Directory Traversal

Refer for theory: https://portswigger.net/web-security/file-path-traversal

Vulnerability Labs(Apprentice):

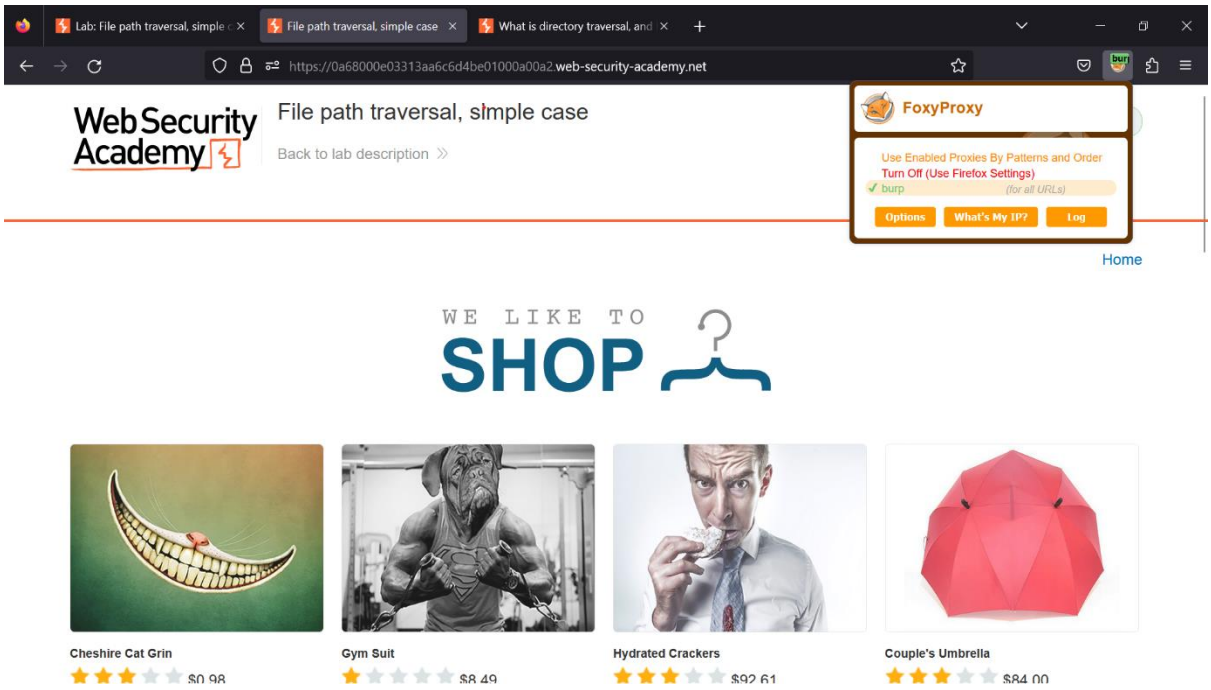
1. File path traversal, simple case.

This lab contains a file path traversal vulnerability in the display of product images.

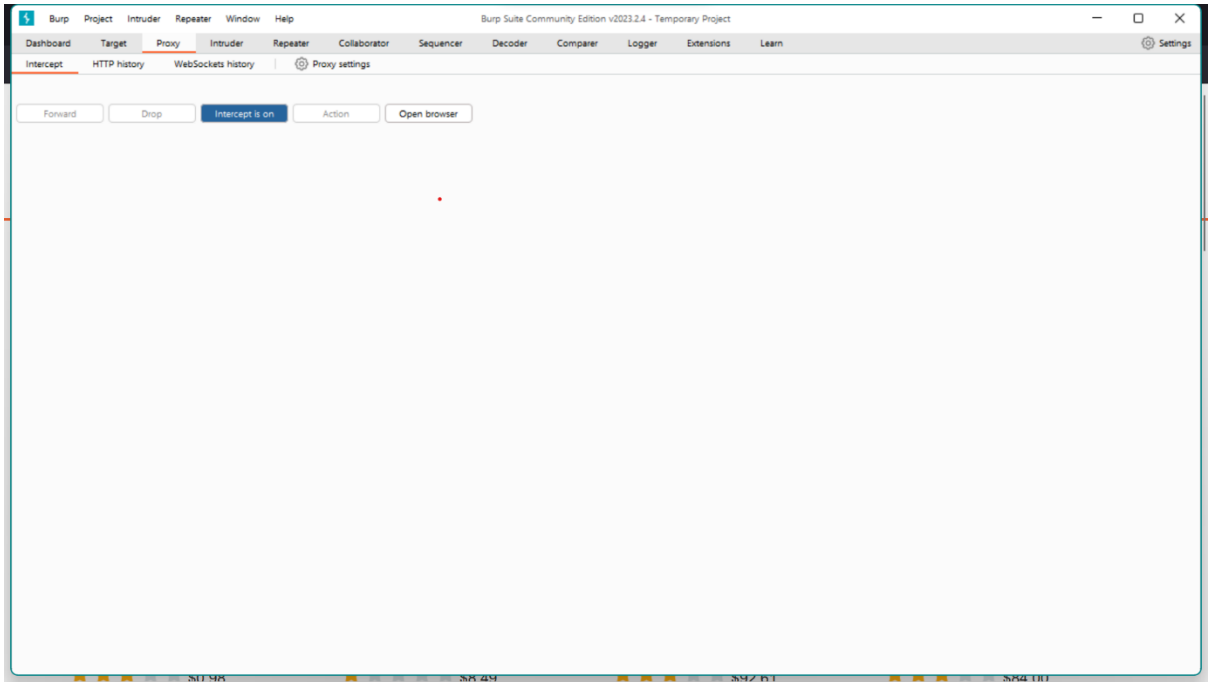
To solve the lab, retrieve the contents of the /etc/passwd file.

Solution:

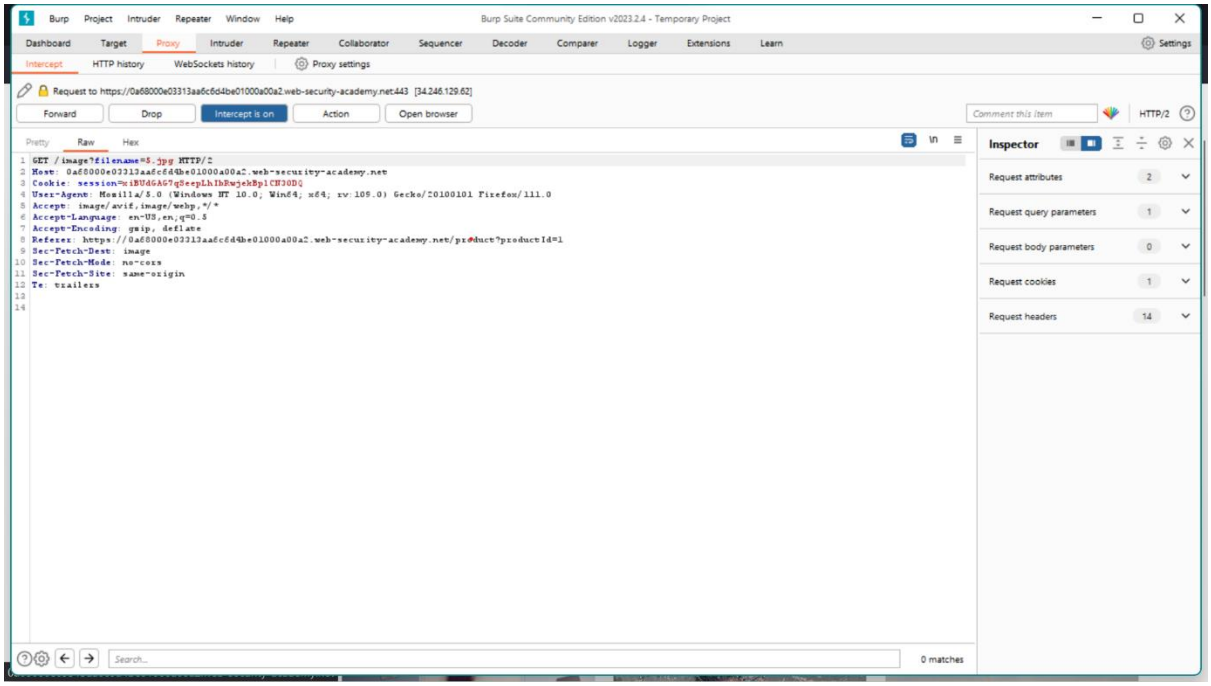
- Access the lab and a e-shopping site will open.
- Turn on your proxy using foxyproxy.



- Open your burpsuite and turn on the intercept in the proxy tab.



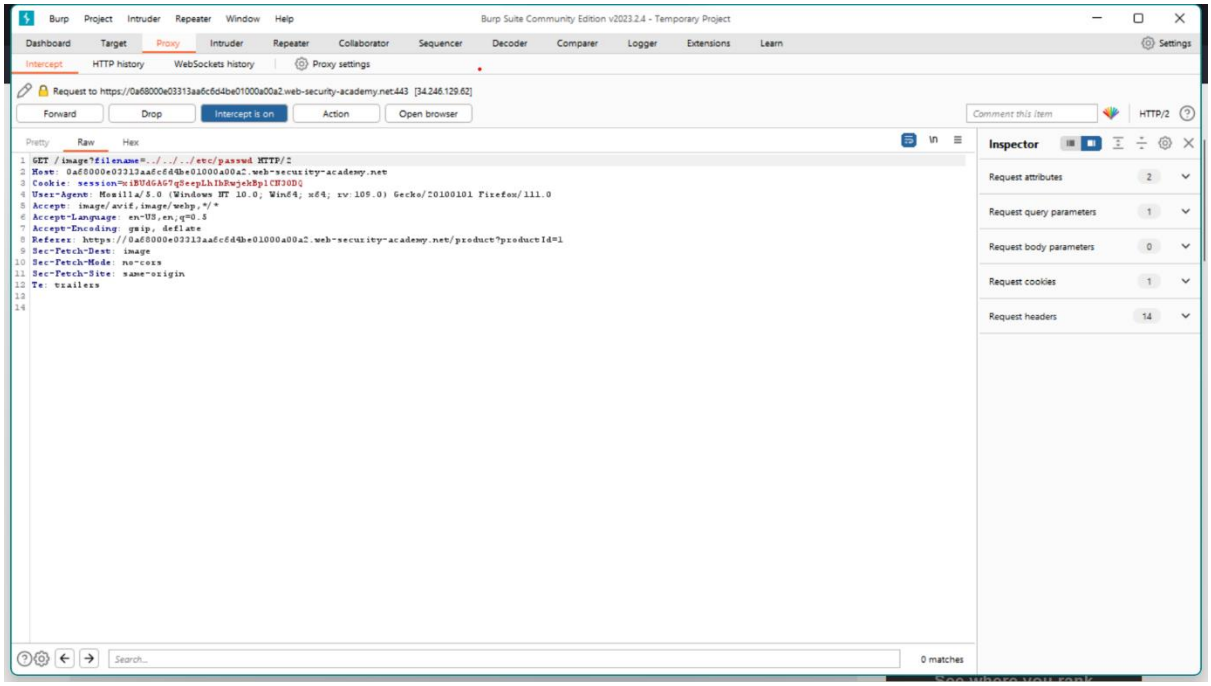
- Refresh your browser and you will receive a warning on the browser. Click on accept the risk and continue.
- On the test lab, click on any product.
- Once there's some activity on the browser, the burp suite will start to capture all the packets that will be sent to the server.
- Start analyzing the packets once you click on a product.



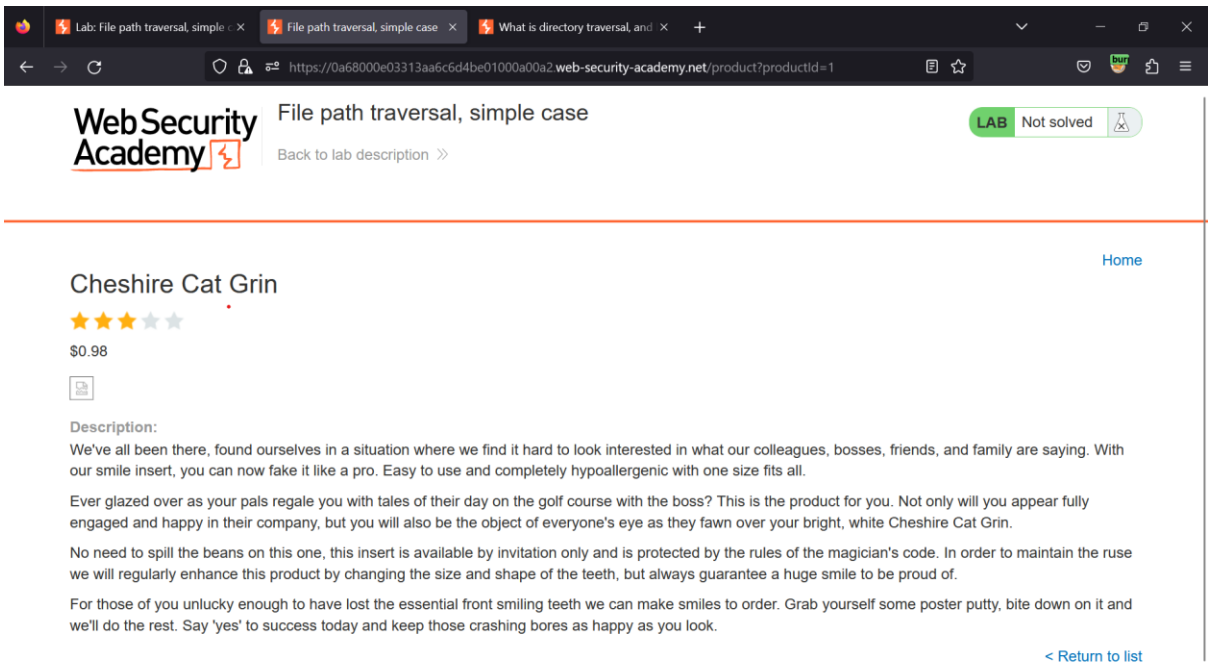
- One of the packets will have a parameter named filename. You will get this by going through all the packets.
- The filename parameter will have value of an image destination. You need to change that to the following:

../../../etc/passwd

- This command will traverse backward on the server side to give us the necessary results.



- Once the change has been made, forward all the further packets and open your lab site.
- You will notice that the image of the product has disappeared.



- Turn off the proxy and refresh your page. Your lab will be solved.