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

Severity: High

Lab description:

* This lab describes about the DOM-XSS vulnerability where the javascript code takes part in the URL allowing attackers to manipulate the href attribute of the link using jQuery.
* The website takes data from untrusted sources and implies in the anchor part of the URL using location.search

Impact:

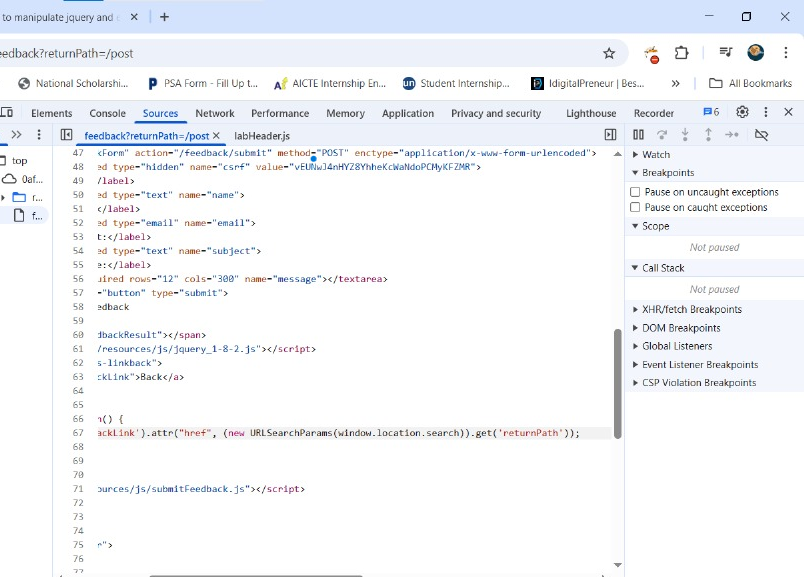
* The attacker can add a malicious link or any scripts to the page using the URL.
* There can happen cookies stealing, session hijacks and dangerous redirections which attacker might have setup.
* The attacker can manipulate users to do malicious activities.

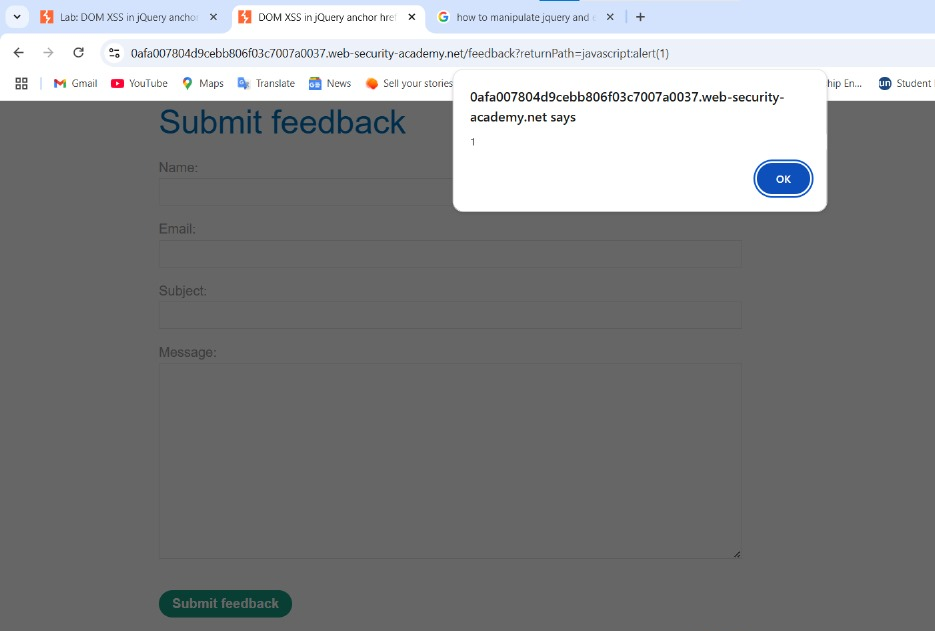
Recommendations:

* Do not directly use *location.search* in parts of the page like *href* or *HTML* or *src.*
* validate and sanitize the inputs before rendering it.
* Avoid inputs from untrusted resources. For example, in jQuery,  
  *$(‘#backLink’), .attr (“href”, .get(‘returnPath’))* these queries will set href to whatever the ‘.get(‘returnPath’) refers to.
* Use DOMPurify libraries to sanitize the input.
* Enable content security policy to block inline scripts.

Steps to reproduce:

1. Access the lab
2. Change the end point to *returnPath=javascript:alert(1)*. Here we are trying to inject script inside the URL.





1. Now, when the *back* button is clicked or hovered over the button, the alert message is popped up.
2. Thus, lab is solved.