Lab name: [DOM XSS in innerHTML sink using source location.search](https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-innerhtml-sink)

Severity: High

Lab description:

* DOM based XSS happens when the Java script updates the page using data from sources like location, document, or window without proper encoding or validation.
* This lab focuses on the vulnerable *innerHTML* tag that fetches data from untrusted sources using *location. search*.

Impact:

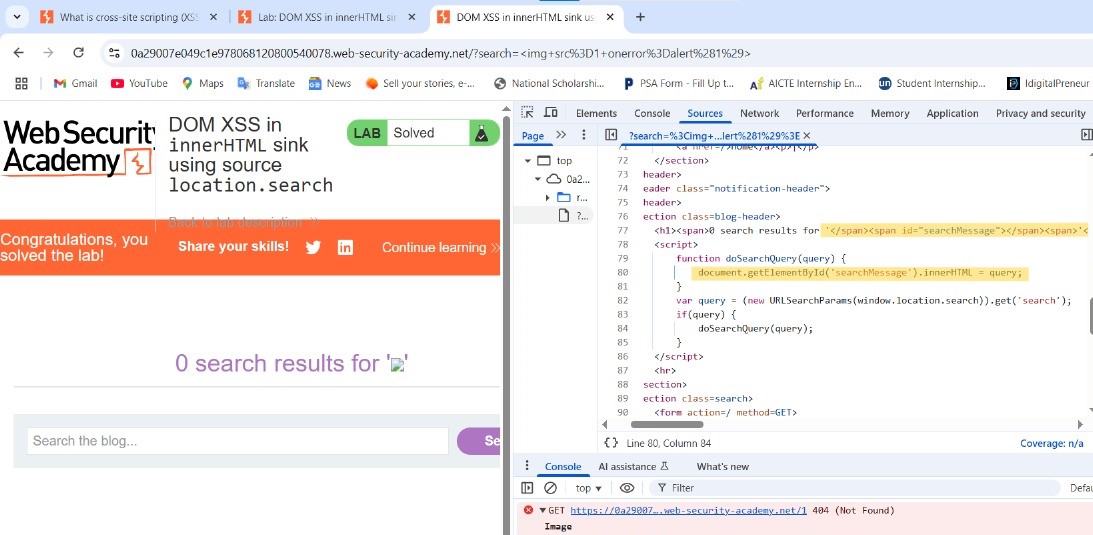
* Theft of session cookies, local Storage data or sensitive information.
* The attackers can manipulate users to redirect to some other vulnerable websites revealing their identity or other confidential information.
* This innerHTML normally retrieves whatever information is put on HTML, this might lead to unauthorized actions also.
* Account hijacks can also happen

Recommendations:

* Do not use innerHTML tags to retrieve data from the input or from any other untrusted resources, instead developers can use textContent or innerText.
* Sanitize and validate all the inputs from the URL before executing it.
* Implement content security policy to restrict any kind of harmful scripts
* Usage of security tools and libraries will help in avoiding the special characters.

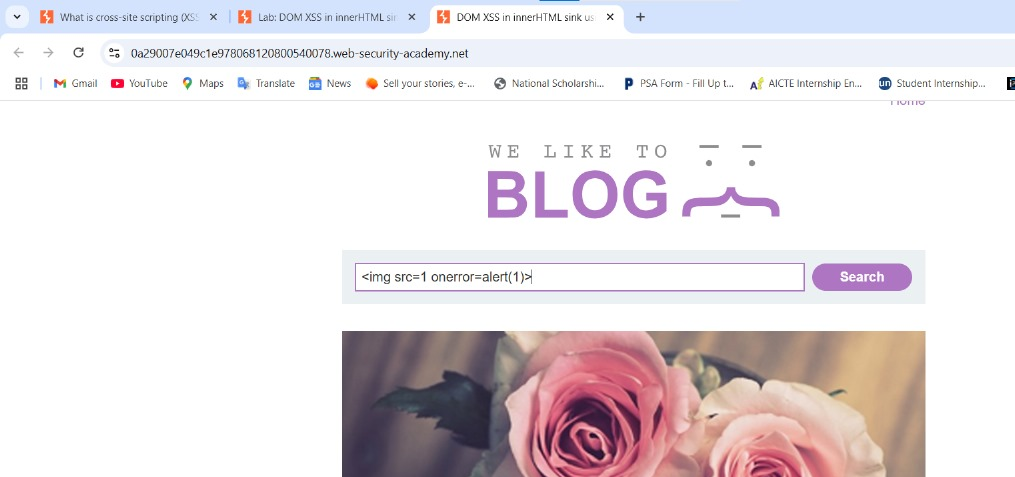
Steps to reproduce:

1. Access the lab and intercept requests using burp suite.
2. When the page is inspected it is found that there is usage of innerHTML tag which retrieves all the query as the heading or a span element within heading tag.



1. Insert an alert script into the search box,

*<img src=1 onerror=alert(1)>*



1. Now click on search, there is an alert pop-up.
2. Thus, the lab is solved by finding the innerHTML vulnerability.