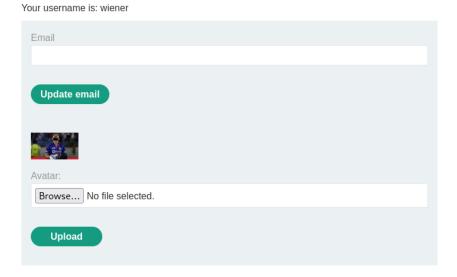
## File Upload Vulnerabilities Lab – 04 Web Shell Upload Via Extension Blacklist Bypass

M.Gobi Shankar CB.SC.P2CYS23019

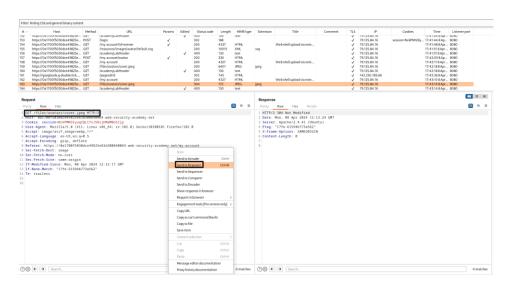
Log in and upload an image as your avatar, then go back to your account page.

Home | My account | Log ou

## My Account



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.



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

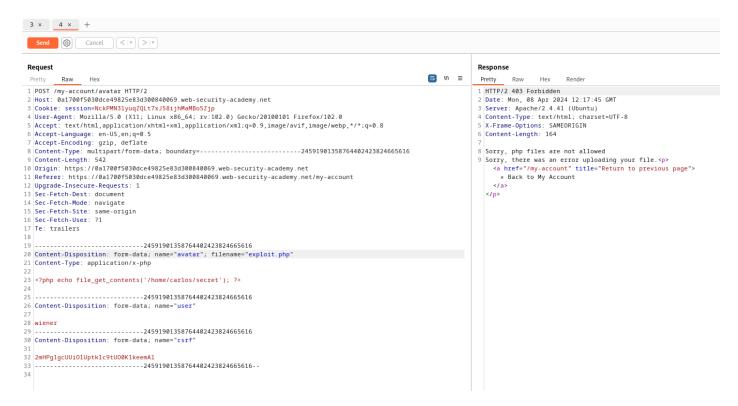
<?php echo file_get_contents('/home/carlos/secret'); ?>
```

Attempt to upload this script as your avatar. The response indicates that you are not allowed to upload files with a .php extension.

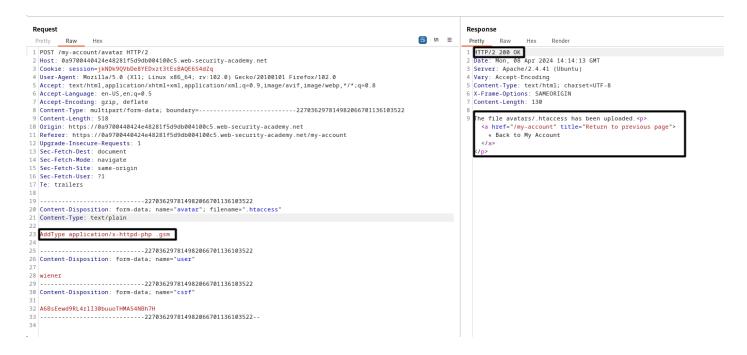
Sorry, php files are not allowed Sorry, there was an error uploading your file.

<u> Back to My Account</u>

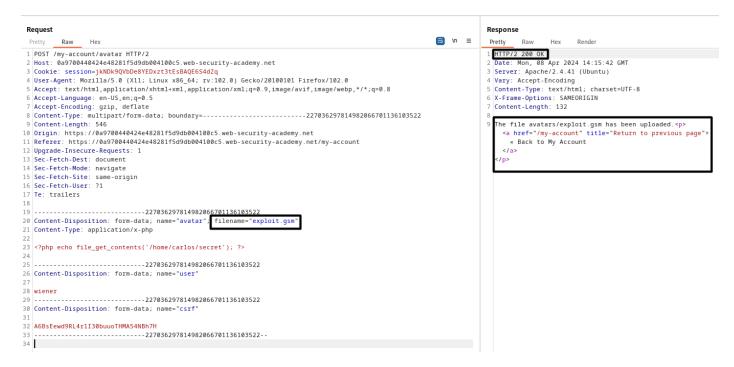
In Burp's proxy history, find the POST/my-account/avatar request that was used to submit the file upload. In the response, notice that the headers reveal that you're talking to an Apache server. Send this request to Burp Repeater.



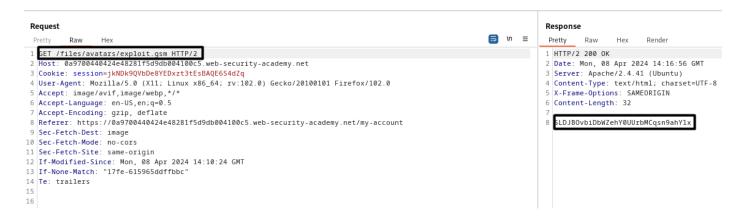
In Burp Repeater, go to the tab for the POST /my-account/avatar request and find the part of the body that relates to your PHP file. Change the value of the filename parameter to .htaccess and Change the value of the Content-Type header to text/plain. Send the request and observe that the file was successfully uploaded.



Use the back arrow in Burp Repeater to return to the original request for uploading your PHP exploit. Change the value of the filename parameter from exploit.php to exploit.gsm. Send the request again and notice that the file was uploaded successfully.

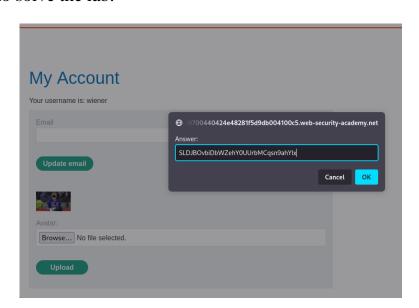


Switch to the other Repeater tab containing the GET /files/avatars/cover.jpeg request. In the path, replace the name of your image file with exploit.gsm and send the request. Observe that Carlos's secret was returned in the response.



Secret: SLDJBOvbiDbWZehY0UUrbMCqsn9ahYlx

Submit the secret to solve the lab.



## Lab Completed Successfully.

Web Security Academy 5  Web shell upload via extension blacklist bypa  Back to lab description >>	ass LAB Solved
Congratulations, you solved the lab!	Share your skills! 🤟 in Continue learning »
	Home   My account   Log out
My Account	
Your username is: wiener	
Email	
Update email	