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

Severity: High

Lab description:

* In this lab, the application uses the location.search() and fetches data directly using the document.write(), it is a vulnerability because attacker can easily inject HTML or scripts and execute it.
* Simple modifications in the URL also can lead to a significant attack.

Impact:

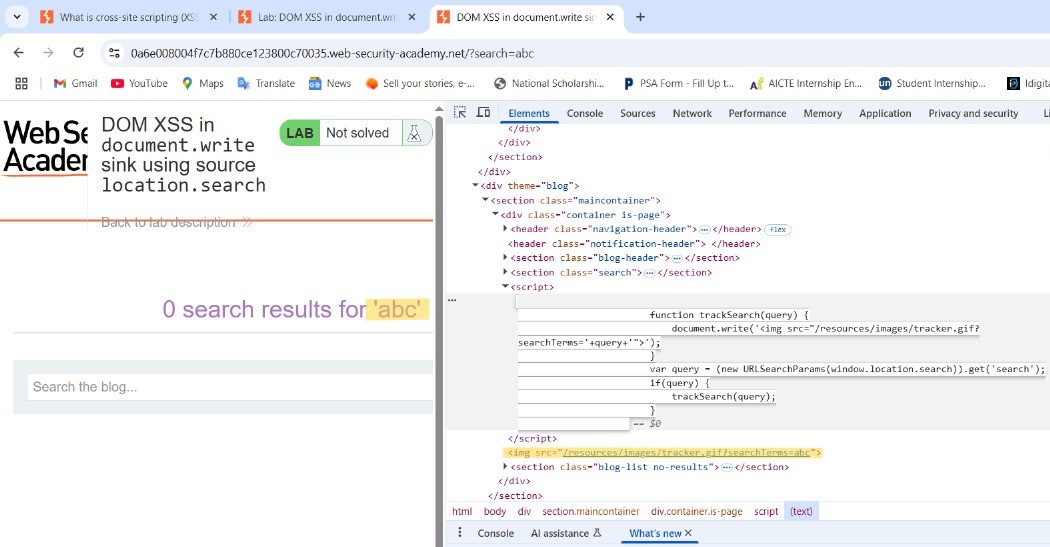
* Attackers can steal data, steal sessions, redirect the victims, perform actions on behalf of victims, phishing attacks, etc.
* This affects confidentiality, so the severity is high.

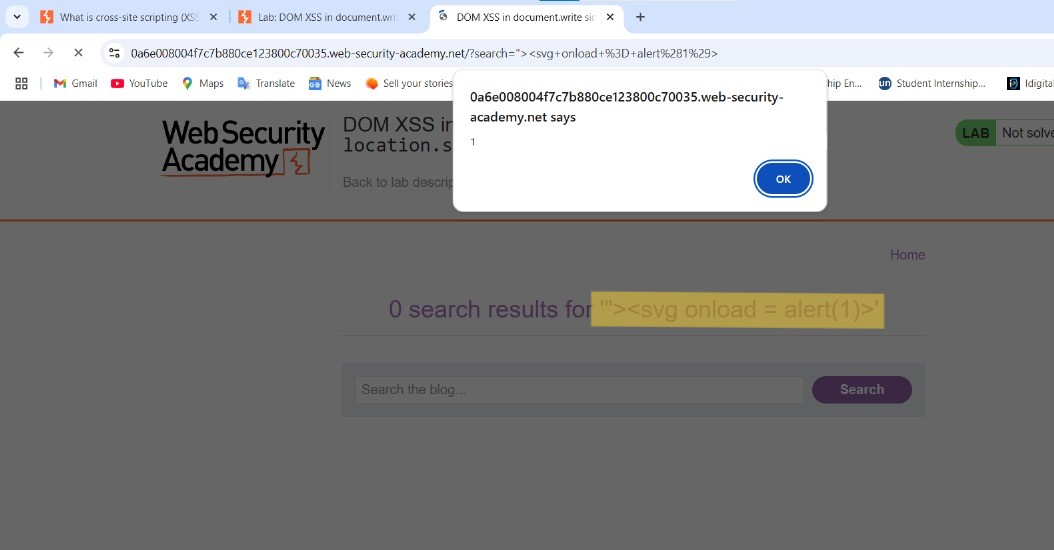
Recommendations:

* Avoid using *document.write()* to display anything, instead usage of textContent() or DOM APIs will be safer methods.
* Escape or sanitize the untrusted input.
* Validate URL parameters like, accepting only expected patterns of input.
* Use security headers like content security policy to limit script execution.

Steps to reproduce:

1. Access the lab along with burpsuite.
2. In the search box, search give input with alphanumeric characters.
3. When inspecting the page, it is understood that the string that is searched is stored in an image src attribute.



1. Now, inject a script with a double quote and that can be executed.  
   *“><svg onload=alert(1)>*
2. Now the location.search() fetches this script and executes leading the victim to a pop-up message.

