
Reflected XSS into HTML context with nothing encoded

1. This lab contains a simple reflected cross-site scripting vulnerability in the search functionality. I try to write anything to see how the website interacts with it. The website takes the input and prints it again on the same page.

[Home](#)

1 search results for 'test'

Search

2. Then, I try to test if there is special character filtration on or not. So, I try this (test'"<>). The website does not sanitize the user input.

[Home](#)

0 search results for 'test'"<>'

Search

```
<section class=blog-header>
  <h1>0 search results for 'test'"<>'</h1>
  <hr>
</section>
```

3. I try to hit this payload (test'><script>alert()</script>) and here we go the lab already solved



Reflected XSS into HTML context with nothing encoded

[Back to lab description >>](#)

LAB Solved 

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

[Home](#)

0 search results for 'testâ€œ>'

Search

[< Back to Blog](#)