OS Command Injection

Refer for theory: https://portswigger.net/web-security/os-command-injection

Vulnerability labs (apprentice):

1. OS command injection, simple case.

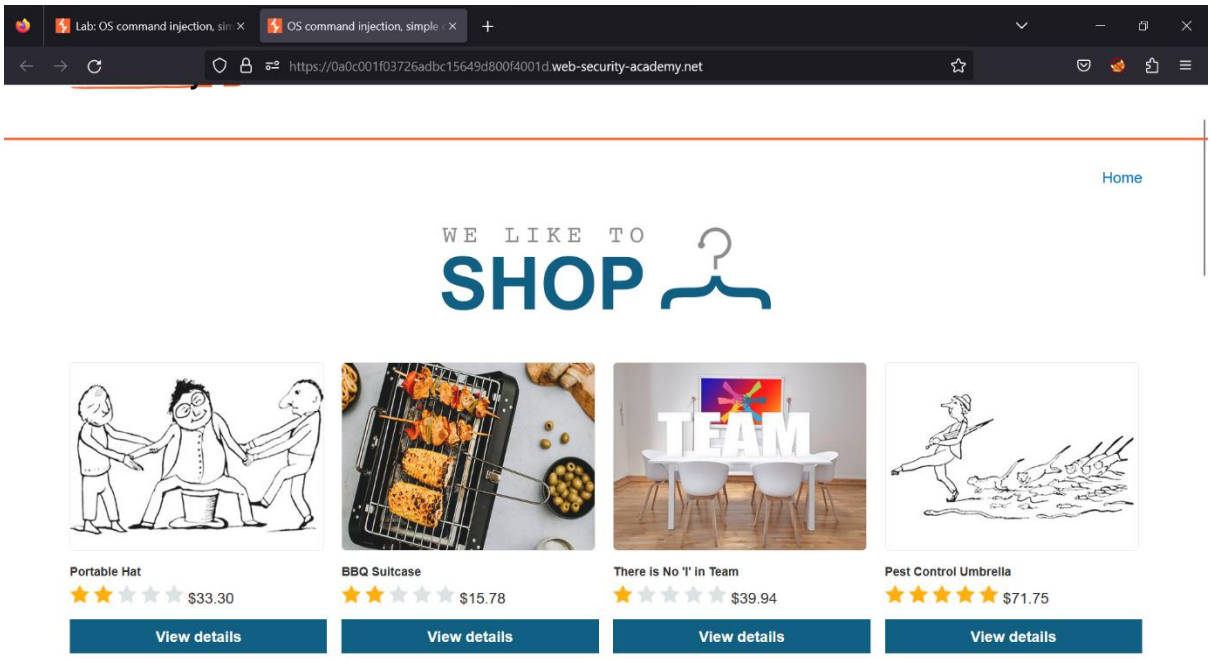
This lab contains an OS command injection vulnerability in the product stock checker.

The application executes a shell command containing user-supplied product and store IDs, and returns the raw output from the command in its response.

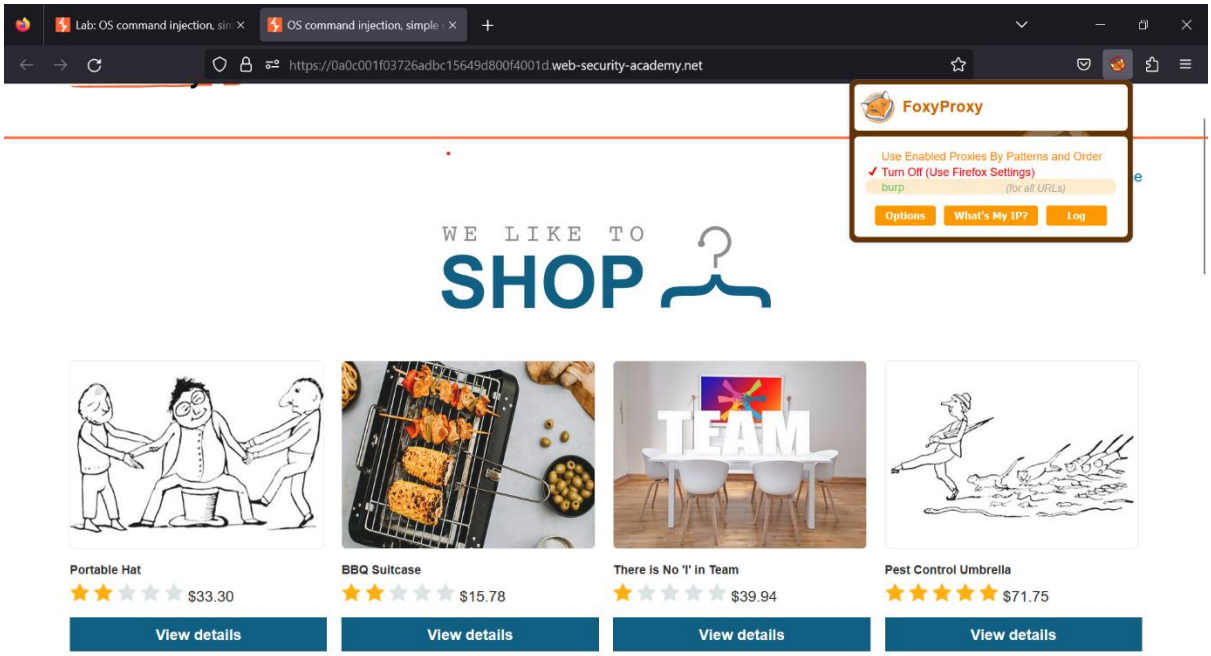
To solve the lab, execute the whoami command to determine the name of the current user.

Solution:

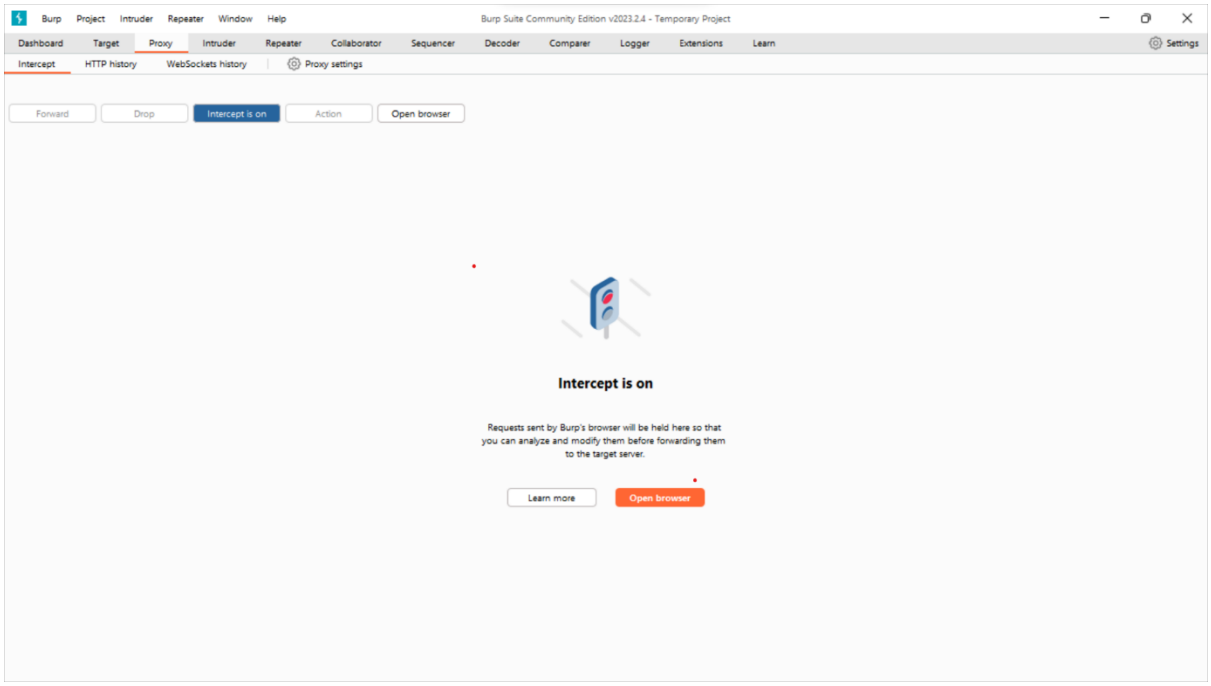
- Once the lab is accessed you will see a shopping site.



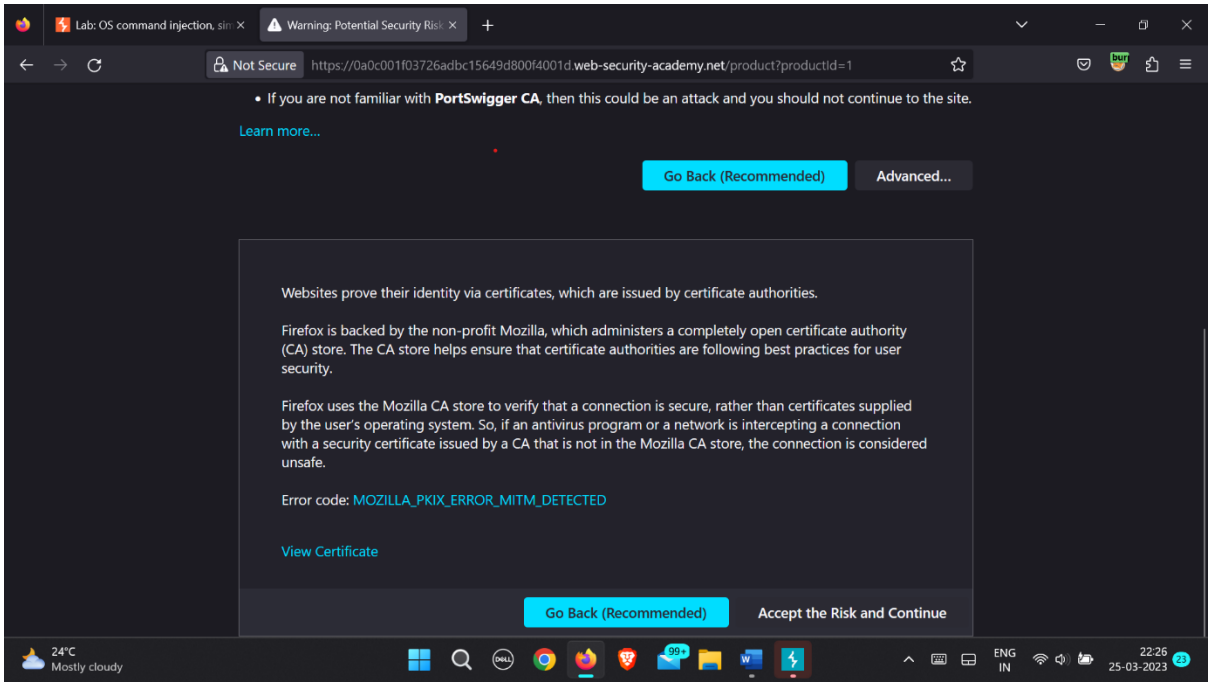
- We will be using foxy proxy and burp suite for this lab.
- Start your foxy proxy by clicking on the pinned extension in your Firefox browser.



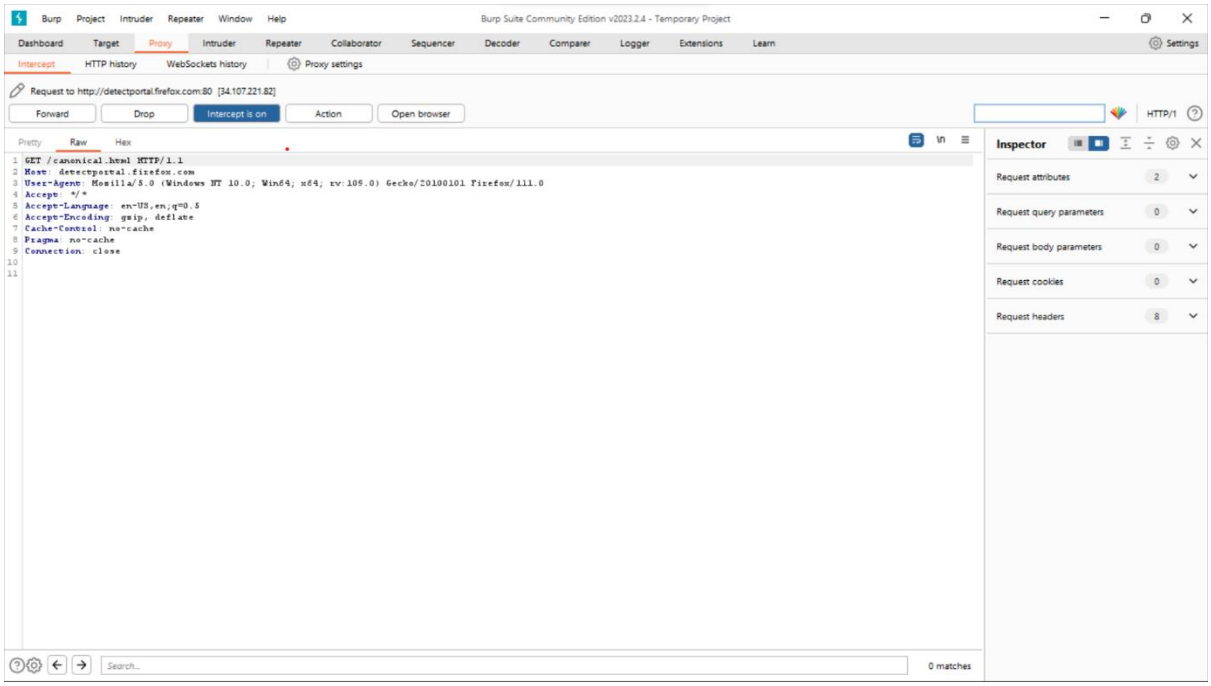
- Start your burp suite and go to proxy. Turn on the intercept.



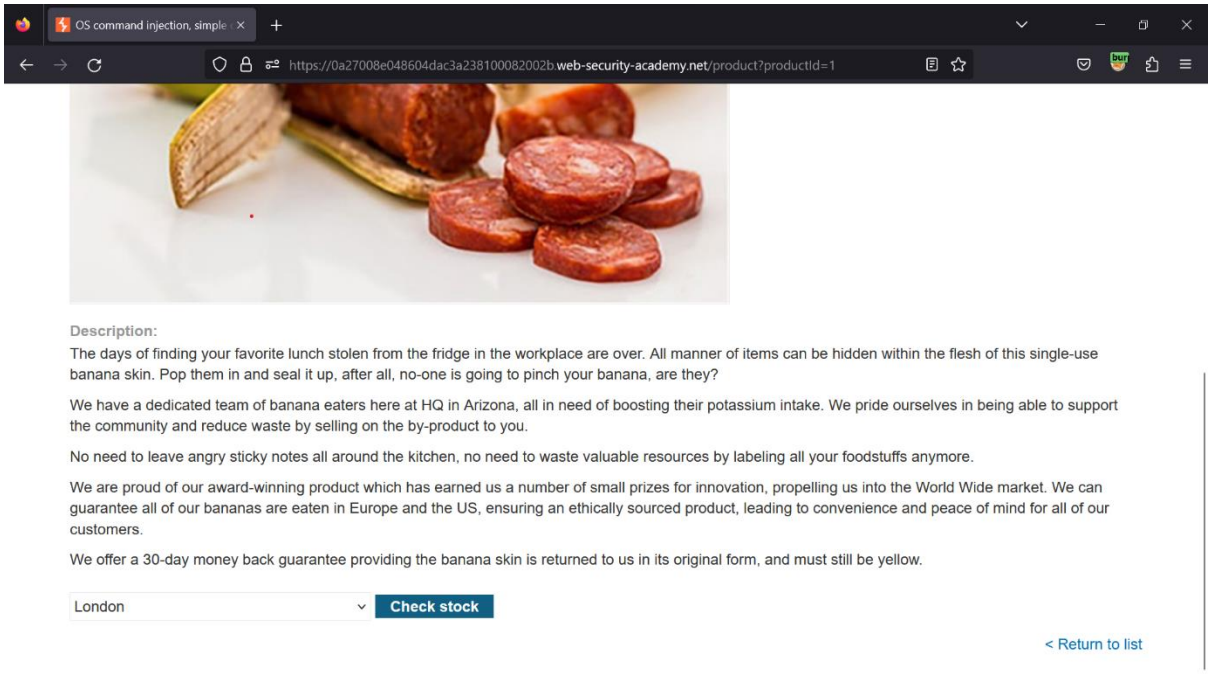
- Once you've done this, if you click on any option on the browser, you will be redirected to a warning page. Click on advanced and select accept the risk and continue.



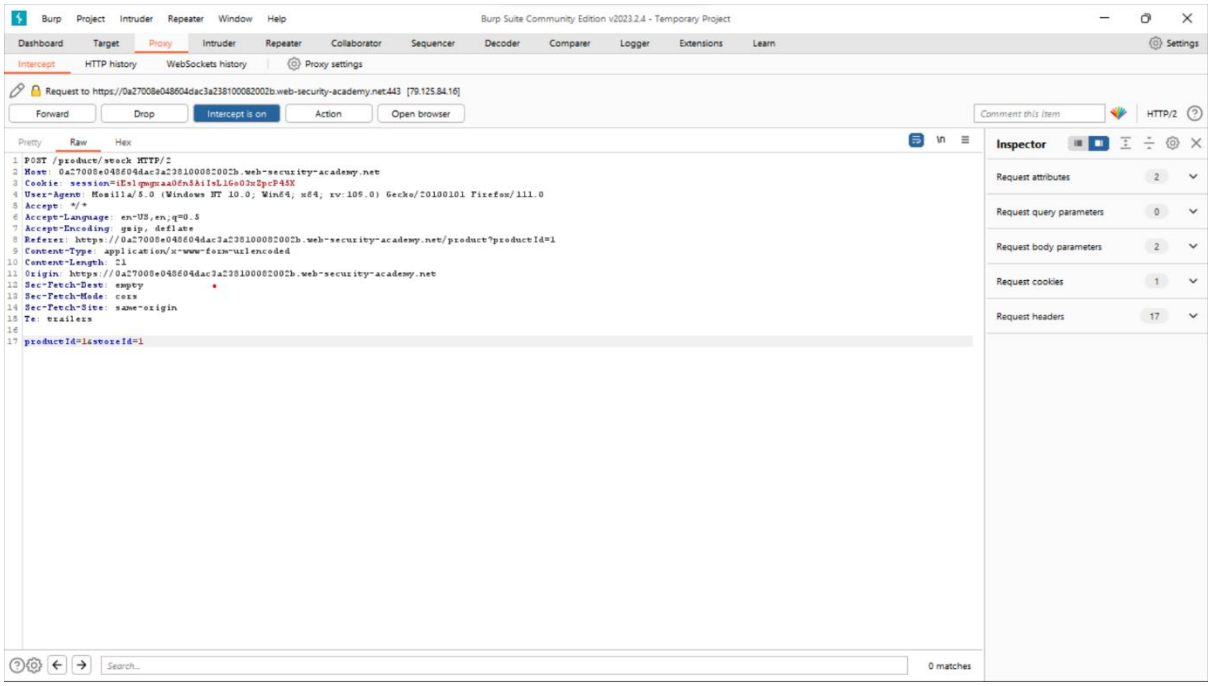
- You will start getting certain alerts from burp suite because it has started to capture the packets. We will only analyze the packets that we need to alter. For the rest keep forwarding them as shown below.



- Select any product on the site and scroll down to see the check stock option.



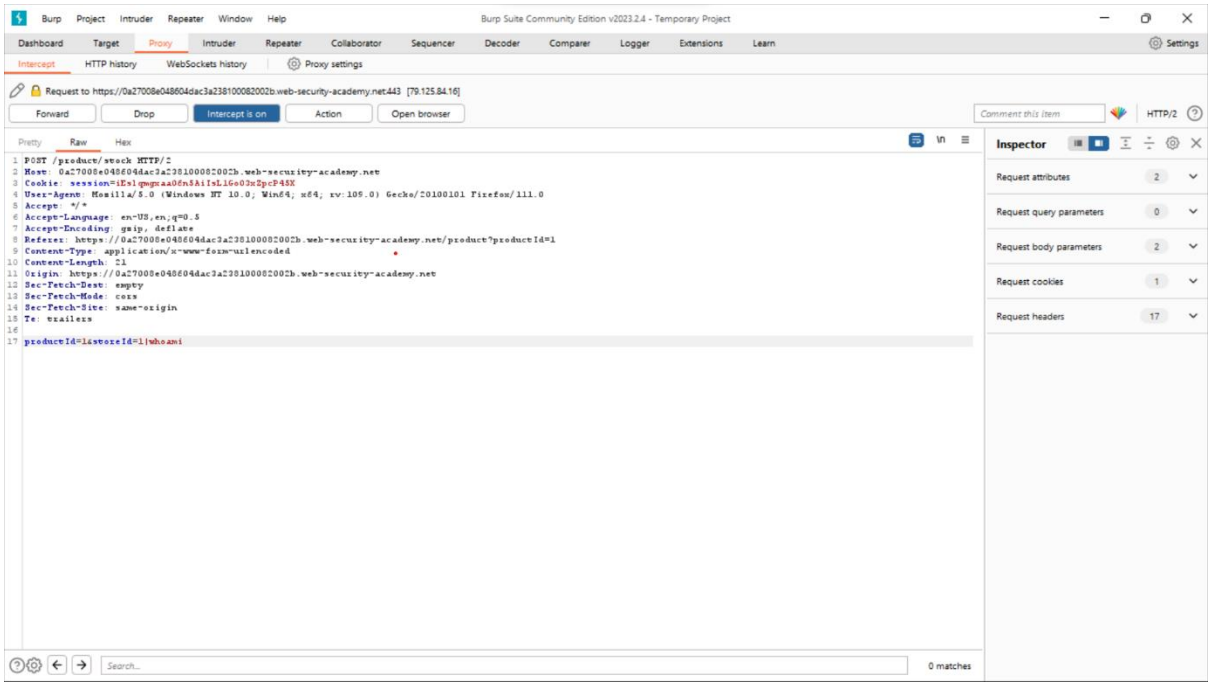
- Note that youll keep getting packets on burpsuite which youll need to forward time to time.
- Click on the check stock option and open your burpsuite.



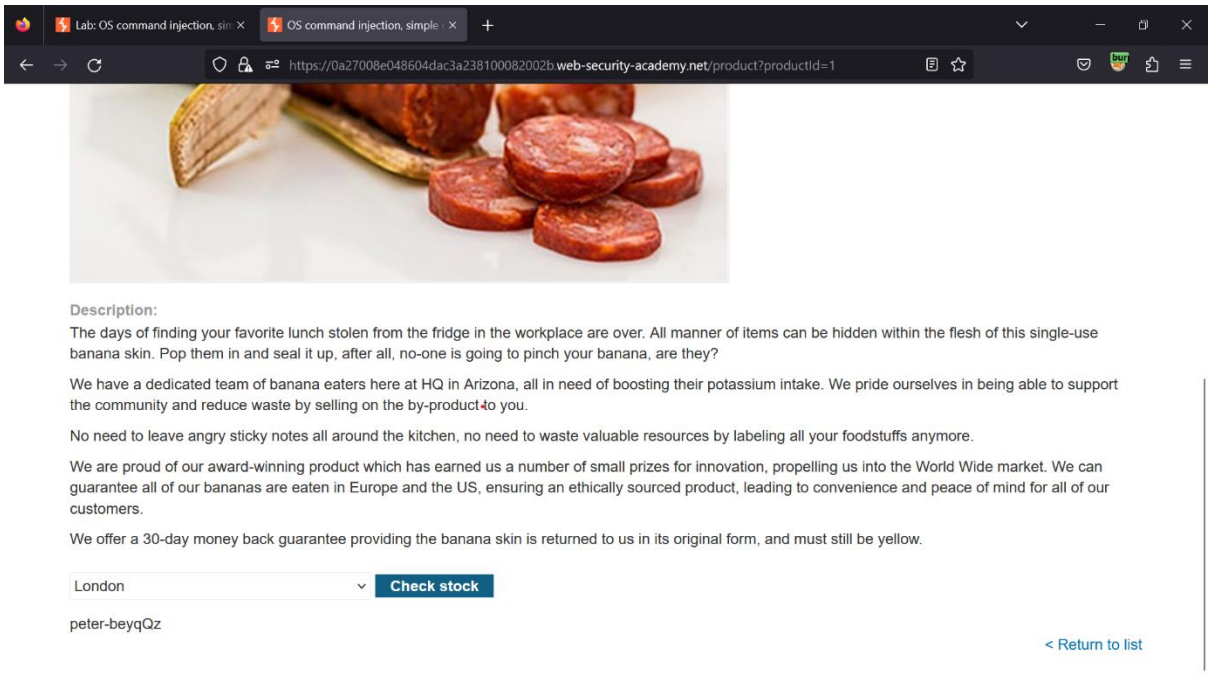
- The packet that requests for the stock option is captured on burpsuite. Change the storied parameter to:

1 | whoami

- whoami is a OS command that tells us the name of the system or server in this case.



- Once the parameter is changed, forward the packet and check your browser for the name of the server.



- Once the name is displayed, turn of the foxy proxy and burp suite. Your lab will be completed.