
Stored XSS into HTML context with nothing encoded

1. This lab contains a stored cross-site scripting vulnerability in the comment functionality. Let's try to test it. First, I want to understand the behavior of this function.

Leave a comment

Comment:

test1'<>

Name:

test2'<>

Email:

test@test.test

Website:

https://www.test.com

Post Comment

2. When I saw the page source I found the name encoded but the comment does not have any encoding or sanitization.

```
</p>
<p>test1'<></p>
<p></p>
```

```
<a id="author" href="https://www.test.com">test2'&apos;&quot;&lt;&gt;&lt;/a> | 20 September 2025
```

3. So, Let's try to inject the payload in comment section. The payload was (test'><script>alert()</script>). And finally, the lab solved.

Congratulations, you solved the lab!

Share your skills!



[Continue learning](#) >>

[Home](#)

Thank you for your comment!

Your comment has been submitted.

[< Back to blog](#)