

## **ETHICAL HACKING INTERNSHIP**

**Name:** Kartik Muley

**Institutional Affiliation:** Internship Studio

**Email:** [kartikmuley28@gmail.com](mailto:kartikmuley28@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.

 LAB


APPRENTICE

Reflected XSS into HTML context with nothing encoded >>

Not 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.







 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 >> Reflected >> Lab

Lab: Reflected XSS into HTML context with nothing encoded

APPRENTICE

LAB Not 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.

Access the lab

Solution

Community solutions

Track your progress

Learning materials: View all

0%

Vulnerability labs: View all

0%

Level progress:

2 of 52

0 of 137

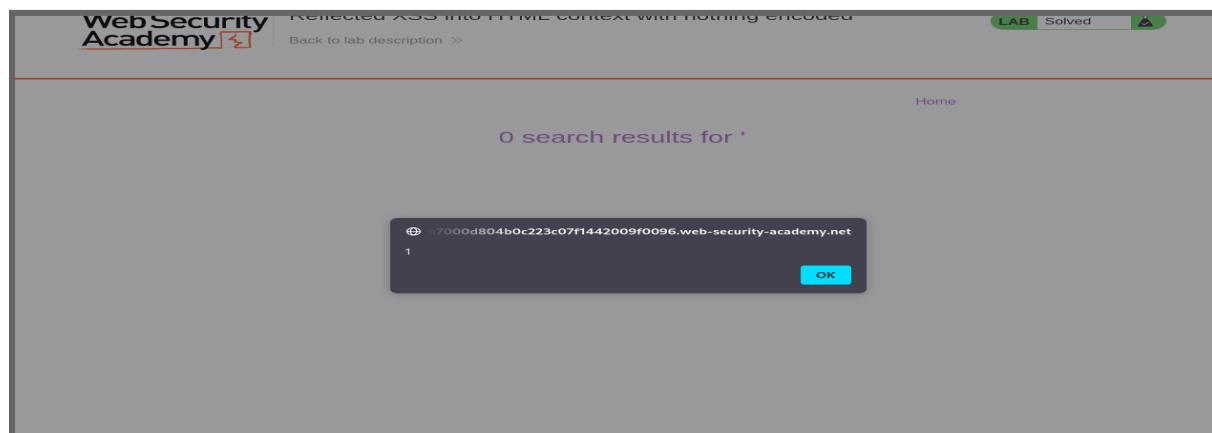
0 of 35

Apprentice Practitioner Expert

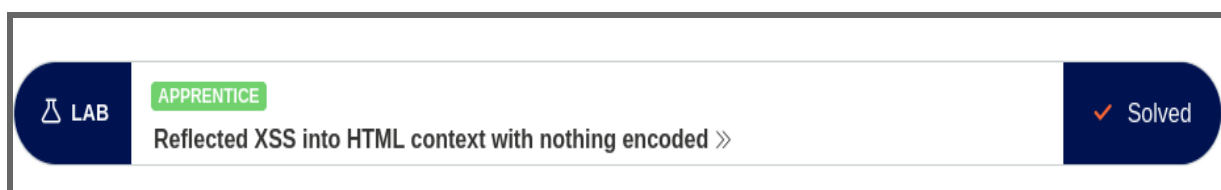
Your level:

NEWBIE

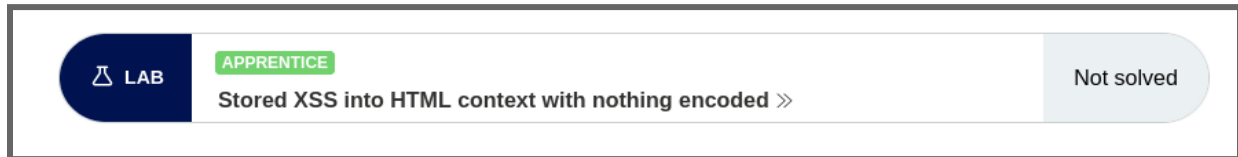
Using the script `<script>alert(1)</script>` we got a pop up.



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

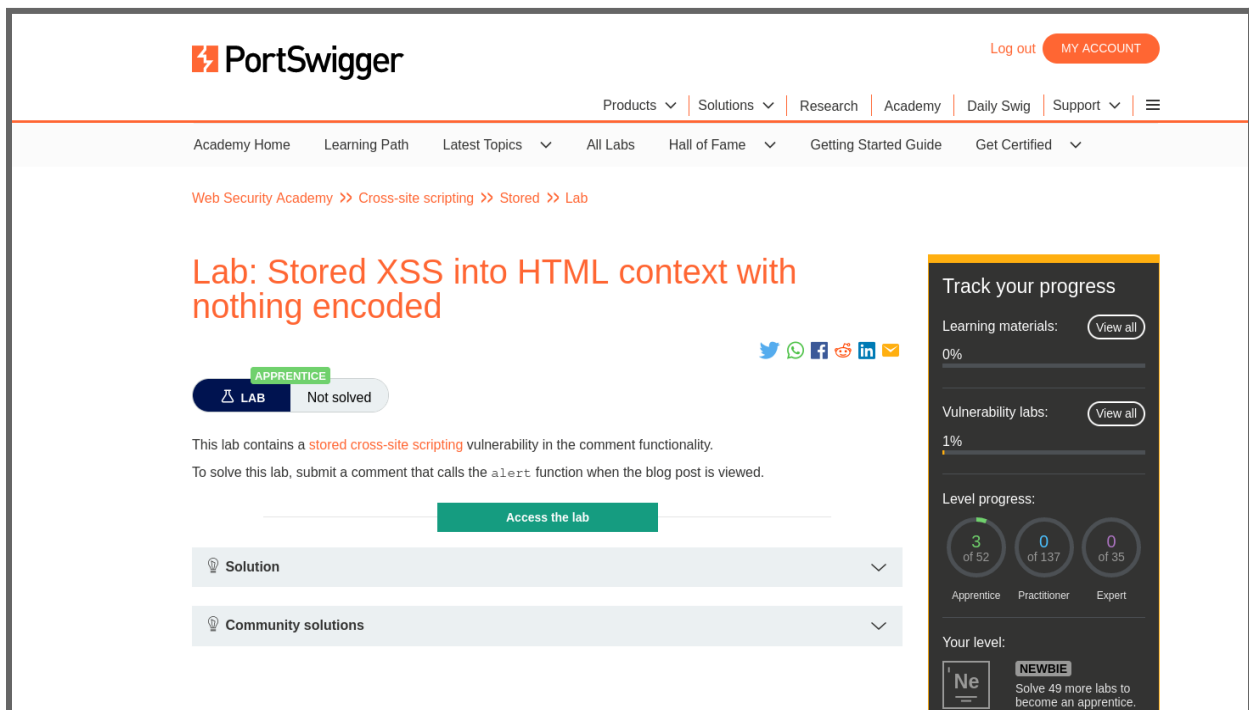


## Lab 2: Stored XSS into HTML context with nothing encoded.



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 Academy lab page. The page has a white header with the PortSwigger logo on the left and 'Log out' and 'MY ACCOUNT' on the right. Below the header is a navigation bar with links: Products, Solutions, Research, Academy, Daily Swig, and Support. The main content area has a breadcrumb trail: 'Web Security Academy >> Cross-site scripting >> Stored >> Lab'. The lab title is 'Lab: Stored XSS into HTML context with nothing encoded'. Below the title is a green badge with 'APPRENTICE' and a button with 'LAB' and 'Not solved'. The lab 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 is a green button labeled 'Access the lab'. Below this are two expandable sections: 'Solution' and 'Community solutions'. On the right side of the page is a dark sidebar titled 'Track your progress'. It shows progress for '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, it shows 'Your level: NEWBIE' and a goal to '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>`

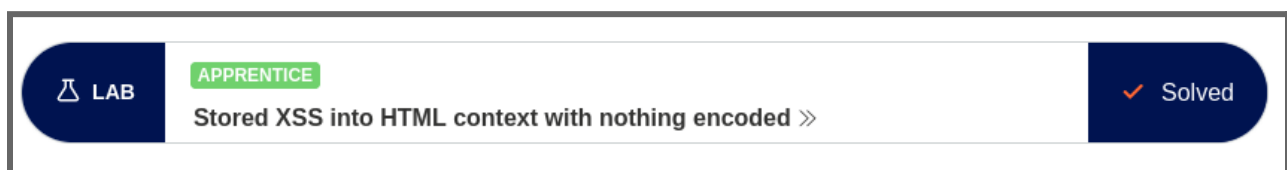
Name:  
Kalyani

Email:  
Kalyanilnkar5@gmail.com

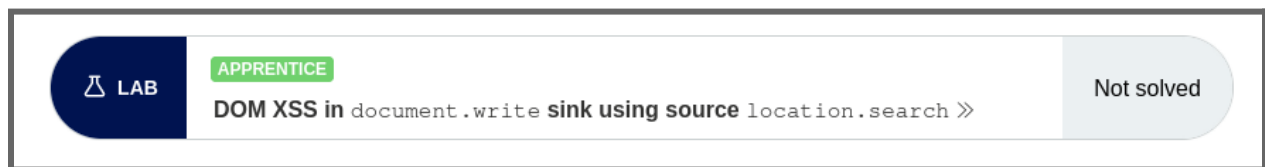
Website:  
https://google.com

Post Comment

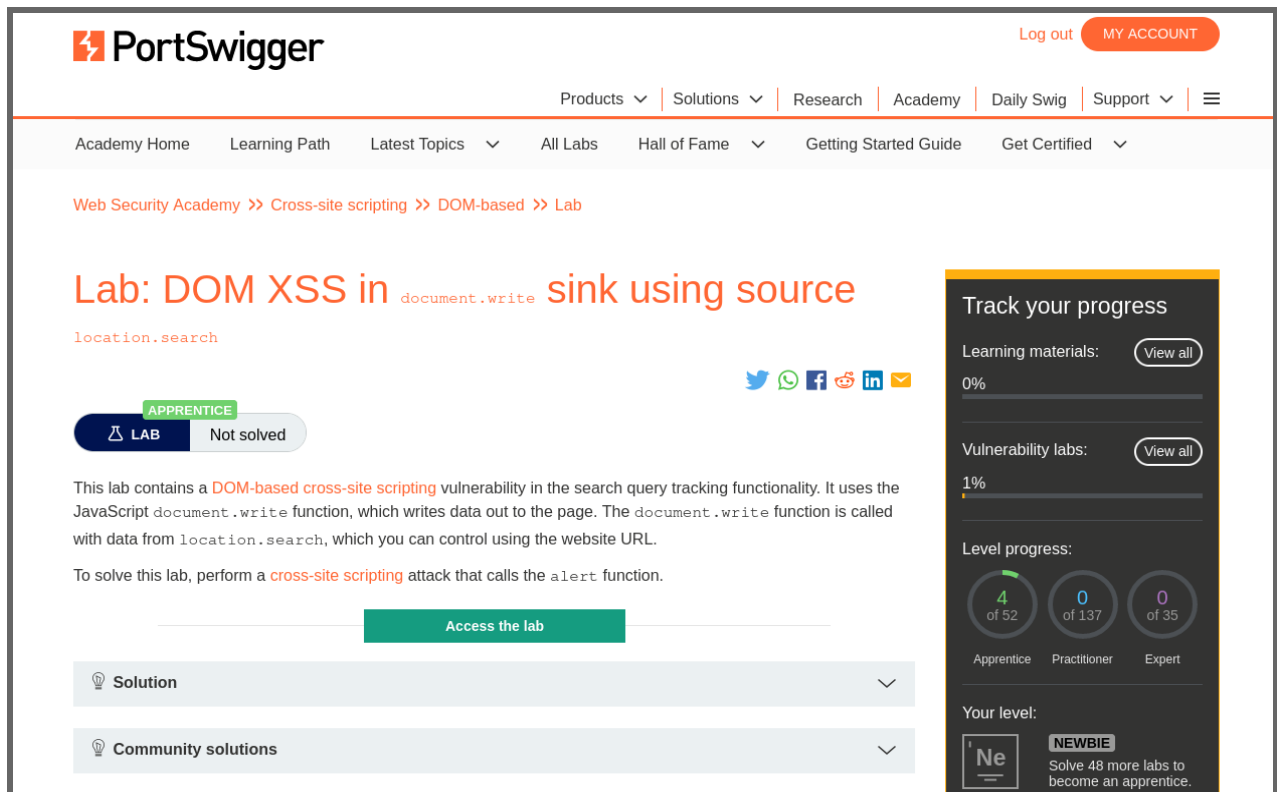
Hence we have completed the Lab.



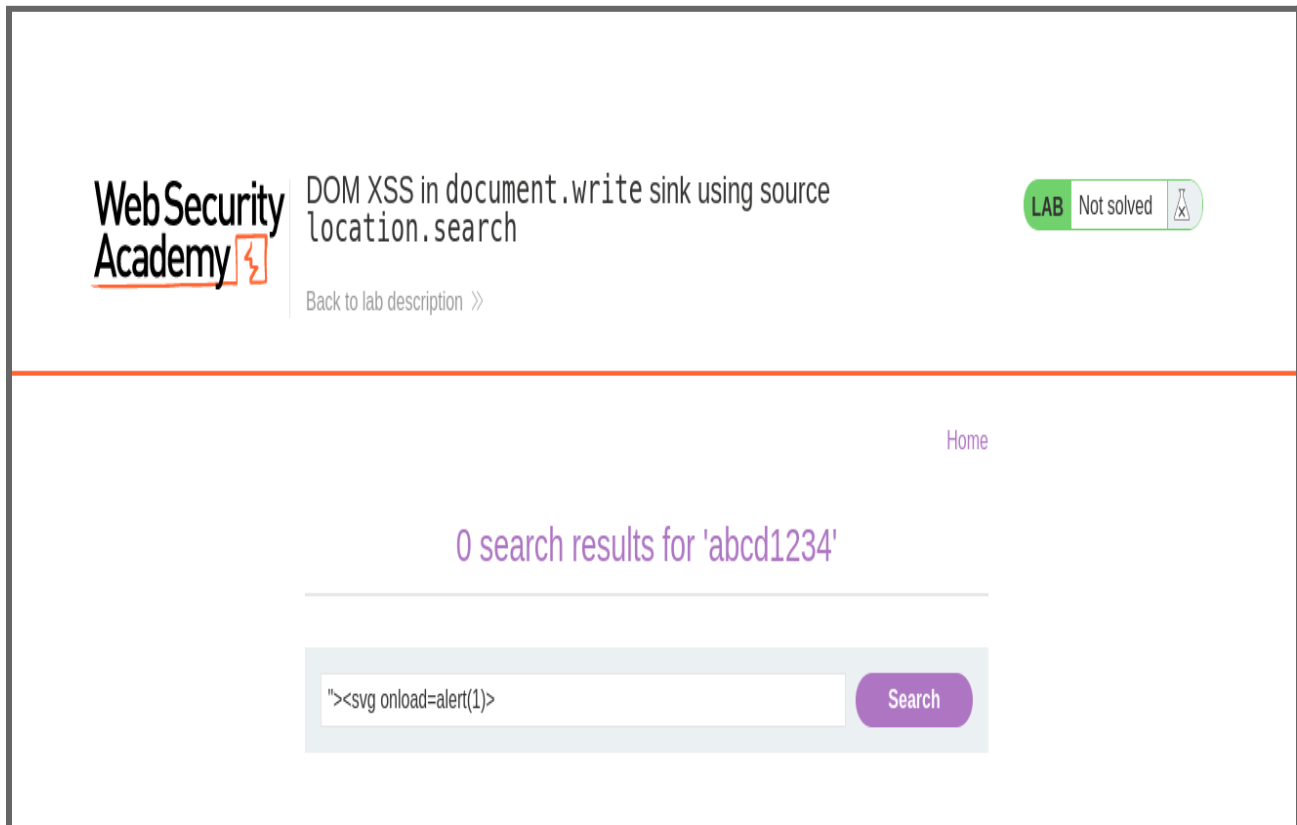
## Lab 3: DOM XSS document.write sink using source location.search



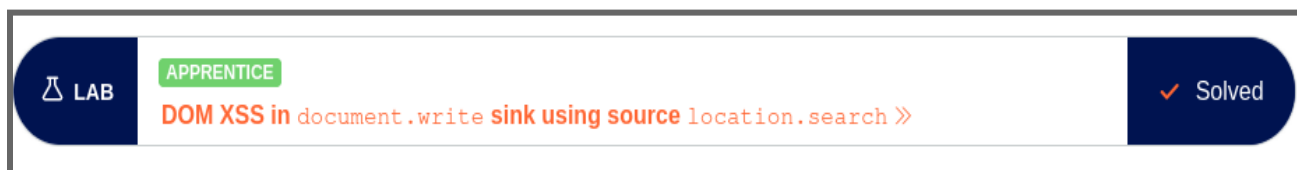
This lab contains a *DOM-based cross-site scripting* vulnerability in the search query tracking functionality. It uses the JavaScript **document.write** function, which writes data out to the page. The document.write function is called with data from **location.search**, which you can control using the website URL. To solve this lab, perform a *cross-site scripting* attack that calls the **alert** function.

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

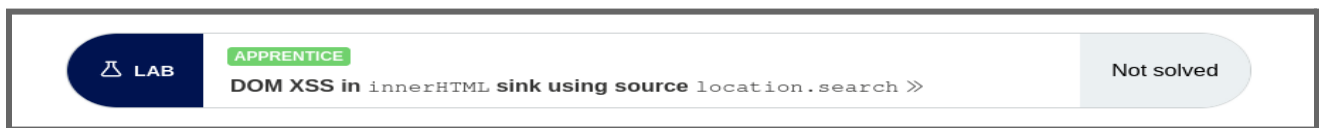
Performing a cross-site scripting attack that calls the alert function.



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

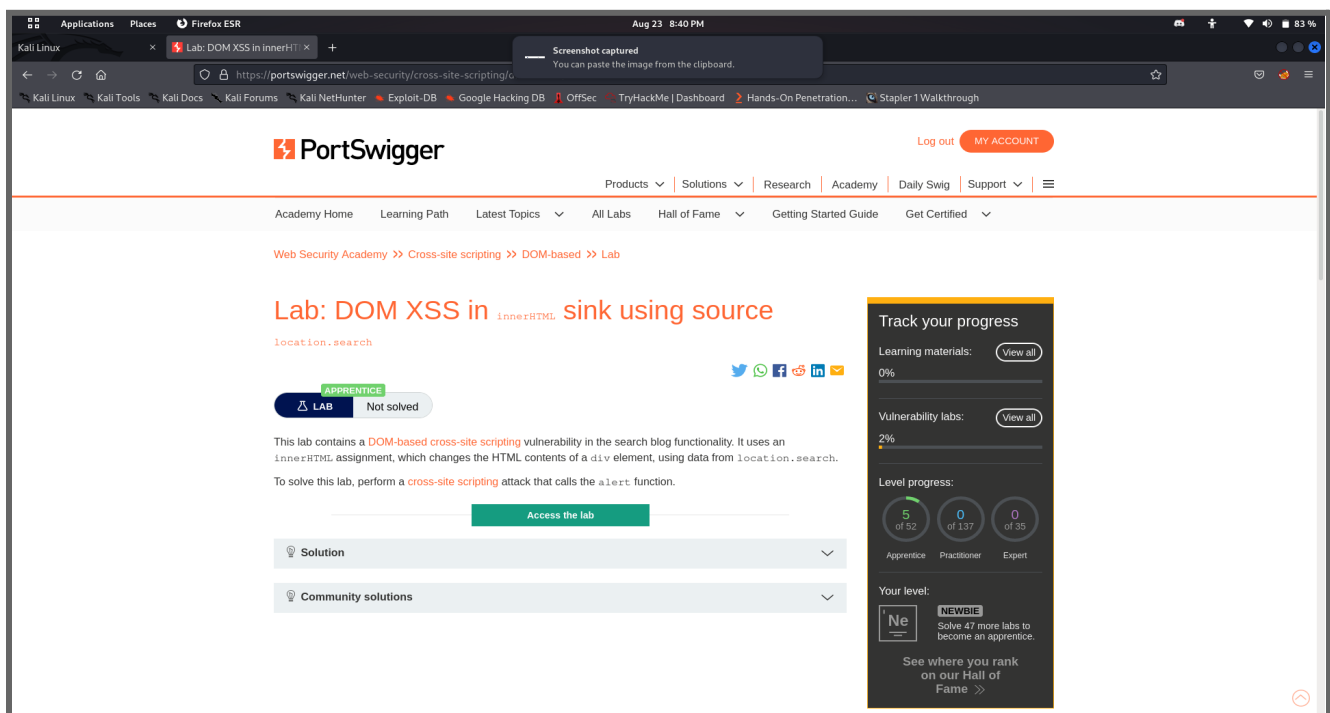


## Lab 4: DOM XSS in innerHTML sink using source location.search



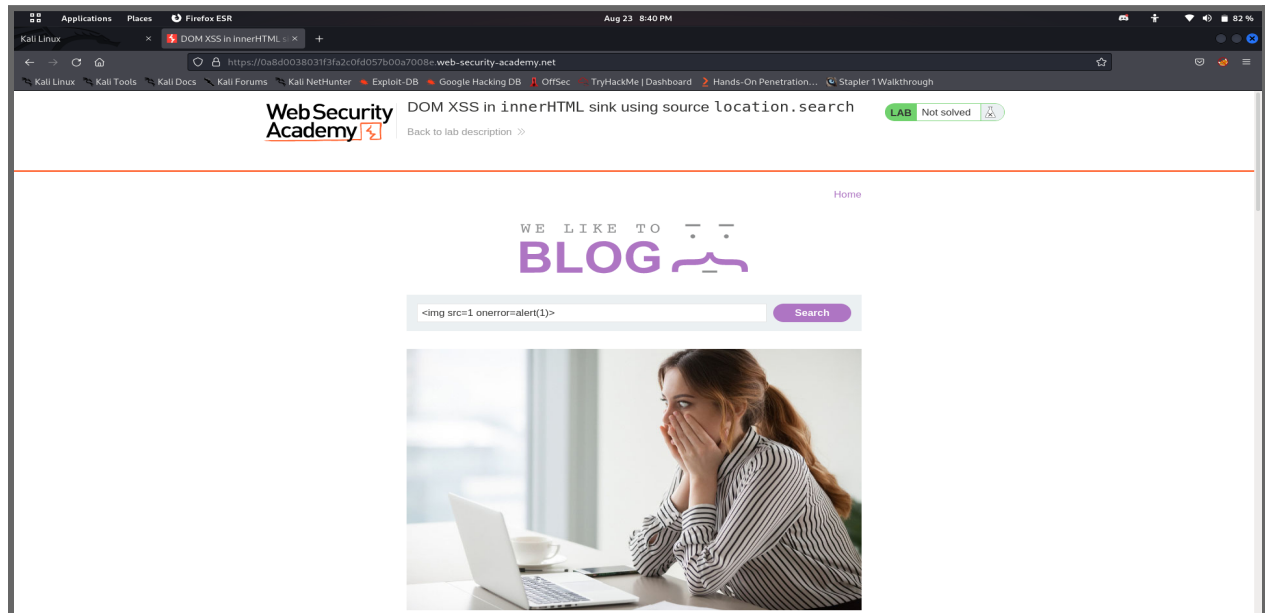
This lab contains a *DOM-based cross-site scripting* vulnerability in the search blog functionality. It uses an innerHTML assignment, which changes the HTML contents of a div element, using data from location.search.

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

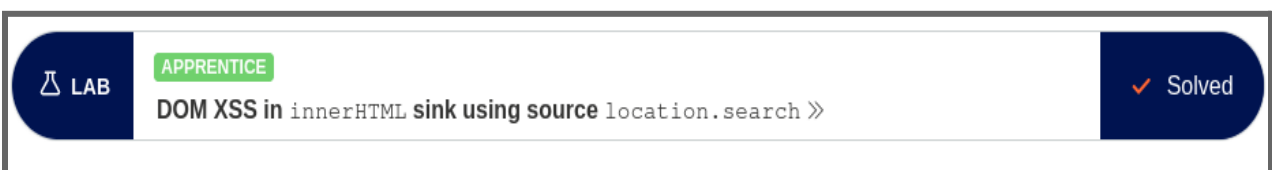
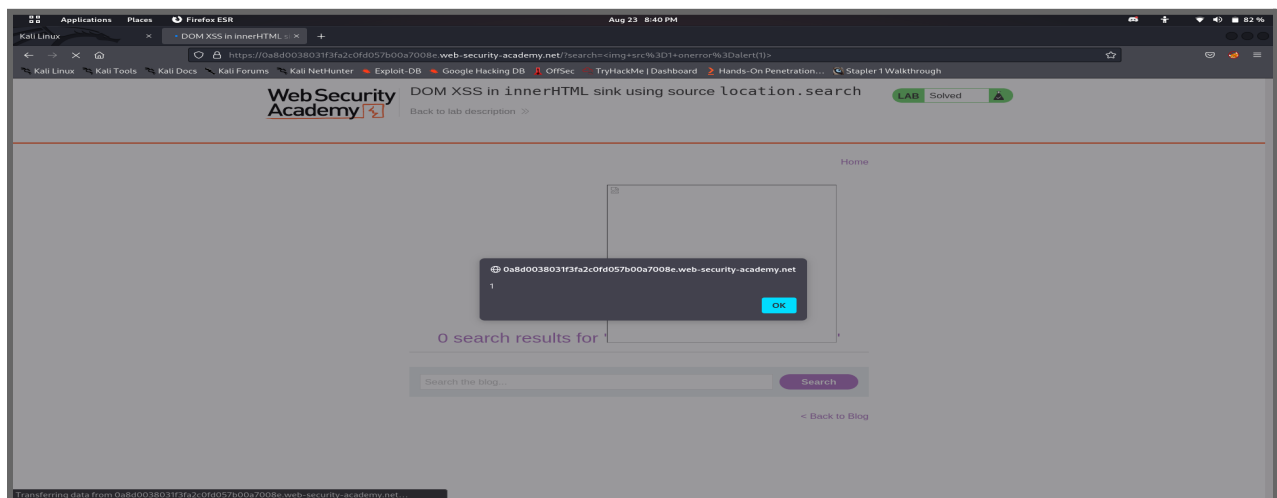




Using the Script `<img src=1 onerror=alert(1)>`



Hence after the pop up arrives the lab is completed



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

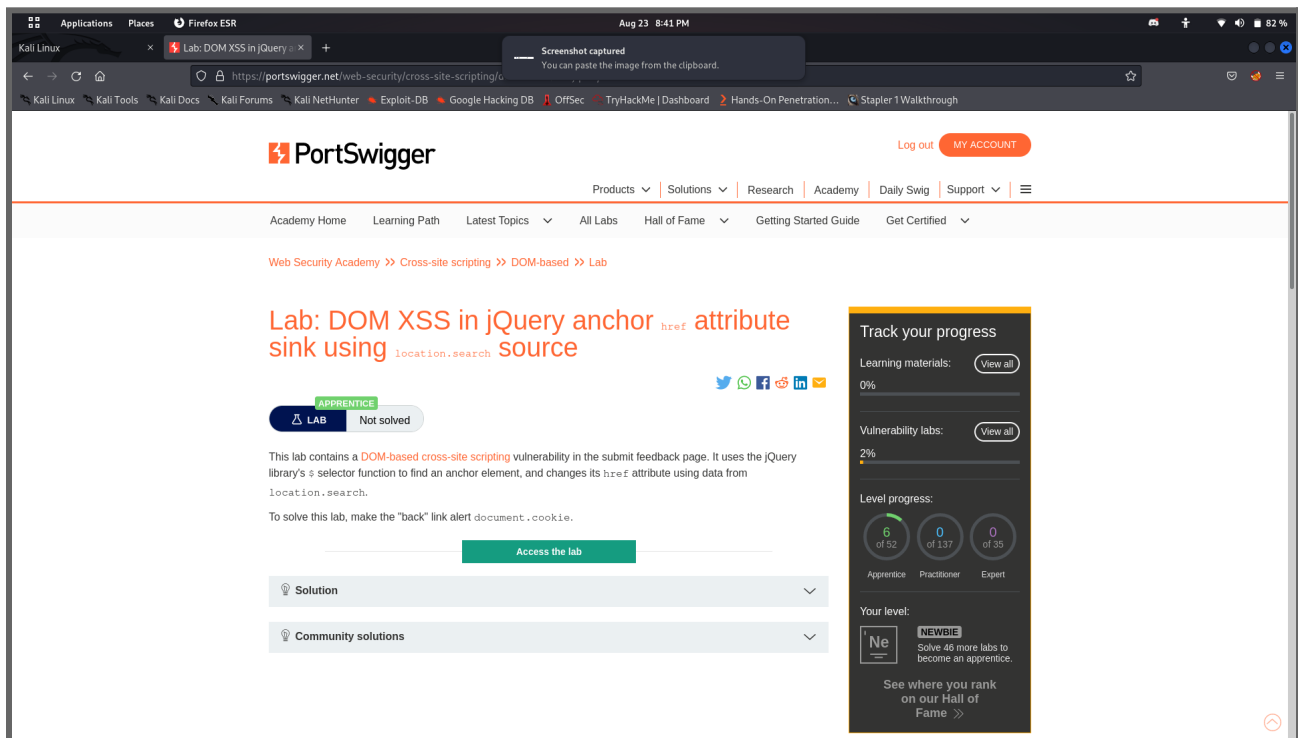
 LAB

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

Not solved

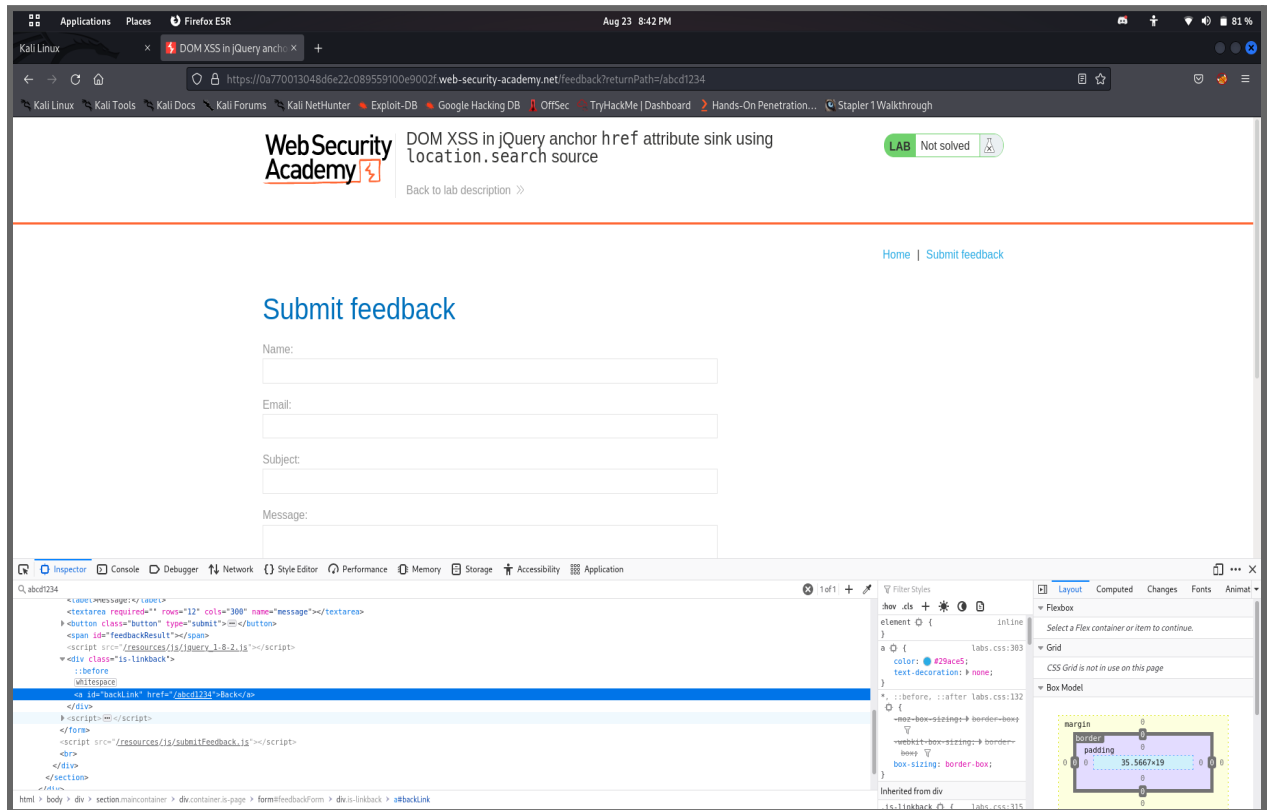
This lab contains a DOM-based cross-site scripting vulnerability in the submit feedback page. It uses the jQuery library \$ selector function to find an anchor element, and changes its href attribute using data from location.search.

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

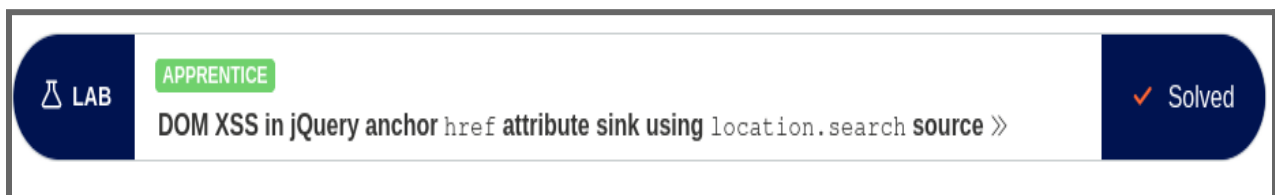


The screenshot shows the PortSwigger Web Security Academy interface. The lab title is "Lab: DOM XSS in jQuery anchor href attribute sink using location.search source". It is categorized as "APPRENTICE" and "Not solved". The description states: "This lab contains a DOM-based cross-site scripting vulnerability 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 button labeled "Access the lab". 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 92 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.

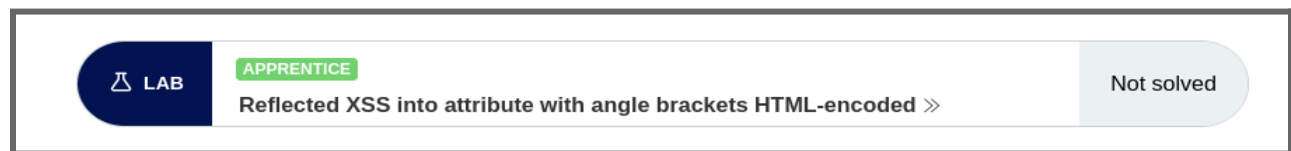
After accessing the lab inspect the page, then search abc1234



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

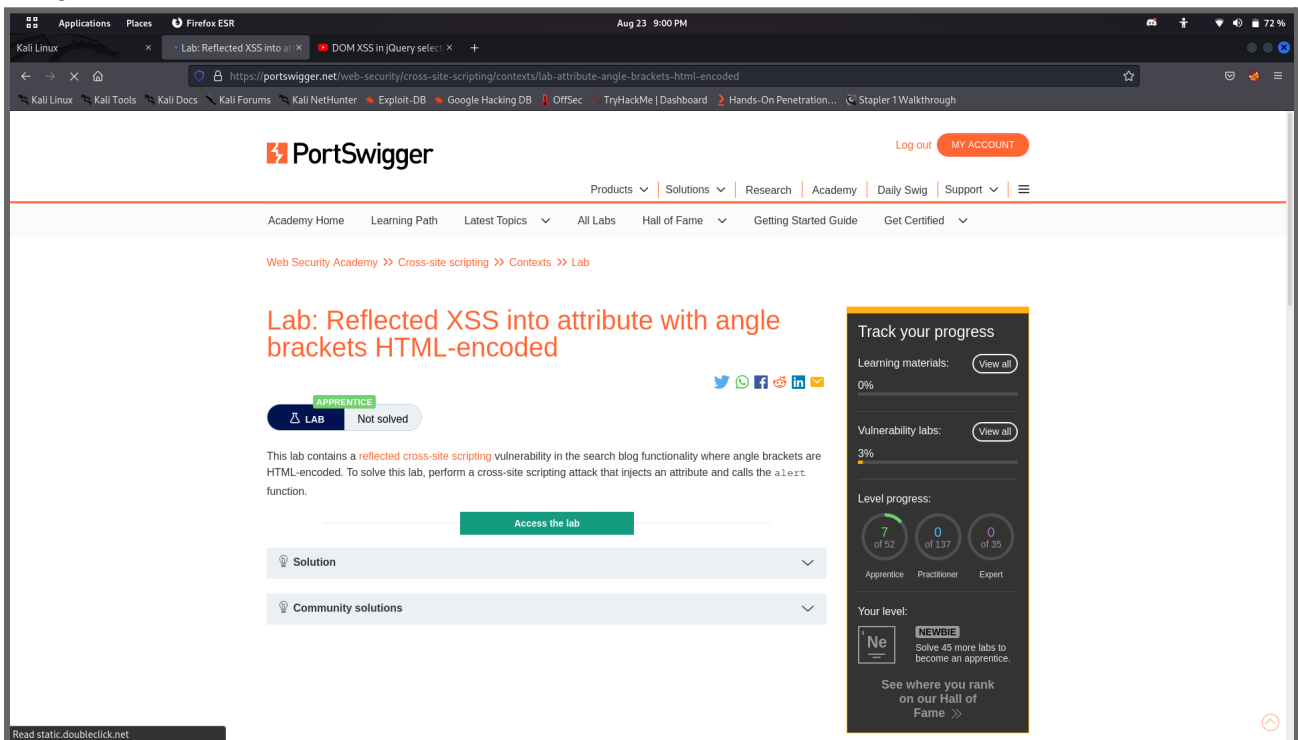


## Lab 6: Reflected XSS into attribute with angle brackets HTML-encoded

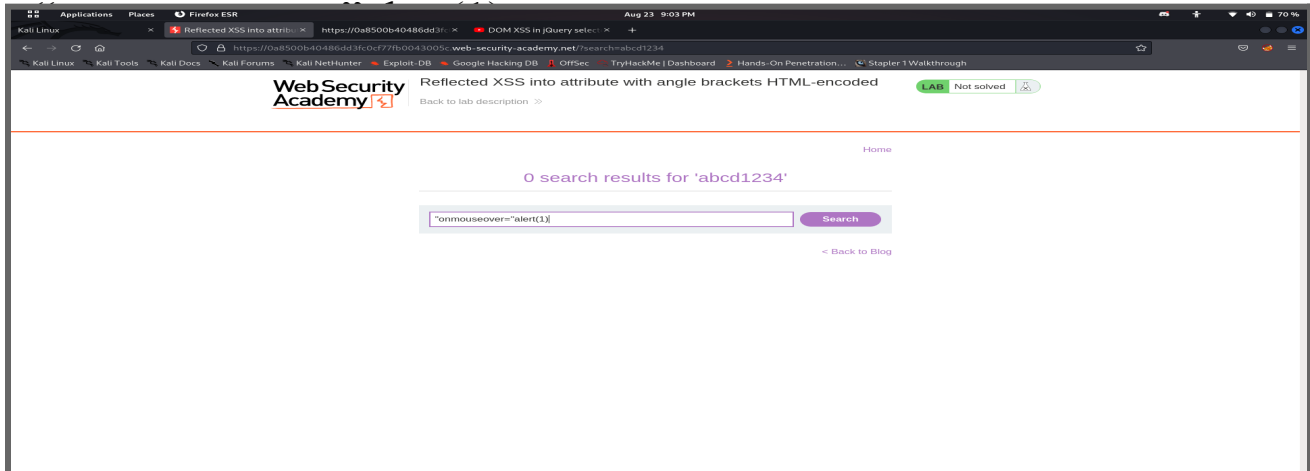


The lab contains a *reflected cross-site scripting* vulnerability in the search blog functionality where angle brackets are HTML-encoded.

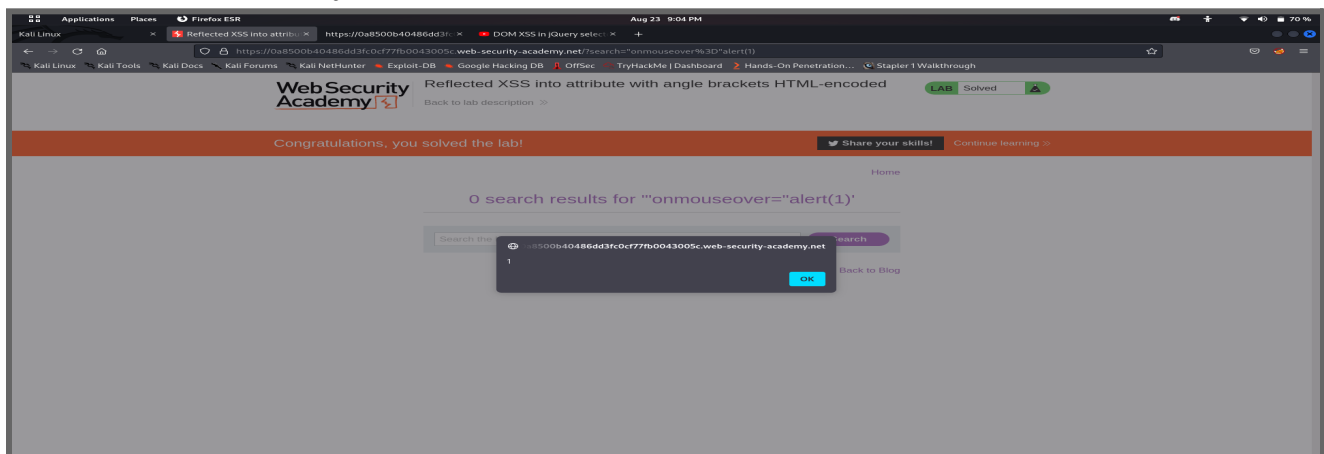
To solve this lab, perform a *cross-site scripting* attack that injects an attribute and calls the **alert** function.

A screenshot of a web browser displaying the PortSwigger Academy interface. The browser's address bar shows the URL: https://portswigger.net/web-security/cross-site-scripting/contexts/lab-attribute-angle-brackets-html-encoded. The page title is 'Lab: Reflected XSS into attribute with angle brackets HTML-encoded'. Below the title, there is a green 'APPRENTICE' tag and a 'LAB' button. A description states: 'This 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.' A green 'Access the lab' button is visible. On the right, a 'Track your progress' sidebar shows: 'Learning materials: 0% (View all)', 'Vulnerability labs: 3% (View all)', and 'Level progress: 7 of 52 (Apprentice), 0 of 137 (Practitioner), 0 of 35 (Expert)'. It also indicates 'Your level: NEWBIE' and 'Solve 45 more labs to become an apprentice.' The bottom left of the browser shows a 'Read static.doubleclick.net' message.

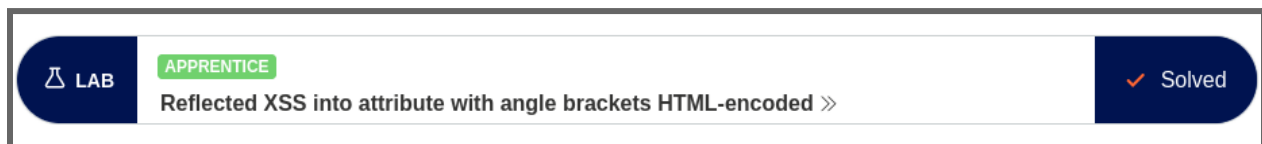
## Putting the Script in the search blog functionality



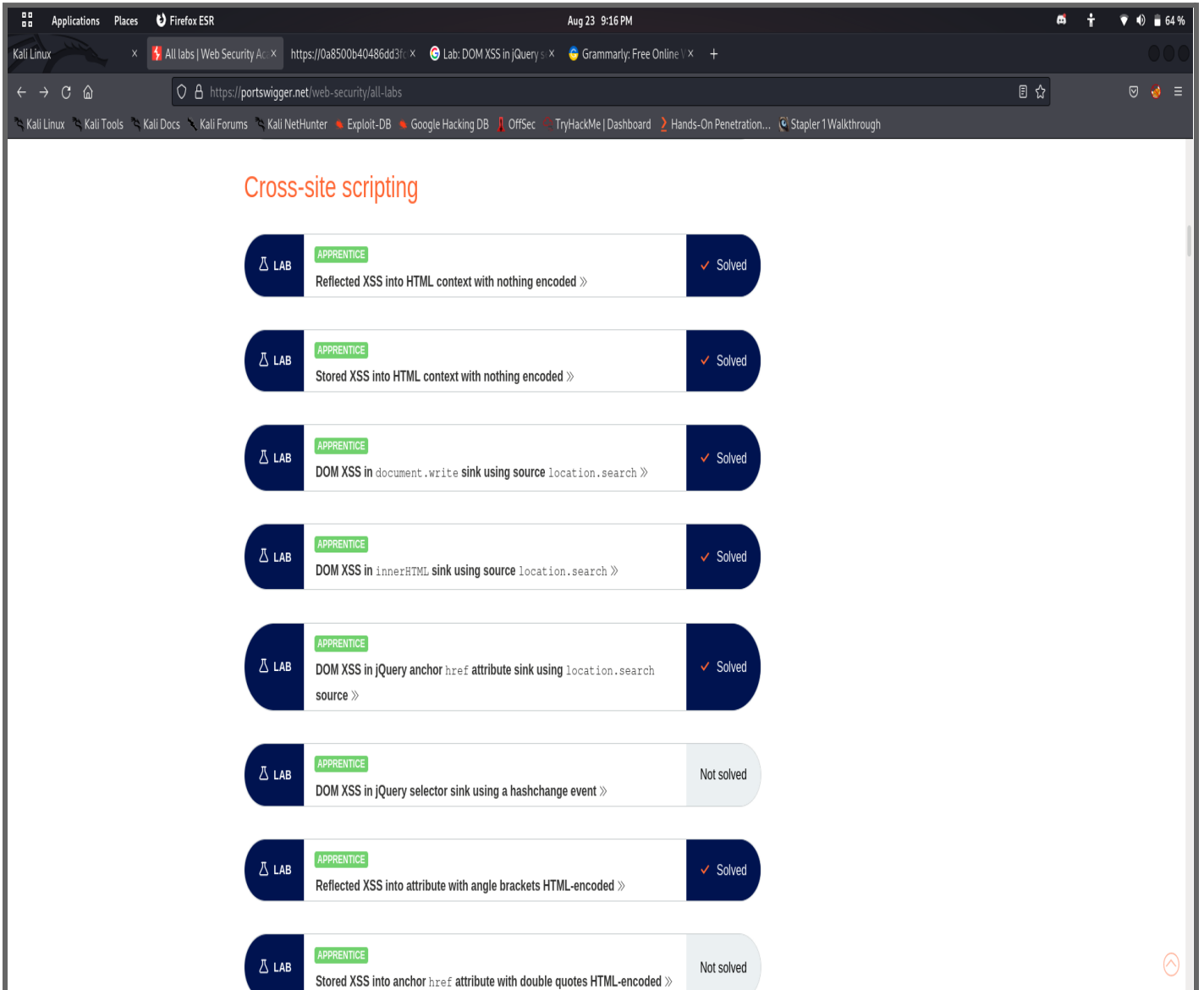
After putting in the script and pressed enter got a pop up we got the vulnerability.



Hence the lab is solved.



## 5 Portswigger Vulnerability Labs are Completed



The screenshot shows the Portswigger Labs interface for Cross-site scripting (XSS) challenges. The browser window displays the URL <https://portswigger.net/web-security/all-labs>. The page title is "Cross-site scripting". There are 8 labs listed, 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	Description	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