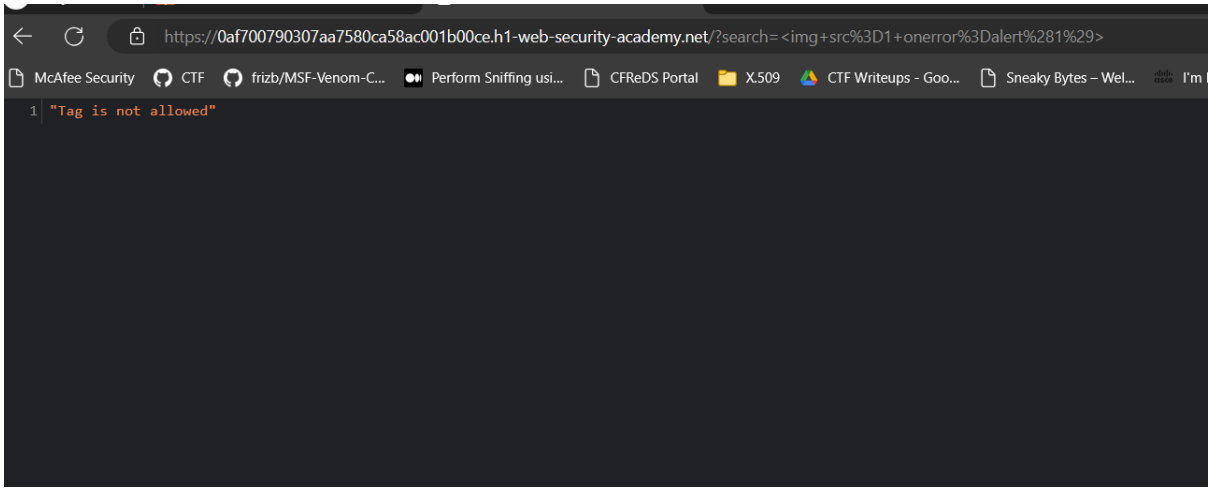
This lab has a simple reflected XSS vulnerability. The site is blocking common tags but misses some SVG tags and events.

To solve the lab, perform a cross-site scripting attack that calls the alert() function.

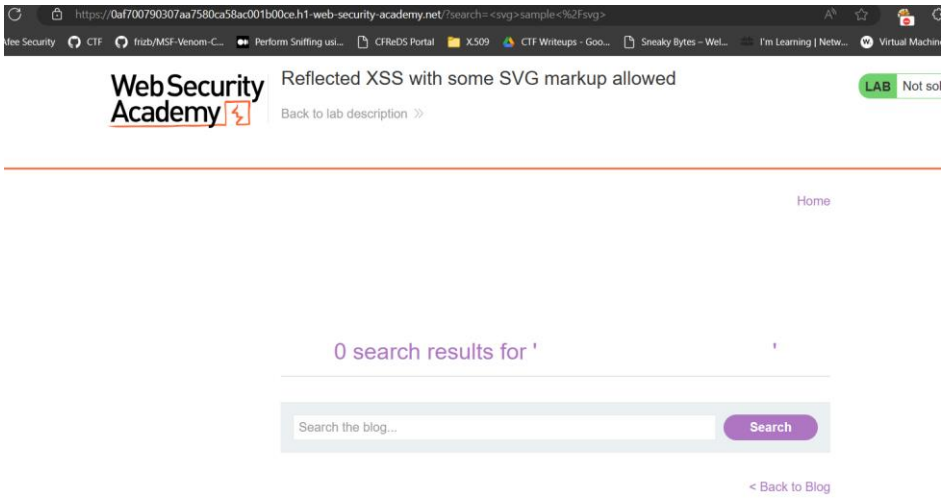
Inject a standard XSS payload, such as:

<img src=1 onerror=alert(1)>

Observe that this payload gets blocked. In the next few steps, we'll use Burp Intruder to test which tags and attributes are being blocked.

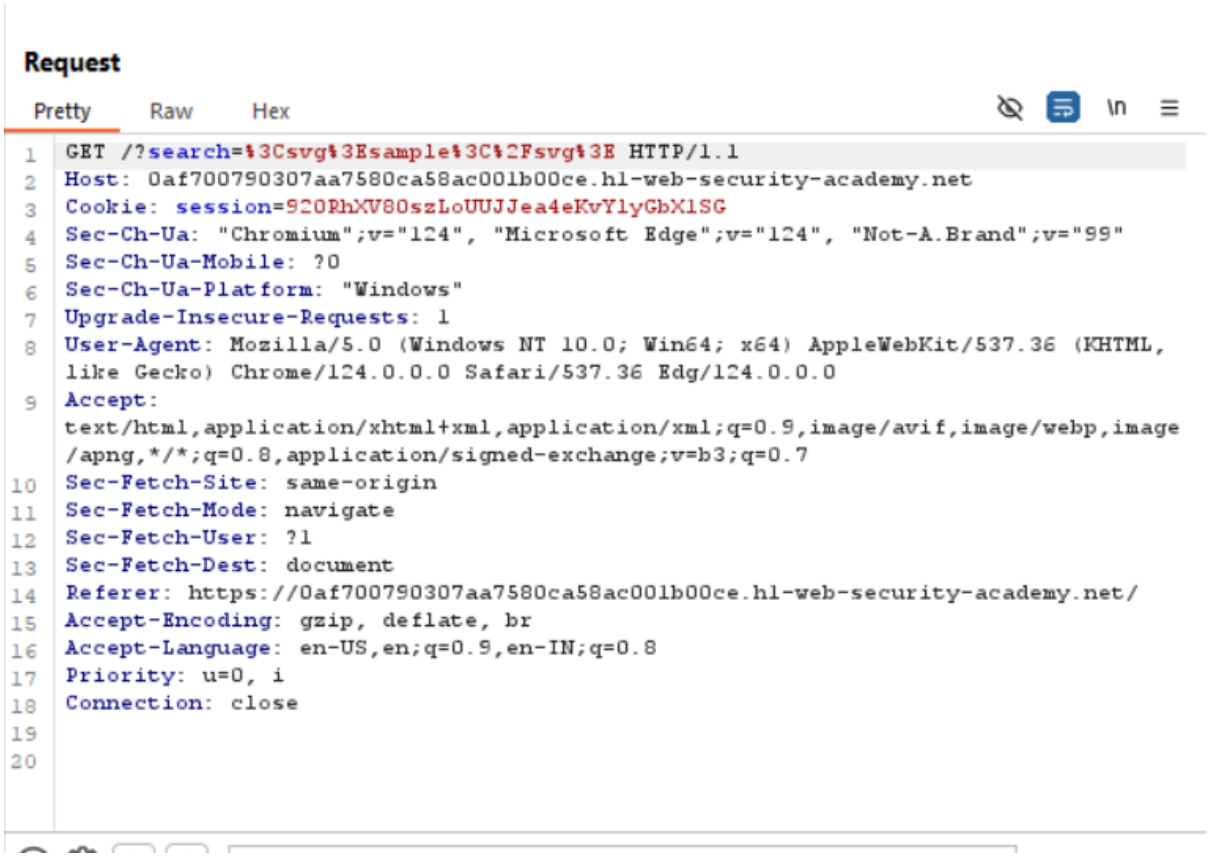


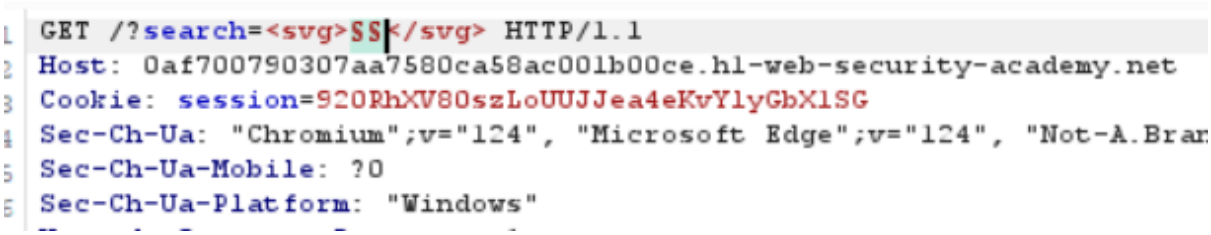
Result is,



The site is not blocking <svg> tags.

Send the resulting request to Burp Intruder, Find the tag we can use in between svg tags.



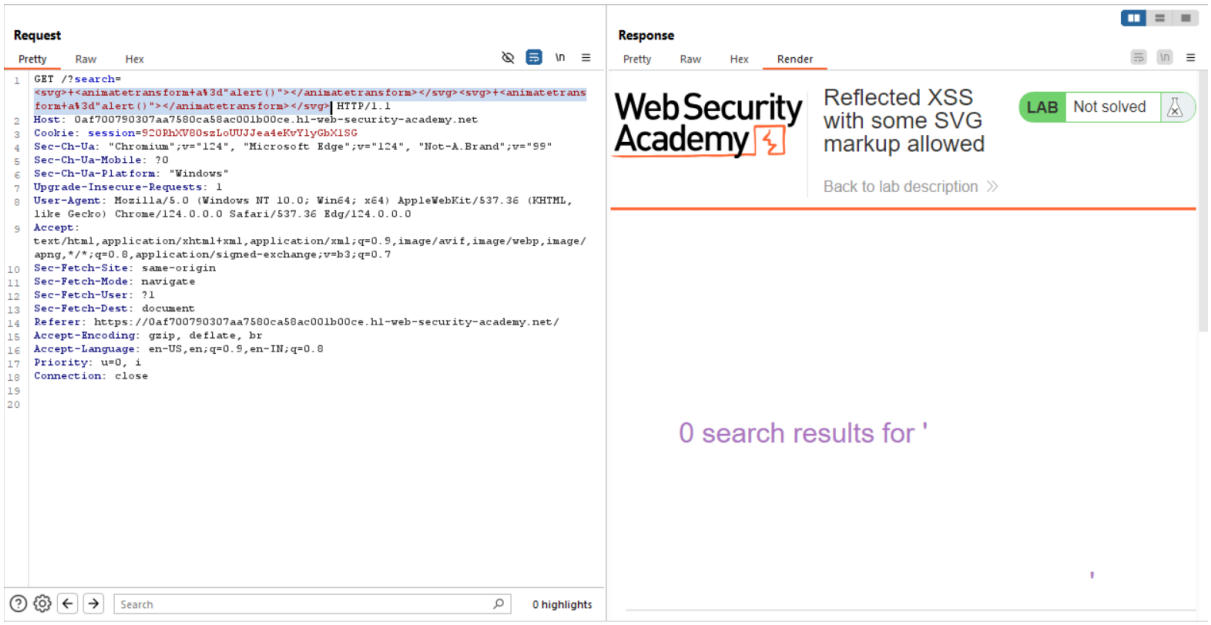


Now Visit the XSS cheat sheet and click "Copy tags to clipboard".

When the attack is finished, review the results. Observe that all payloads caused an HTTP 400 response, except for the ones using the <svg>, <animatetransform>, <title>, and <image> tags, which received a 200 response.

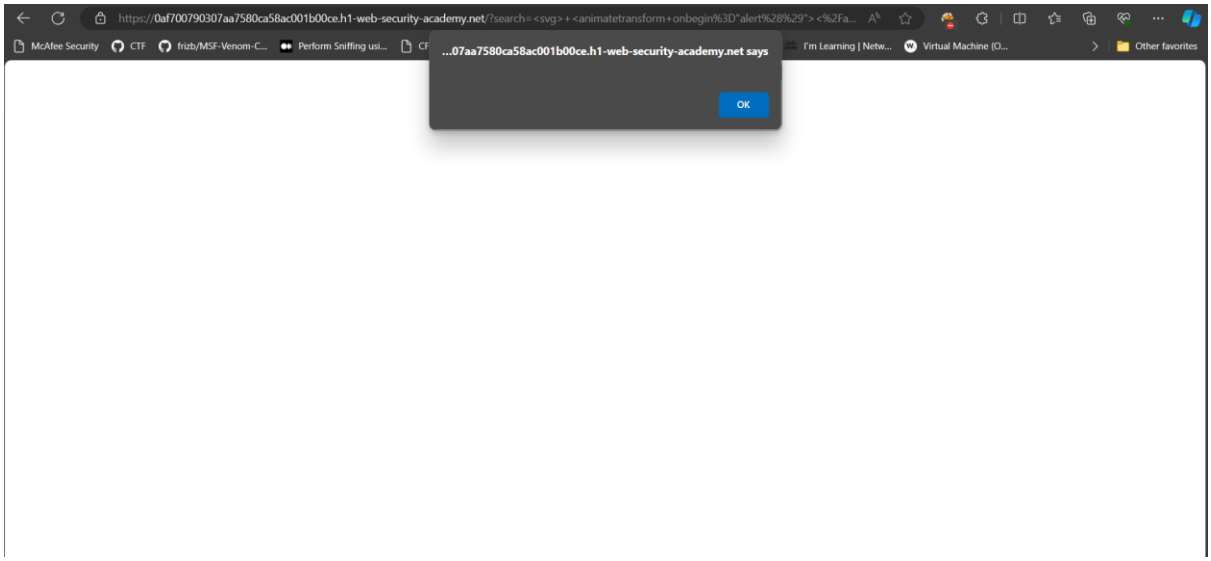
<animatetransform> use an event atribute for finding that i use the payload

Payload: <svg> <animatetransform a="alert()"></animatetransform></svg>



Updated Payload,

<svg> <animatetransform onbegin="alert()"></animatetransform></svg>



S. Giridharan
CB.SC.P2CYS23006