


This lab contains a reflected cross-site scripting vulnerability in the search query tracking functionality. The reflection occurs inside a JavaScript string with single quotes and backslashes escaped.

To solve this lab, perform a cross-site scripting attack that breaks out of the JavaScript string and calls the alert function.

In the search functionality type hello and observe the html code.



Reflected XSS into a JavaScript string with single quote and backslash escaped

LAB Not solved

Back to lab description >>

Home

0 search results for 'hello'

< Back to Blog

Elements

```
on class="maincontainer">
  class="container is-page">
    header class="navigation-header"></header>
    header class="notification-header"></header>
    section class="blog-header">
      h1>0 search results for 'hello'</h1>
      hr>
      section>
        section class="search">
          script></script>
    </section>
  </div>
</div>
```


Styles

element.style { }

[theme=blog] h1 { font-size: 1.8em; }

h1:first-child, h2:first-child, h3:first-child...

Try sending the payload test'payload and observe that your single quote gets backslash-escaped, preventing you from breaking out of the string.



Reflected XSS into a JavaScript string with single quote and backslash escaped

LAB Not solved

Back to lab description >>

Home

0 search results for 'test'payload '

< Back to Blog

Elements

```
on class="maincontainer">
  class="container is-page">
    header class="navigation-header"></header>
    header class="notification-header"></header>
    section class="blog-header">
      h1>0 search results for 'test'payload '</h1>
      hr>
      section>
        section class="search">
          script></script>
    </section>
  </div>
</div>
```

Styles

element.style { }

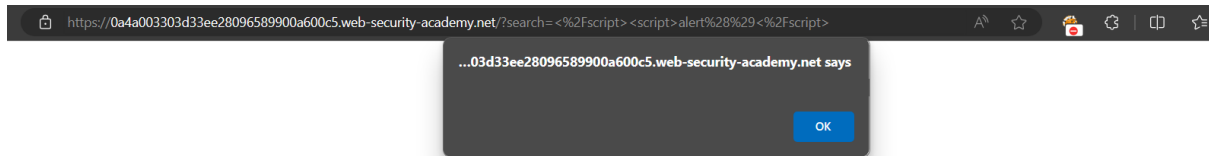
[theme=blog] h1 { font-size: 1.8em; }

h1:first-child, h2:first-child, h3:first-child...

Since we cannot break out of the string context, what if we can close the <script>

Payload will be

```
</script><script>alert()</script>
```



Reflected XSS into a JavaScript string with single quote and backslash escaped

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

[Home](#)

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

'; document.write("");

[< Back to Blog](#)