

ETHICAL HACKING INTERNSHIP

Name: Kalyani Gajanan Lonkar

Institutional Affiliation: Internship Studio

Email: kalyanilonkar5@gmail.com

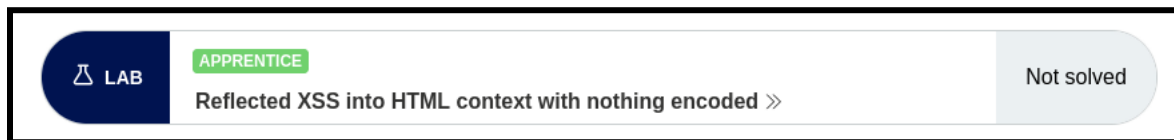
Task : 1

Portswigger Vulnerability Labs

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

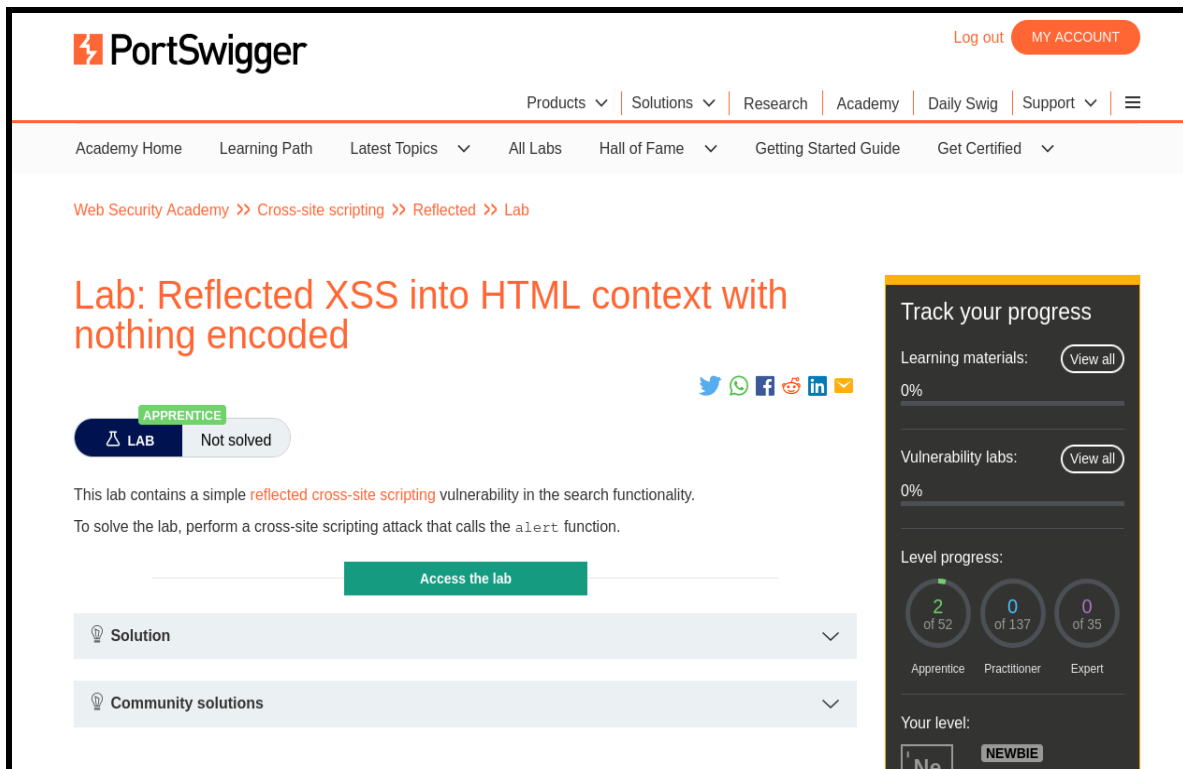
Cross-site scripting

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



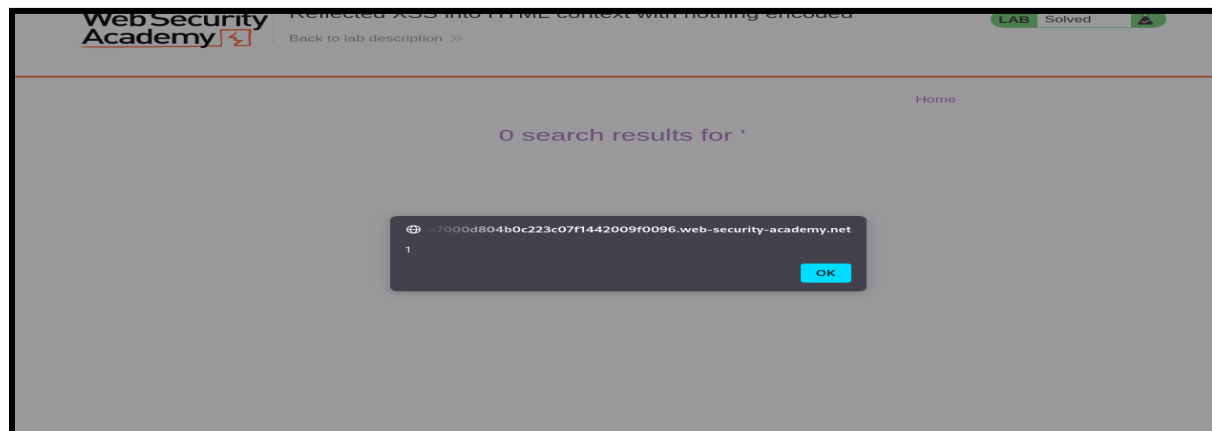
This lab contains a simple *reflected cross-site scripting* vulnerability in the search functionality.

To solve the lab, perform a *cross-site scripting* attack that calls the **alert** function.

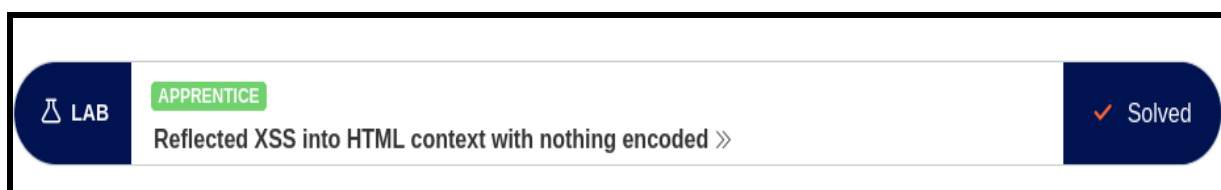


The screenshot shows the PortSwigger Web Security Academy interface. At the top, there's a navigation bar with 'Log out' and 'MY ACCOUNT'. Below it, a secondary navigation bar lists various categories like 'Products', 'Solutions', 'Research', 'Academy', 'Daily Swig', and 'Support'. The main content area displays the lab title 'Lab: Reflected XSS into HTML context with nothing encoded' in orange. Below the title, there's a 'LAB' button with a 'Not solved' status and a green 'APPRENTICE' tag. A 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 'Access the lab' button is present. On the right, a 'Track your progress' sidebar shows 'Learning materials: 0%' and 'Vulnerability labs: 0%'. It also displays 'Level progress' with three circular progress indicators for 'Apprentice' (2 of 52), 'Practitioner' (0 of 137), and 'Expert' (0 of 35). At the bottom, there are sections for 'Solution' and 'Community solutions'.

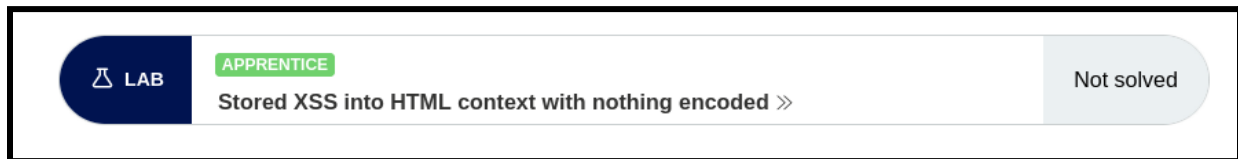
Using the script `<script>alert(1)</script>` we got a pop up.



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

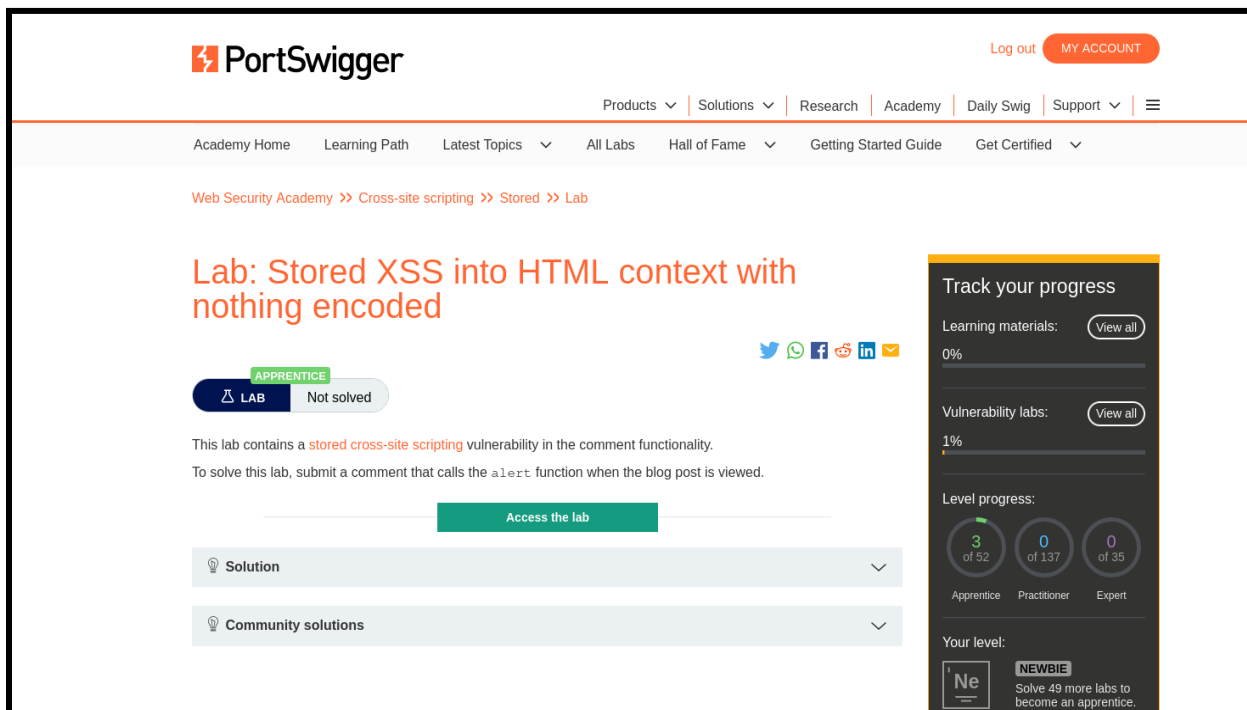


Lab 2: Stored XSS into HTML context with nothing encoded.



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.

A screenshot of the PortSwigger Web Security Academy lab page. The page has a white background with a dark blue header for 'PortSwigger' and a navigation bar with links like 'Products', 'Solutions', 'Research', 'Academy', 'Daily Swig', and 'Support'. Below the navigation bar, there's a breadcrumb trail: 'Web Security Academy >> Cross-site scripting >> Stored >> Lab'. The main heading is 'Lab: Stored XSS into HTML context with nothing encoded' in orange. Below the heading, there's a green 'APPRENTICE' badge and a 'LAB' button. A description states: '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.' There's a green 'Access the lab' button. Below this, there are two expandable sections: 'Solution' and 'Community solutions'. On the right side, there's a dark grey sidebar titled 'Track your progress' showing learning materials (0%), vulnerability labs (1%), and level progress (3 of 52 for Apprentice, 0 of 137 for Practitioner, 0 of 35 for Expert). At the bottom of the sidebar, it says 'Your level: NEWBIE' and 'Solve 49 more labs to become an apprentice.'



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

Leave a comment

Comment:

`<script>alert(1)</script>`

Name:
Kalyani

Email:
Kalyanilonkar5@gmail.com

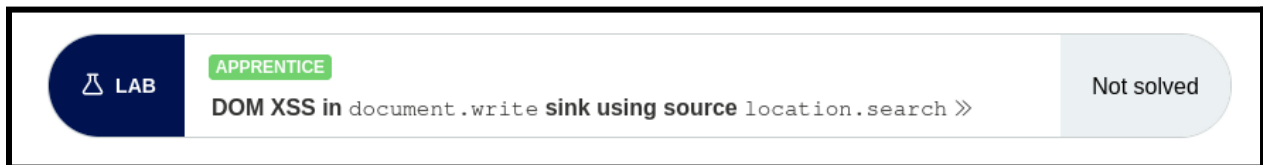
Website:
https://google.com

Post Comment

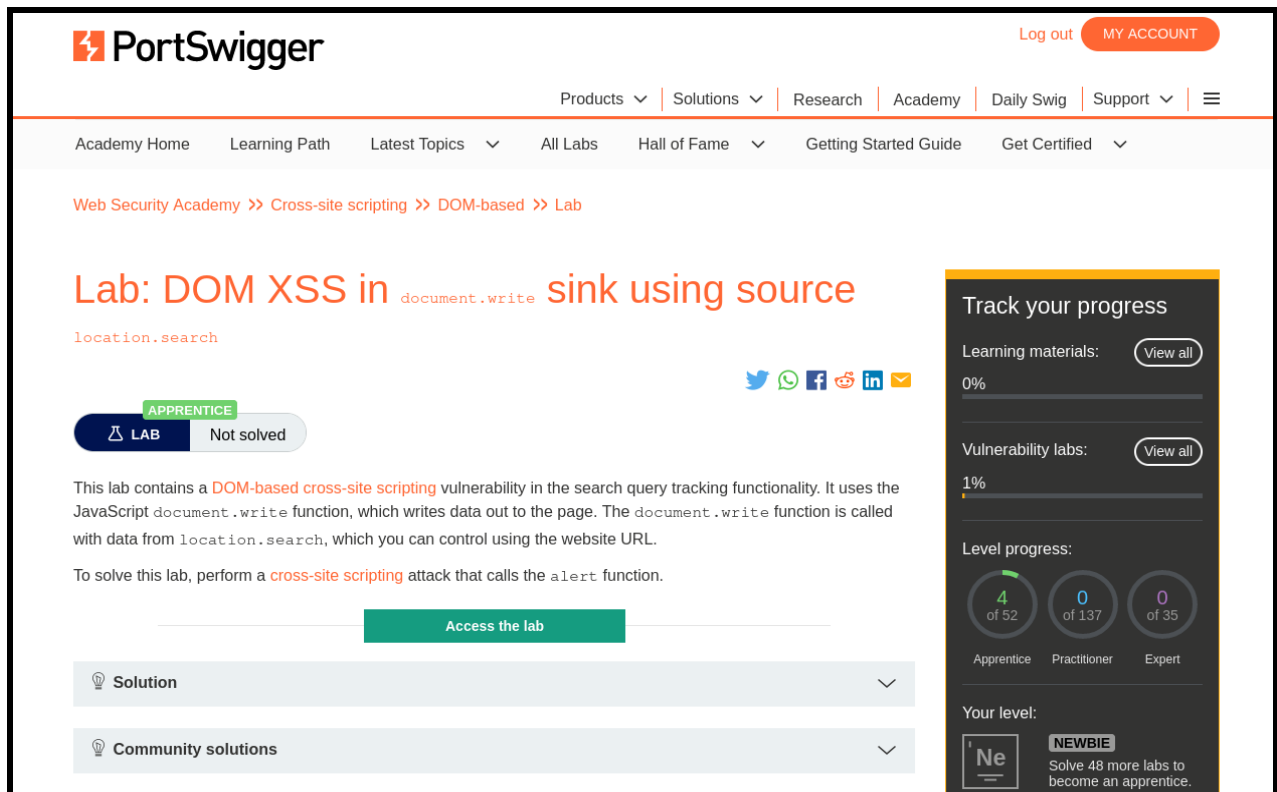
Hence we have completed the Lab.



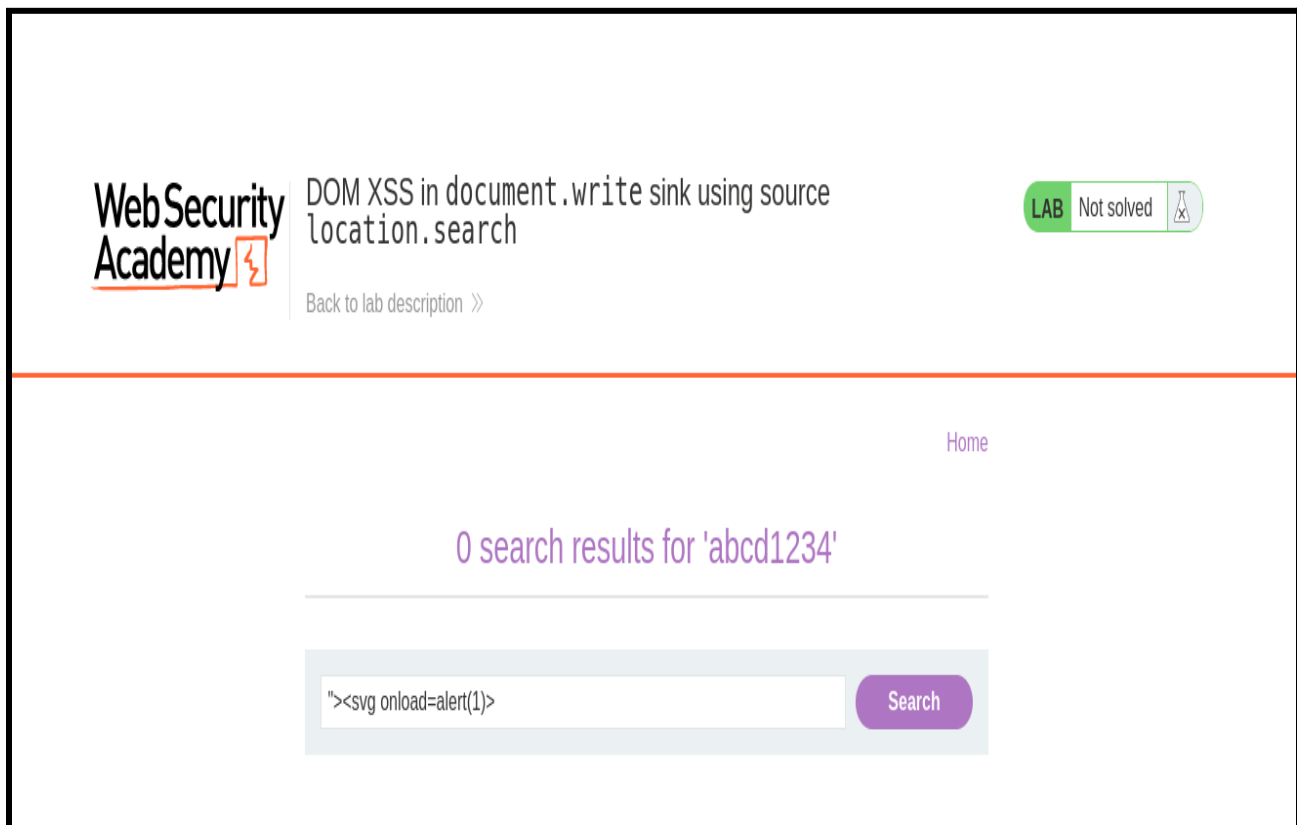
Lab 3: DOM XSS document.write sink using source location.search



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.

The screenshot shows the PortSwigger Academy interface. At the top is the PortSwigger logo and navigation links. Below is a breadcrumb trail: 'Web Security Academy >> Cross-site scripting >> DOM-based >> Lab'. The main heading is 'Lab: DOM XSS in document.write sink using source location.search'. It includes a green 'APPRENTICE' tag, a 'LAB' button, and a 'Not solved' status. The description explains the DOM-based cross-site scripting vulnerability and the document.write function. A green 'Access the lab' button is present. On the right, a 'Track your progress' sidebar shows learning materials (0%), vulnerability labs (1%), and level progress (4 of 52 for Apprentice, 0 of 137 for Practitioner, 0 of 35 for Expert). The user's level is 'NEWBIE' with a goal to solve 48 more labs to become an apprentice. At the bottom, there are expandable sections for 'Solution' and 'Community solutions'.

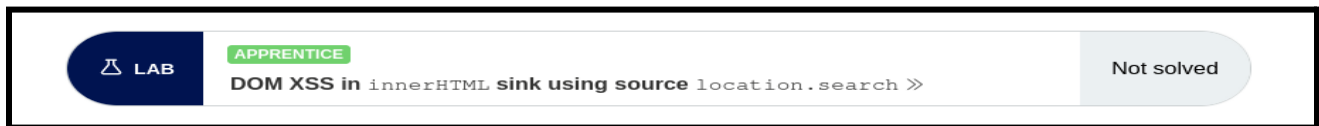
Performing a cross-site scripting attack that calls the alert function.



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

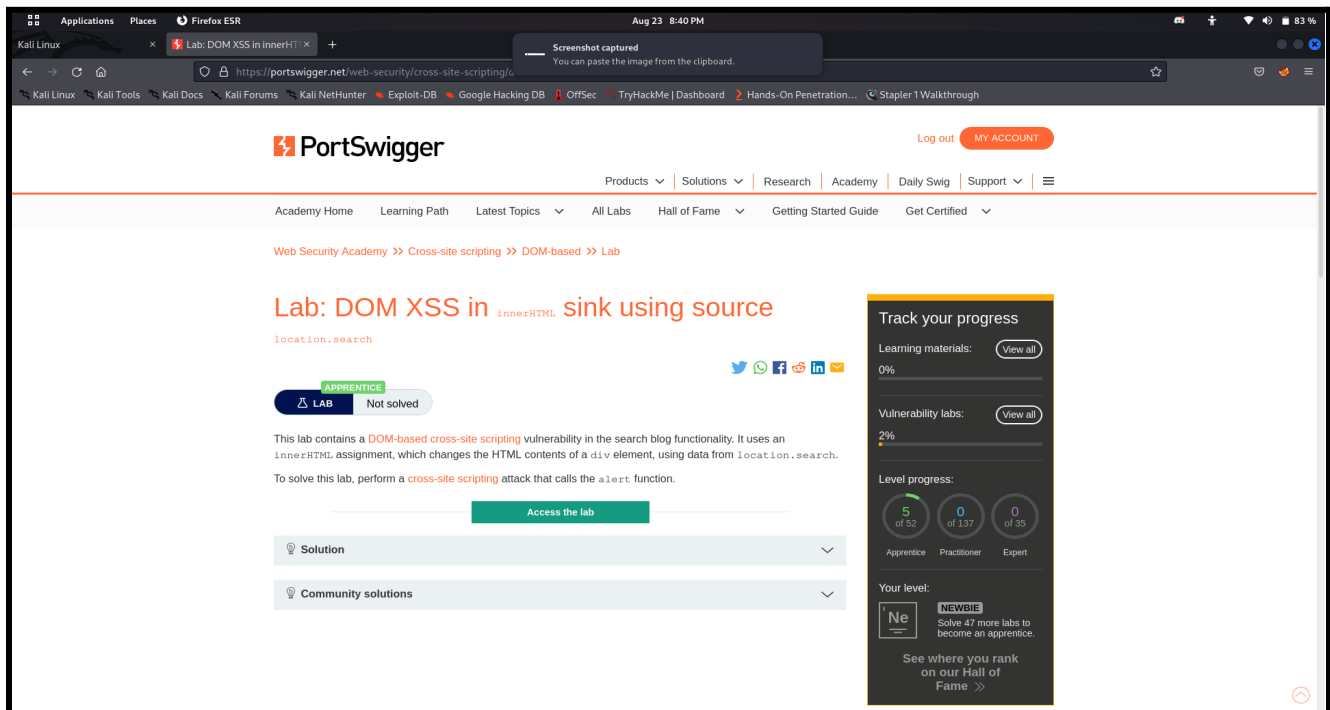


Lab 4: DOM XSS in innerHTML sink using source location.search

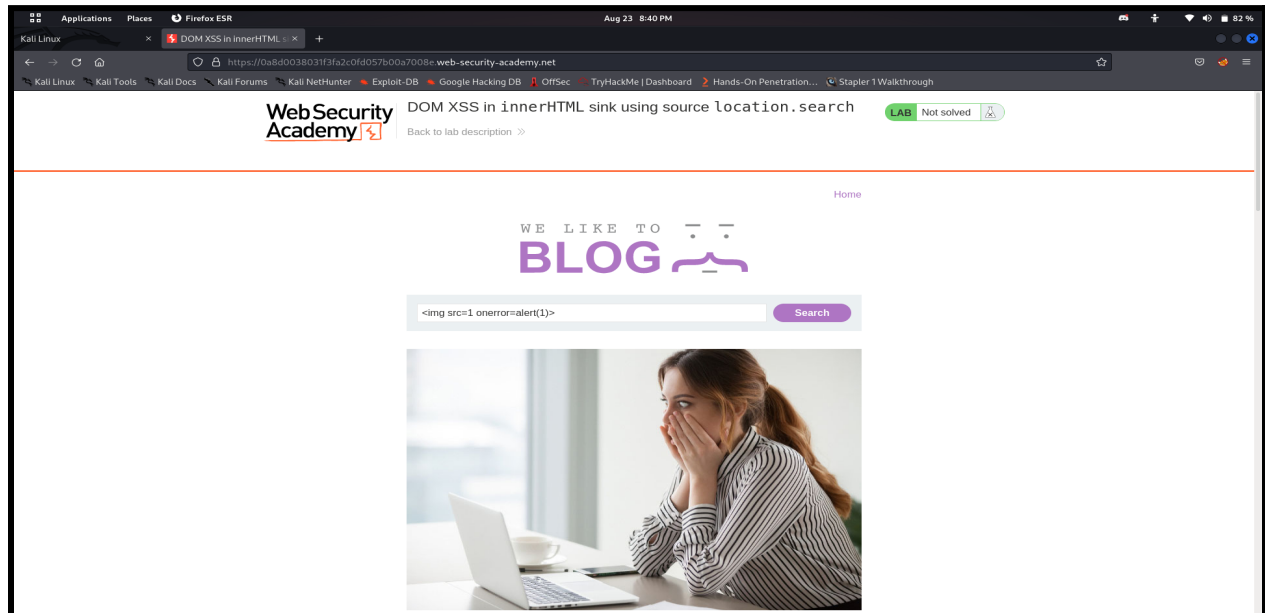


This lab contains a *DOM-based cross-site scripting* vulnerability in the search blog functionality. It uses an innerHTML assignment, which changes the HTML contents of a div element, using data from location.search.

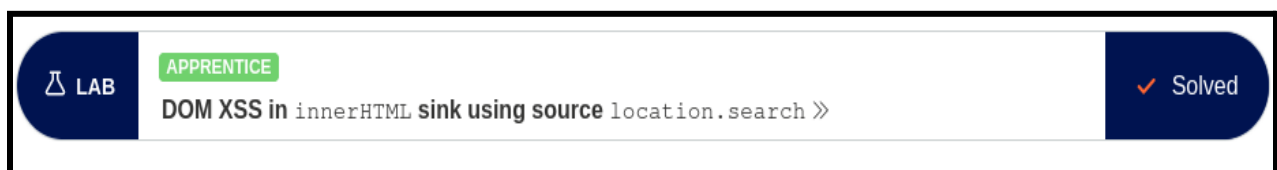
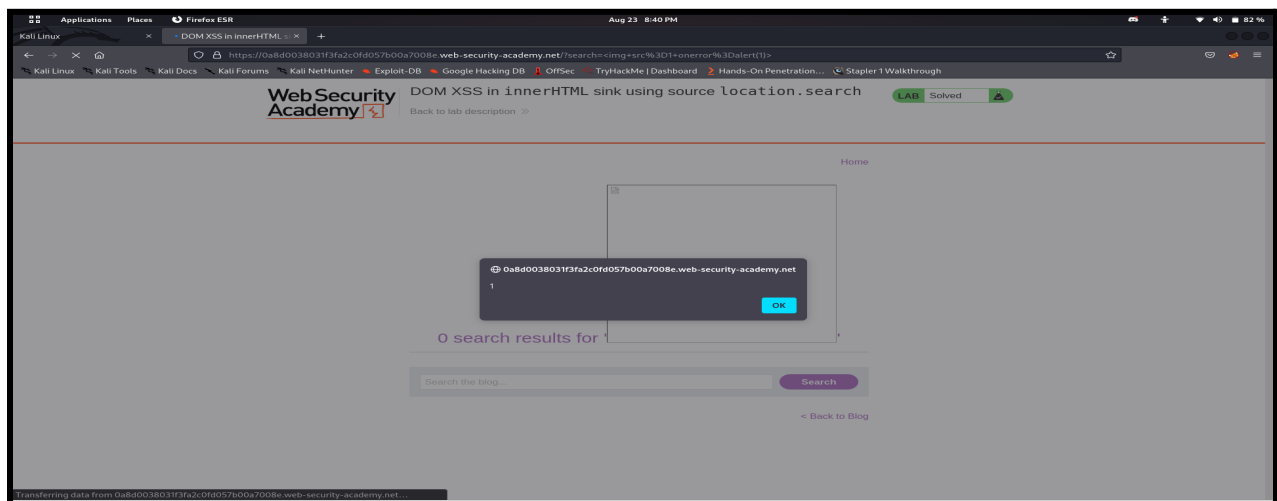
To solve this lab, perform a *cross-site scripting* attack that calls the **alert** function.



Using the Script ``



Hence after the pop up arrives the lab is completed



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

 LAB

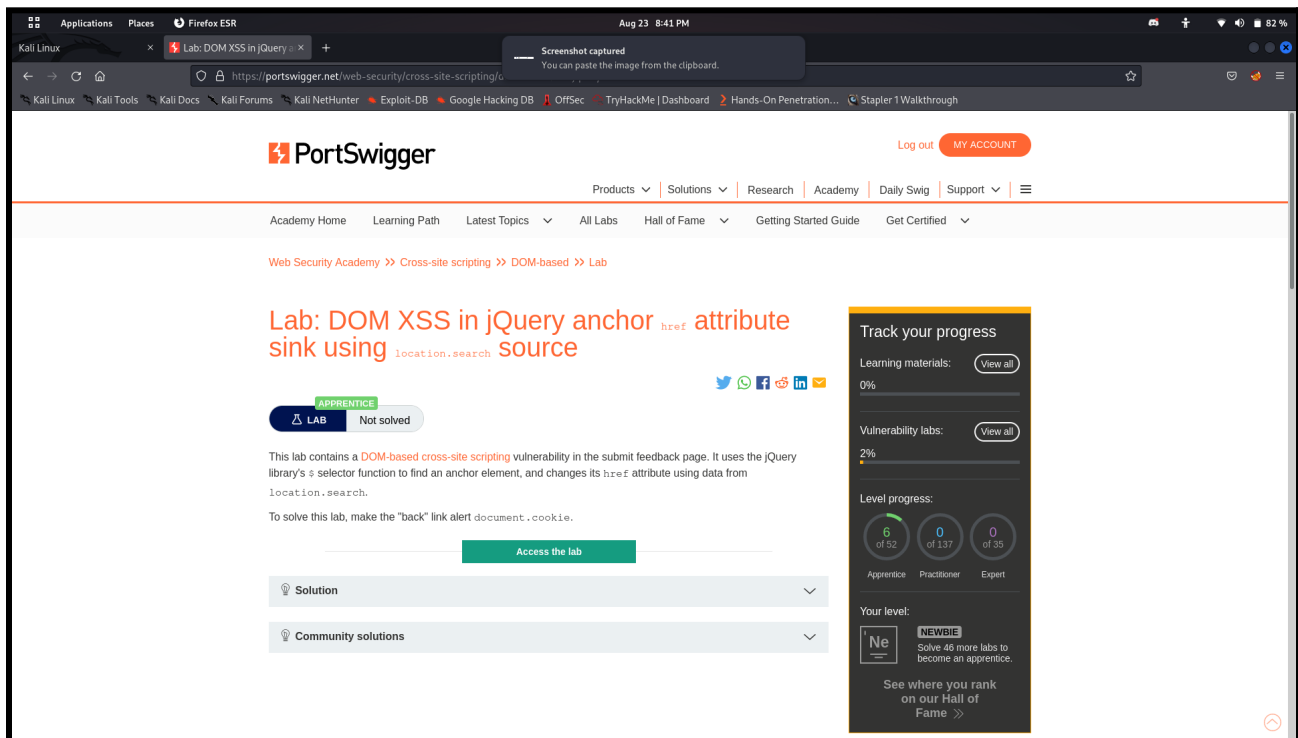
APPRENTICE

DOM XSS in jQuery anchor href attribute sink using location.search source >>

Not solved

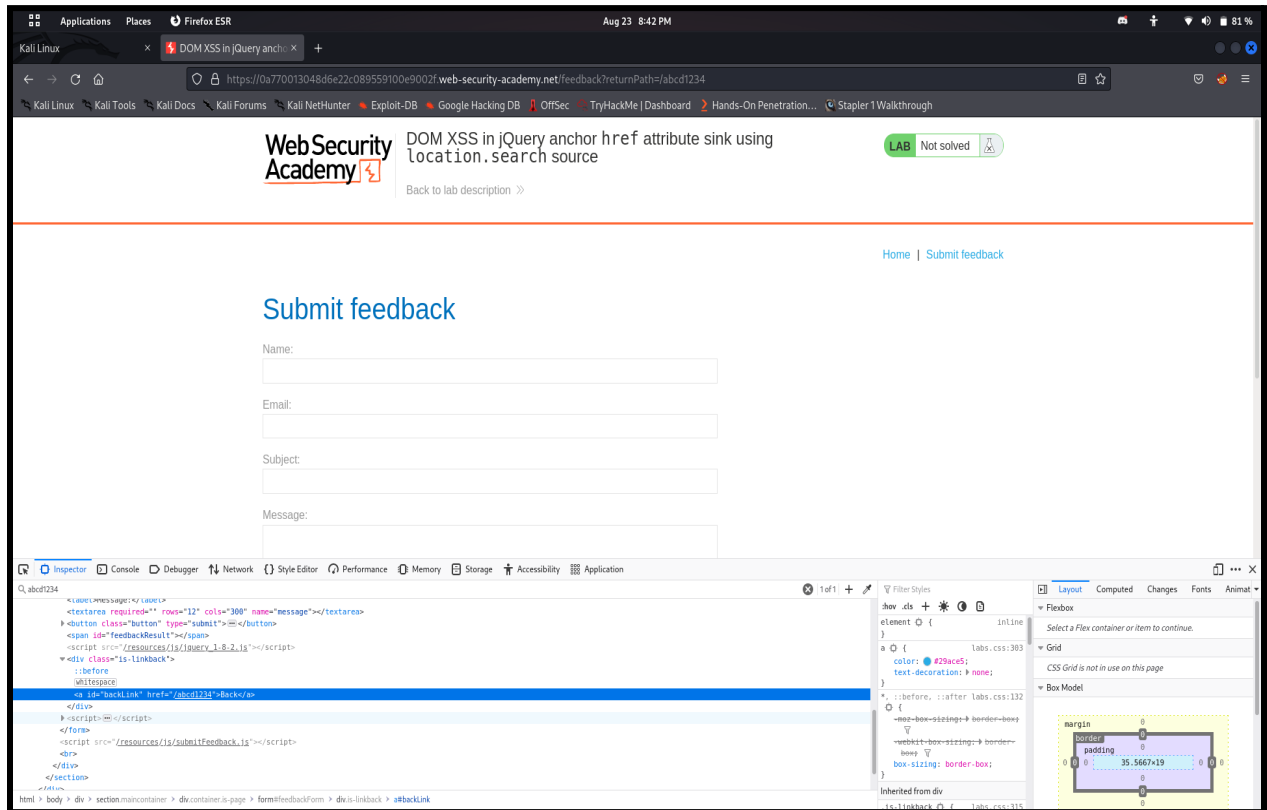
This lab contains a DOM-based cross-site scripting vulnerability in the submit feedback page. It uses the jQuery library \$ selector function to find an anchor element, and changes its href attribute using data from location.search.

To solve this lab, make the “back” link alert document.cookie.



The screenshot shows the PortSwigger Web Security Academy interface. The lab title is "Lab: DOM XSS in jQuery anchor href attribute sink using location.search source". It is categorized as "APPRENTICE" and "Not solved". The description states: "This lab contains a DOM-based cross-site scripting vulnerability in the submit feedback page. It uses the jQuery library's \$ 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." There is a green "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 (6 of 52 for Apprentice, 0 of 137 for Practitioner, 0 of 35 for Expert). The user's level is "NEWBIE" with a goal to solve 45 more labs to become an apprentice.

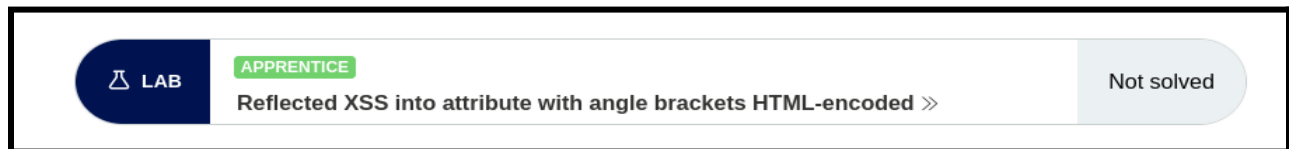
After accessing the lab inspect the page, then search abc1234



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

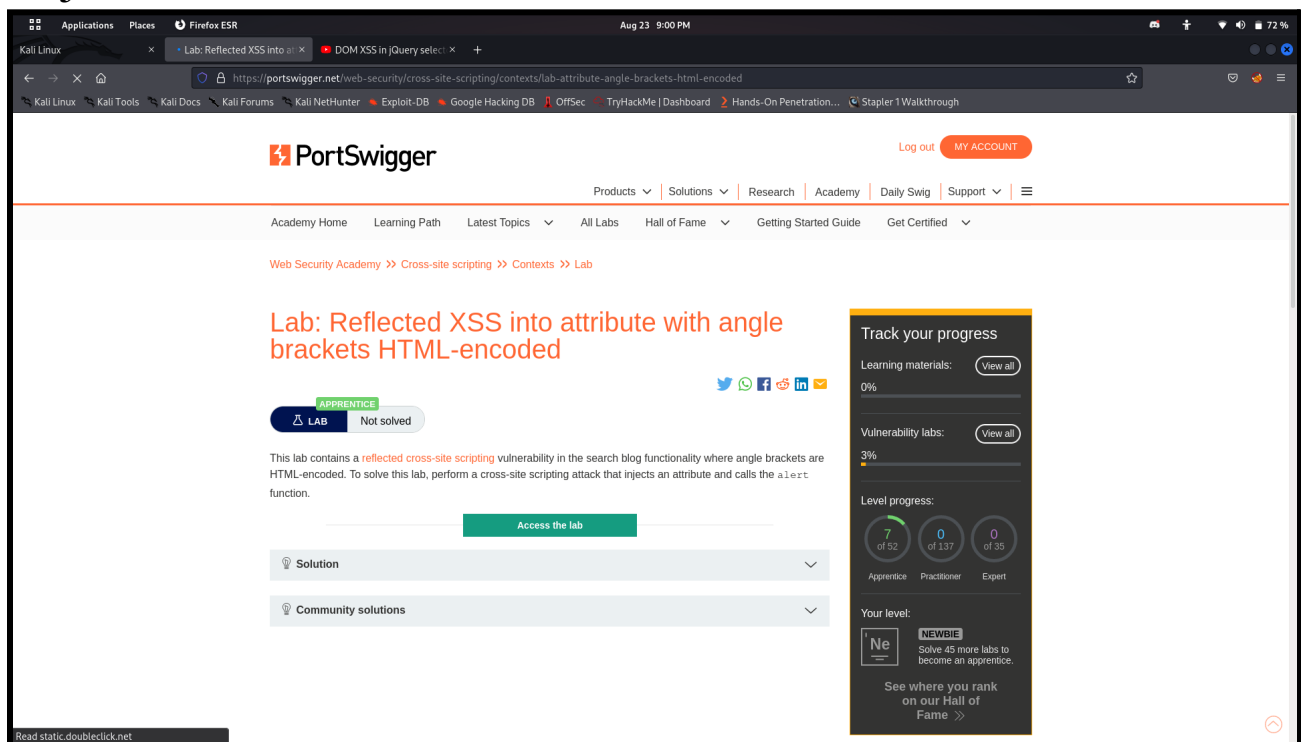


Lab 6: Reflected XSS into attribute with angle brackets HTML-encoded

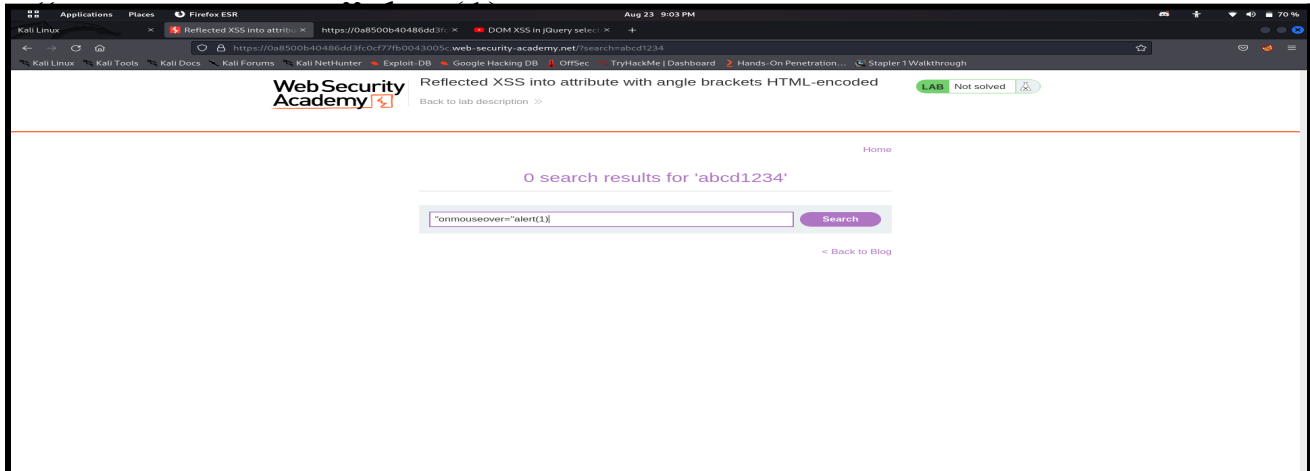


The lab contains a *reflected cross-site scripting* vulnerability in the search blog functionality where angle brackets are HTML-encoded.

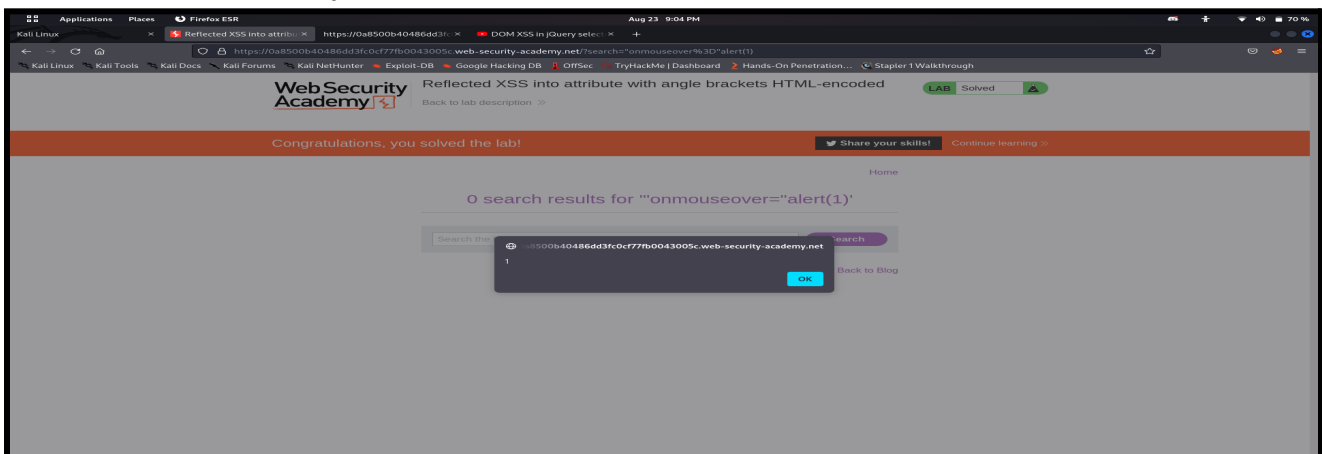
To solve this lab, perform a *cross-site scripting* attack that injects an attribute and calls the **alert** function.



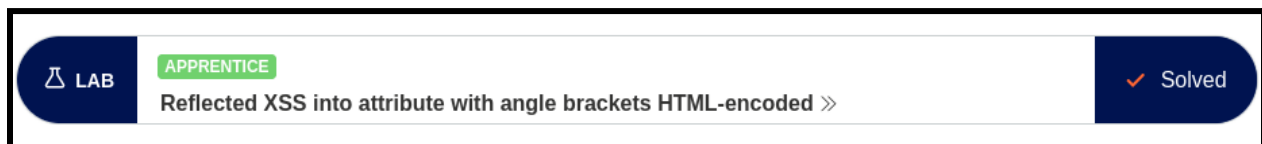
Putting the Script in the search blog functionality



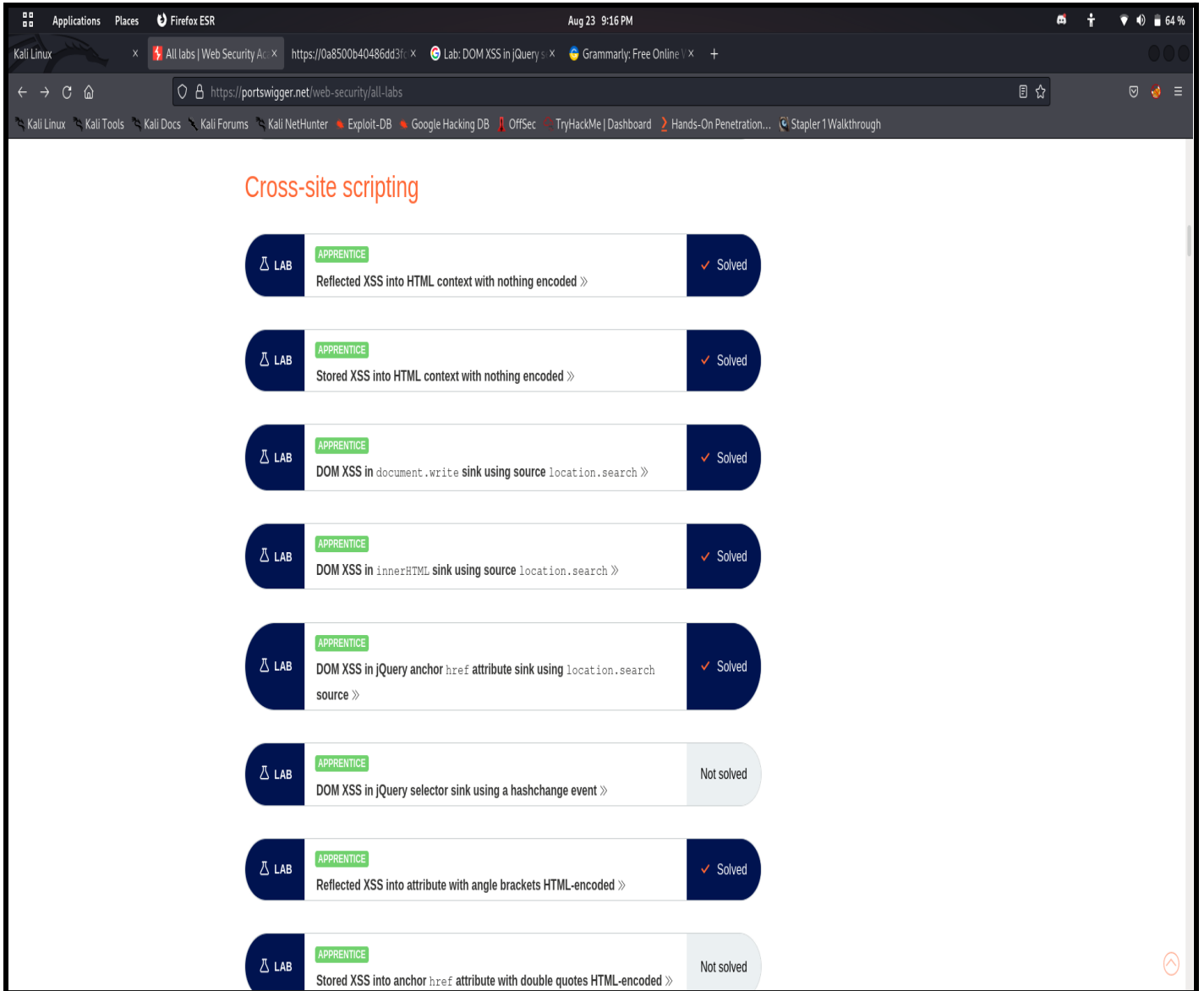
After putting in the script and pressed enter got a pop up we got the vulnerability.



Hence the lab is solved.



5 Portswigger Vulnerability Labs are Completed



The screenshot shows the Portswigger Labs interface for the 'Cross-site scripting' category. It lists 8 labs, each with a difficulty level of 'APPRENTICE'. The status of each lab is indicated by a checkmark and the word 'Solved' or 'Not solved'.

Lab ID	Difficulty	Challenge	Status
LAB	APPRENTICE	Reflected XSS into HTML context with nothing encoded »	Solved
LAB	APPRENTICE	Stored XSS into HTML context with nothing encoded »	Solved
LAB	APPRENTICE	DOM XSS in document.write sink using source location.search »	Solved
LAB	APPRENTICE	DOM XSS in innerHTML sink using source location.search »	Solved
LAB	APPRENTICE	DOM XSS in jQuery anchor href attribute sink using location.search source »	Solved
LAB	APPRENTICE	DOM XSS in jQuery selector sink using a hashchange event »	Not solved
LAB	APPRENTICE	Reflected XSS into attribute with angle brackets HTML-encoded »	Solved
LAB	APPRENTICE	Stored XSS into anchor href attribute with double quotes HTML-encoded »	Not solved