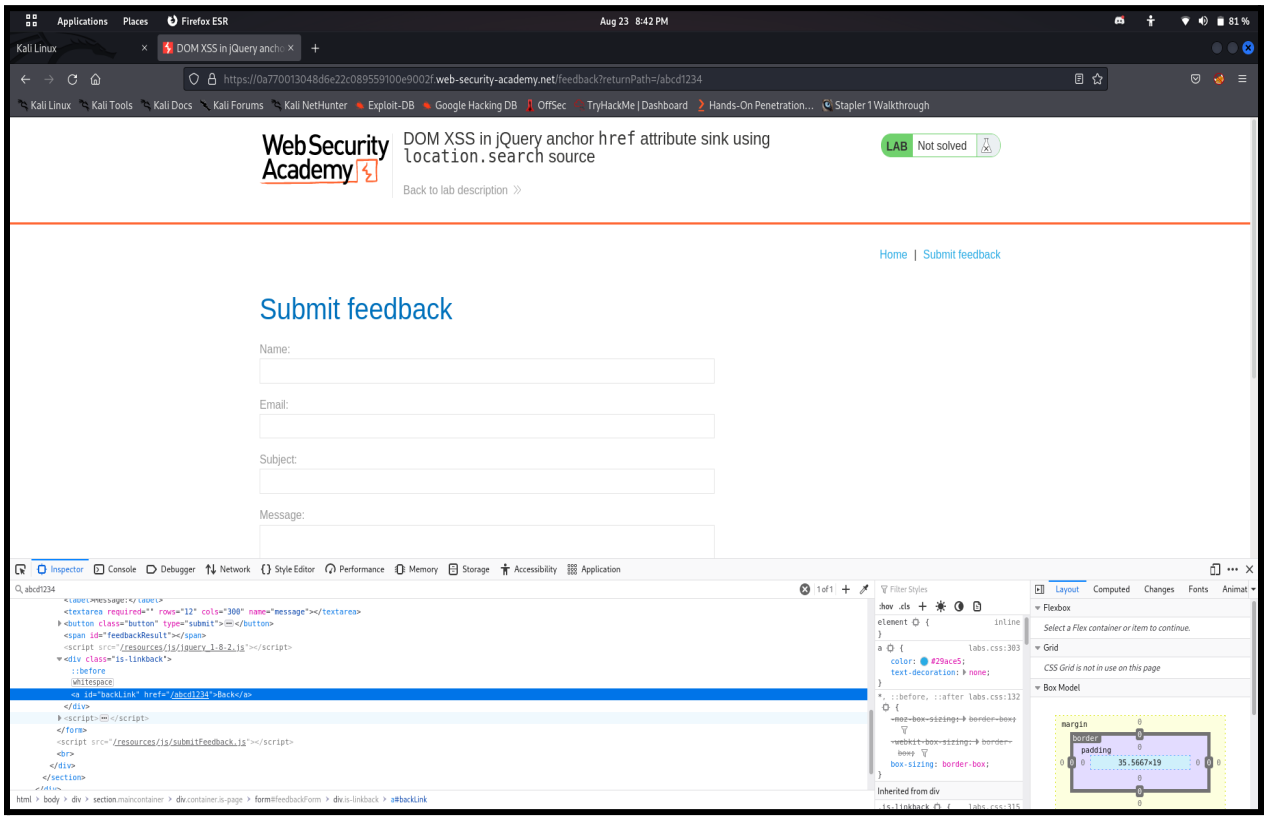
Lab 5: DOM XSS in jQuery anchor href attribute sink using location.search source.

This lab contains a DOM-based cross-site scripting vulnerability in the submit feedback page. It uses the jQuery library $ selector function to find an anchor element, and changes its href attribute using data from location.search.
To solve this lab, make the “back” link alert document.cookie.

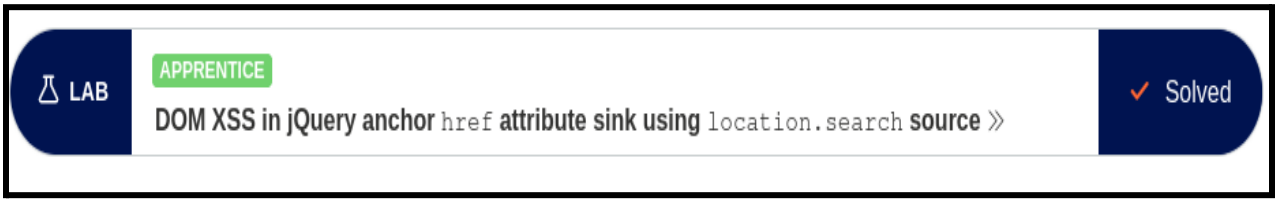


internship studio

After accessing the lab inspect the page, then search abc1234



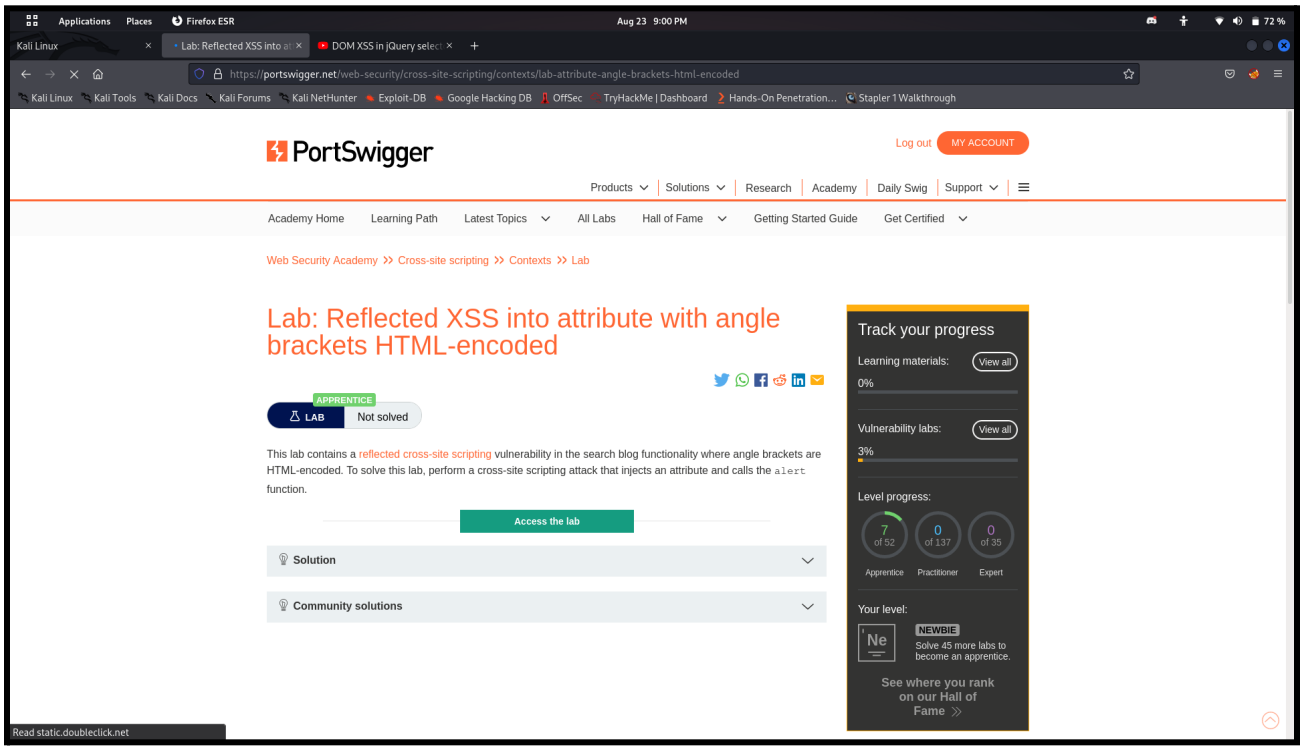
Using the script javascript:alert(1) in the page url then enter
The lab is completed.



internship studio

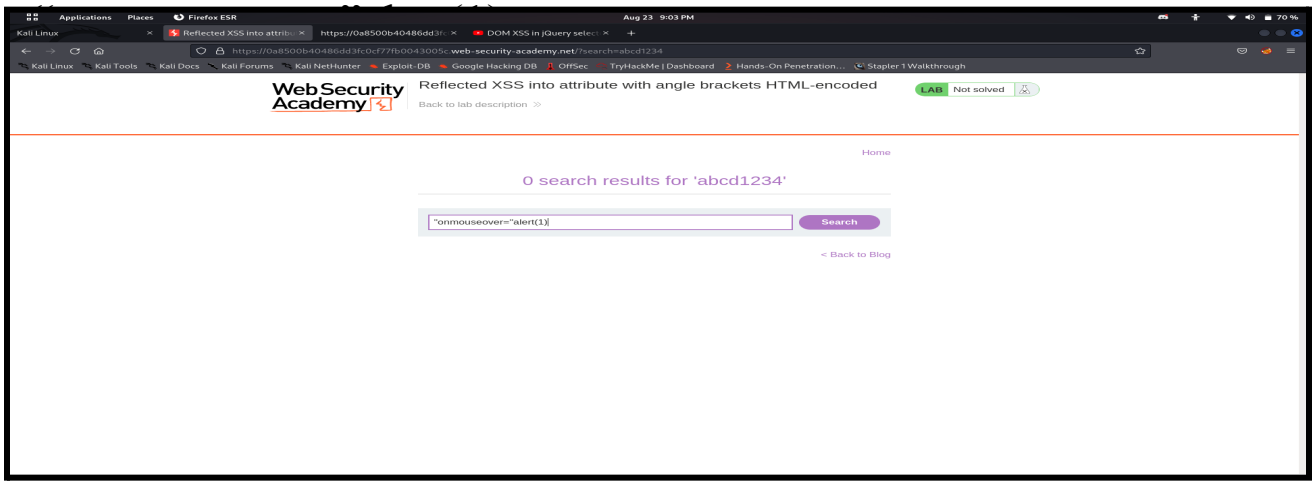
Lab 6: Reflected XSS into attribute with angle brackets HTML-encoded

The 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.

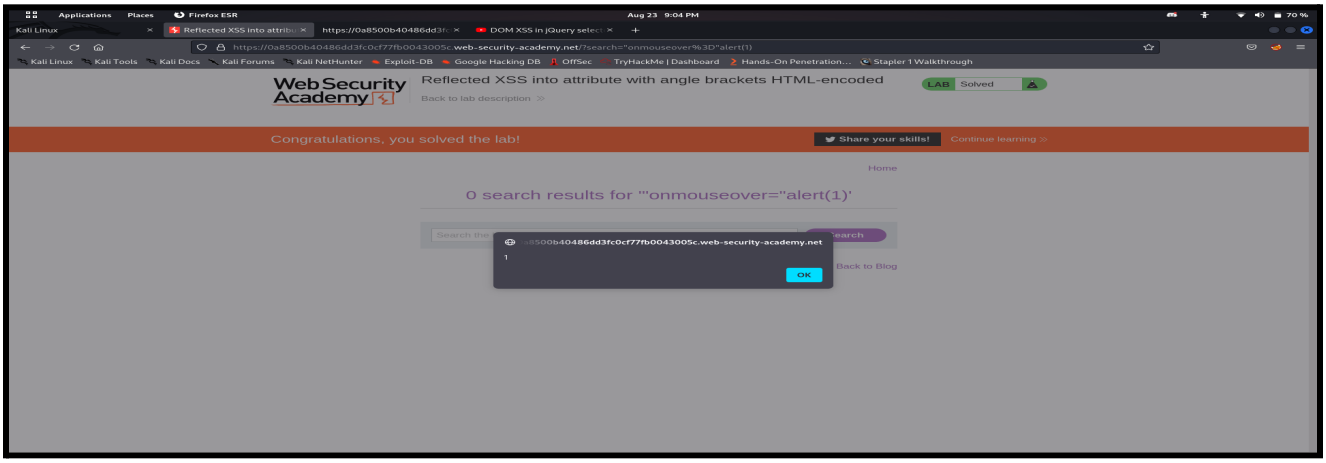


internship studio

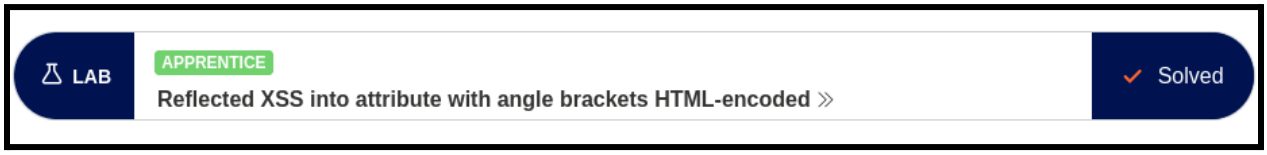
Putting the Script in the search blog functionality



After putting in the script and pressed enter got a pop up we got the vulnerability.



Hence the lab is solved.



internship studio

5 Portswigger Vulnerability Labs are Completed