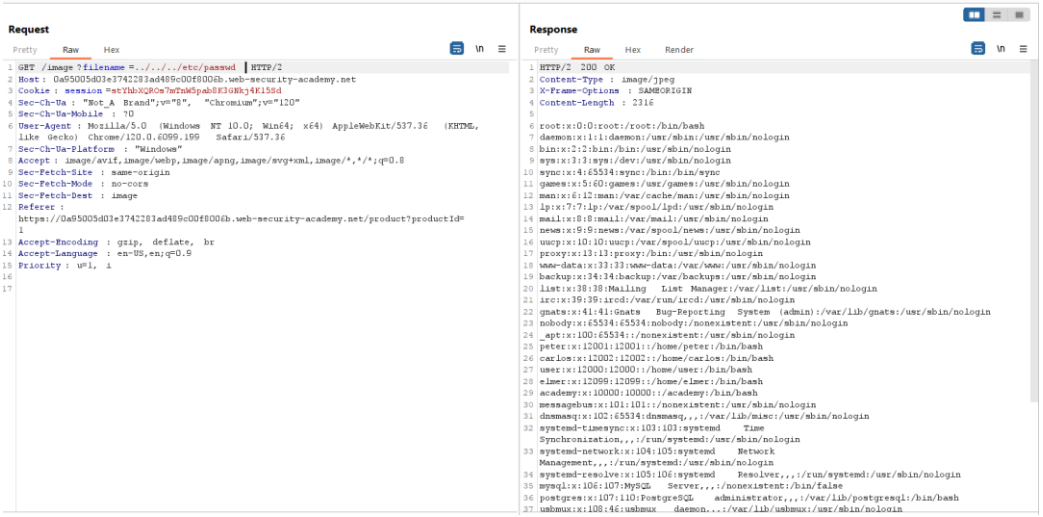
PATH TRAVERSAL

LAB 34 File path traversal, simple case

This lab is vulnerable to pass traversal. I tried to play around with productid parameter in the URL but I wasn't successful. Then, I intercepted a packet that fetches product file image and changed the value of the parameter to ../etc/passwd using Burp Repeater and was walking upwards until I get contents of /etc/passwd file:

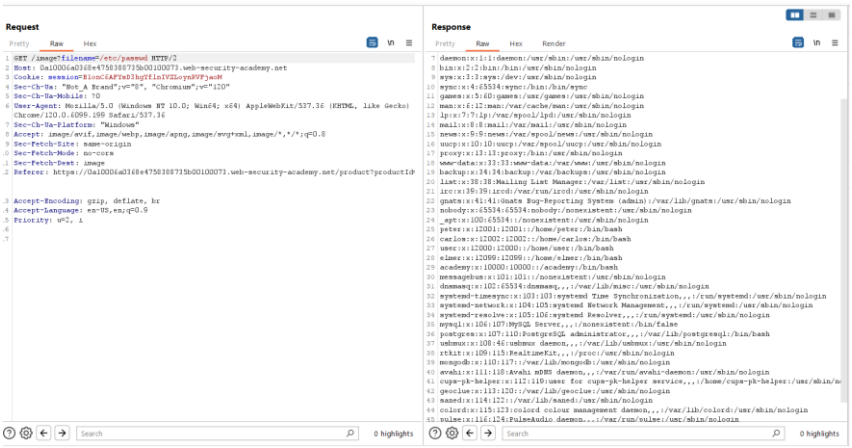


Lab completed!

Congratulations, you solved the lab!

LAB 35 File path traversal, traversal sequences blocked with absolute path bypass

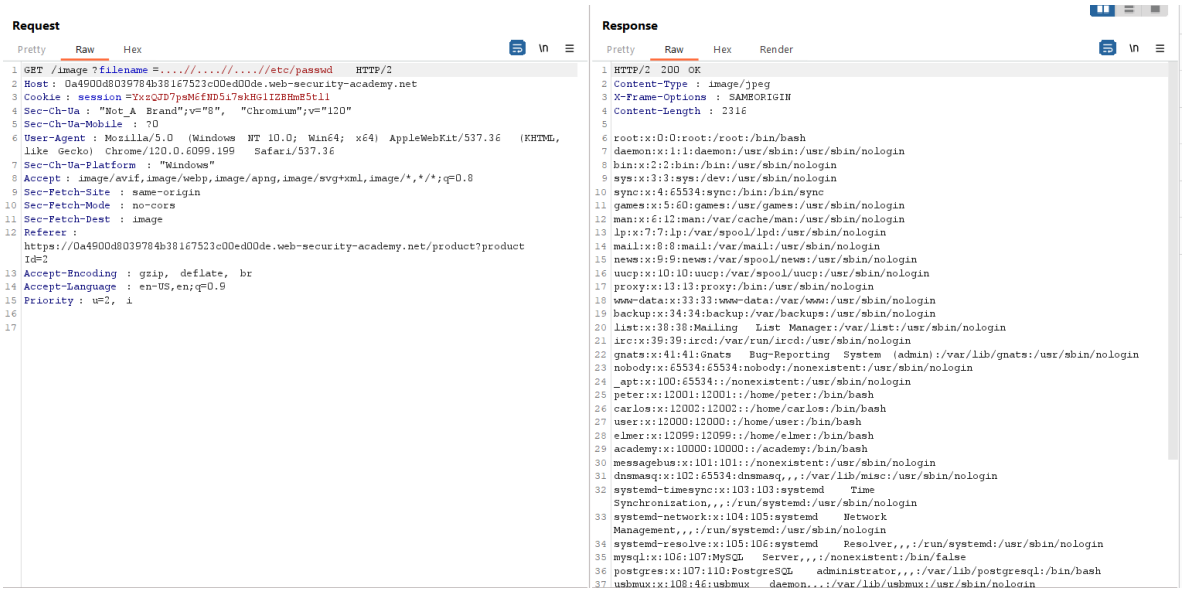
In this lab, naïve path traversal won't work because server uses absolute paths for file names and we cannot really break out of the directory with image files, so I would use simple /etc/passwd absolute path and pass it as parameter:



Congratulations, you solved the lab!

LAB 36 File path traversal, traversal sequences stripped non-recursively

This lab has a protection from path traversal so that strings of file names are parsed and whenever "../" occurs, the string is stripped. To bypass this, I will traverse the path with "....//" instead, so after deletion of "../", the combination will preserve:

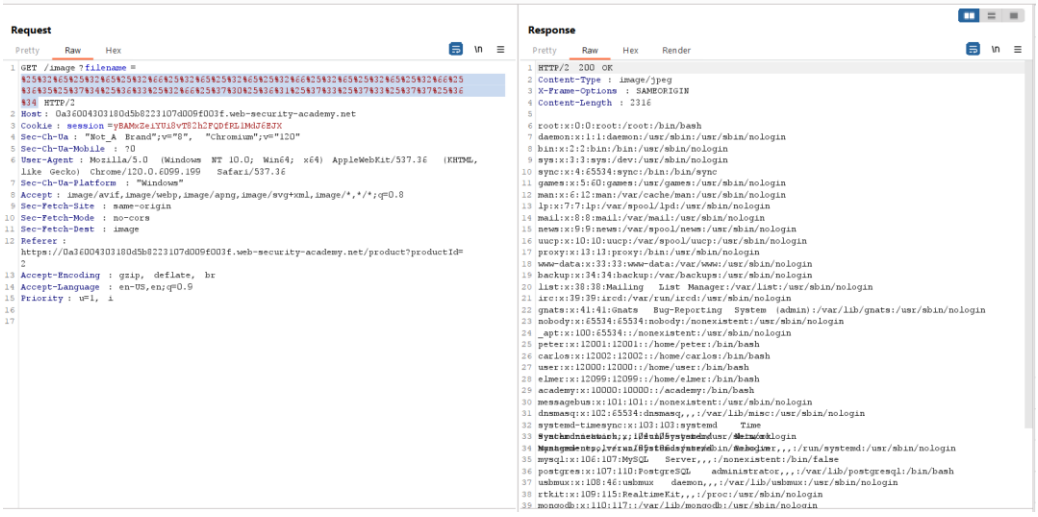


Lab's done!

Congratulations, you solved the lab!

LAB 37 File path traversal, traversal sequences stripped with superfluous URL-decode

This lab has more advanced defense mechanisms of stripping the sequence completely, so method from previous lab won't work. This can be bypassed by URL encoding the sequence:



Single URL encoding did not work, probably because blue team predicted this move, however, double URL encoding was successful and I got /etc/passwd contents.

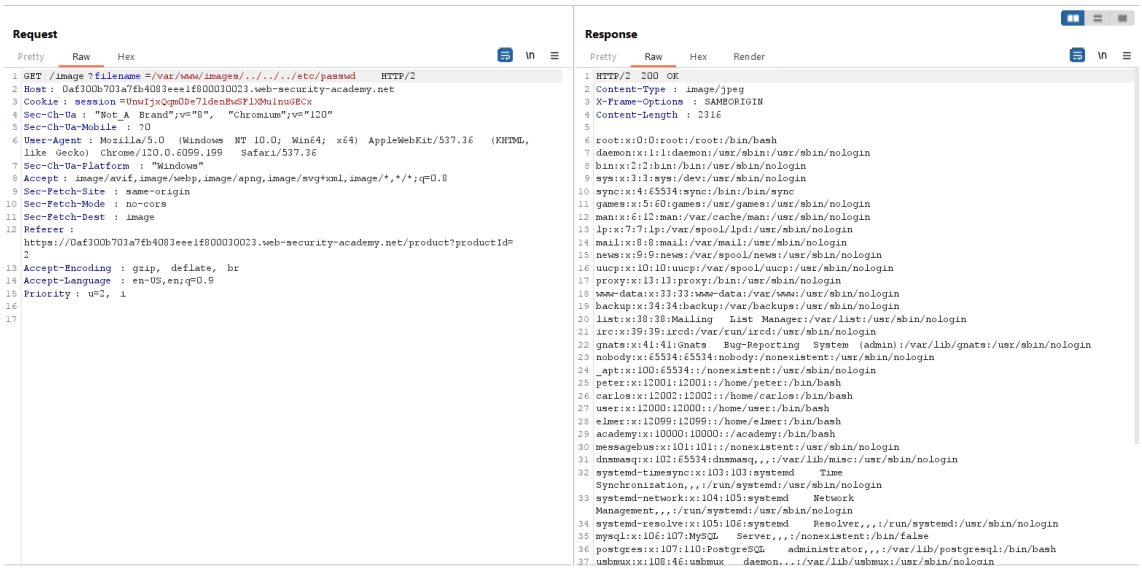
Congratulations, you solved the lab!

LAB 38 File path traversal, validation of start of path

In this lab, service requires the user-defined file name to start from a certain base folder, in this case it was /var/www/images:

```
net/image?filename=/var/www/images/16.jpg
```

So, path traversal can be done as follows:

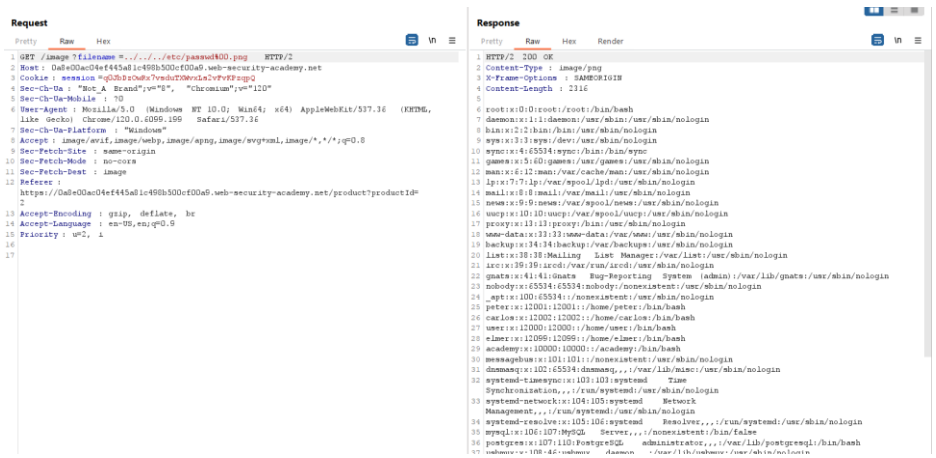


Lab's done!

Congratulations, you solved the lab!

LAB 39 File path traversal, validation of file extension with null byte bypass

In this lab, filenames are checked that they end with an image extension (.jpg, .png). So, to make a successful attack, I will inject a null byte, following with file extension in the end. This will truncate the result to /etc/passwd even though it ends on .png



Congratulations, you solved the lab!