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

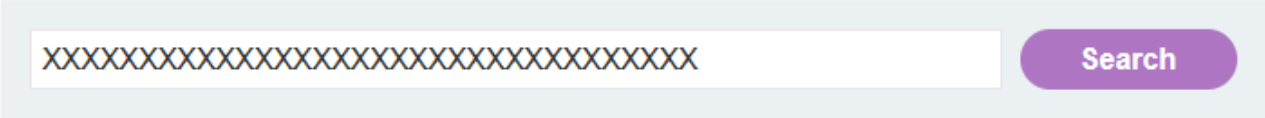
This lab contains a DOM-based cross-site scripting vulnerability in the search query tracking functionality. It uses the JavaScript `document.write` function, which writes data out to the page. The `document.write` function is called with data from `location.search`, which you can control using the website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

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

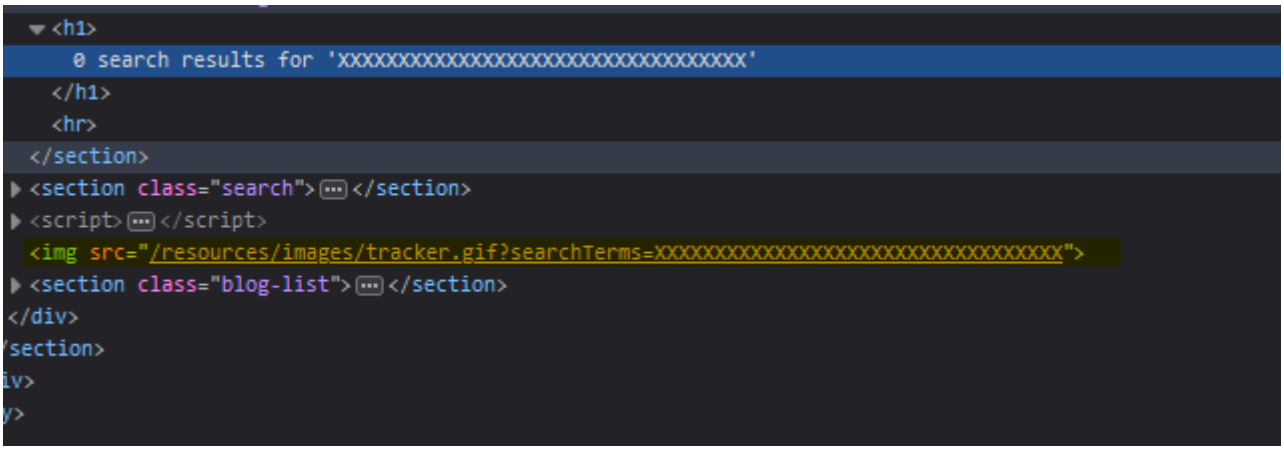
1. Enter a random alphanumeric string into the search box.
2. Right-click and inspect the element, and observe that your random string has been placed inside an `img src` attribute.
3. Break out of the `img` attribute by searching for:

   `"><svg onload=alert(1)>`

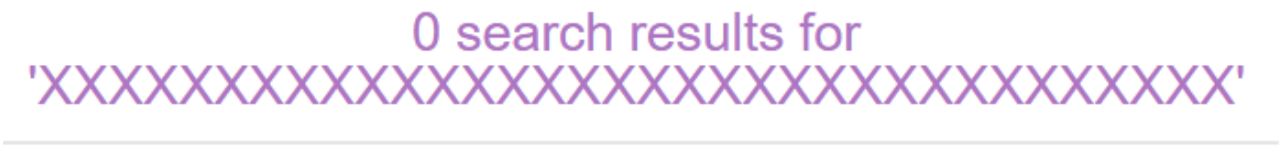
Type/Paste in a silly String

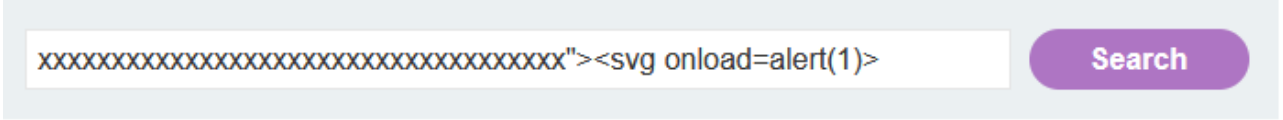


Find the XXXXX string in the Source



Add the Escape Tag





Displayed DOM XSS Pop Up


ada0027043b2629c09d106900d000d5.web-security-academy.net
1
OK