

OS Command Injection

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

Vulnerability labs (apprentice):

1. OS command injection, simple case.

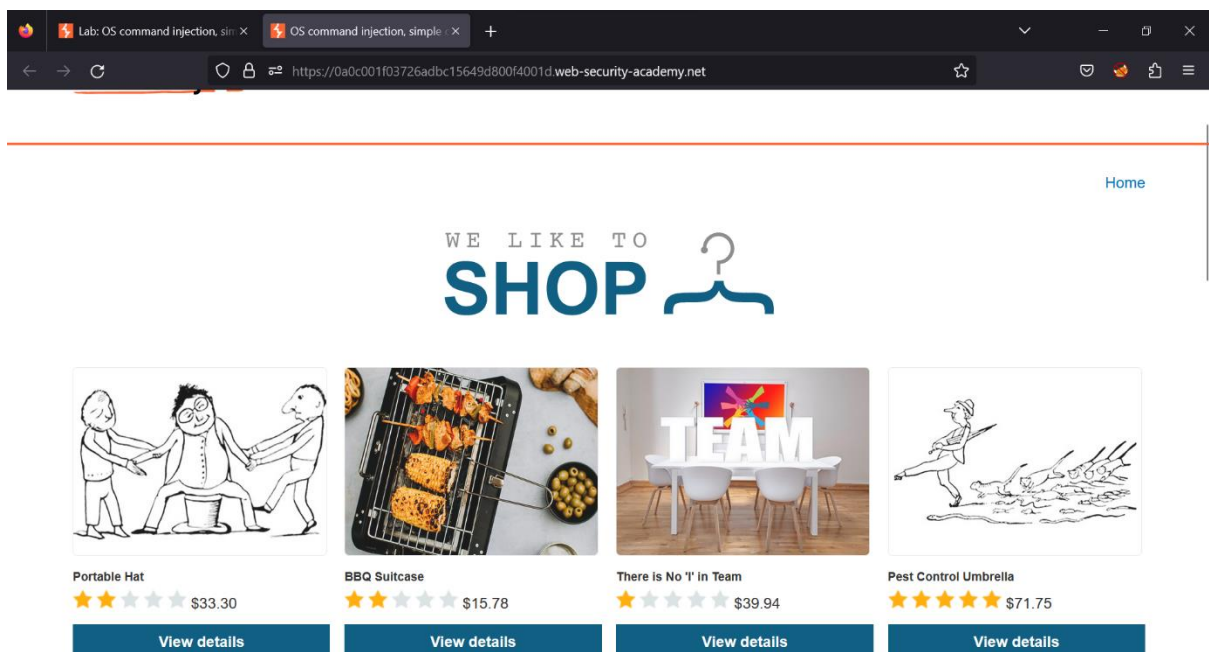
This lab contains an OS command injection vulnerability in the product stock checker.

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

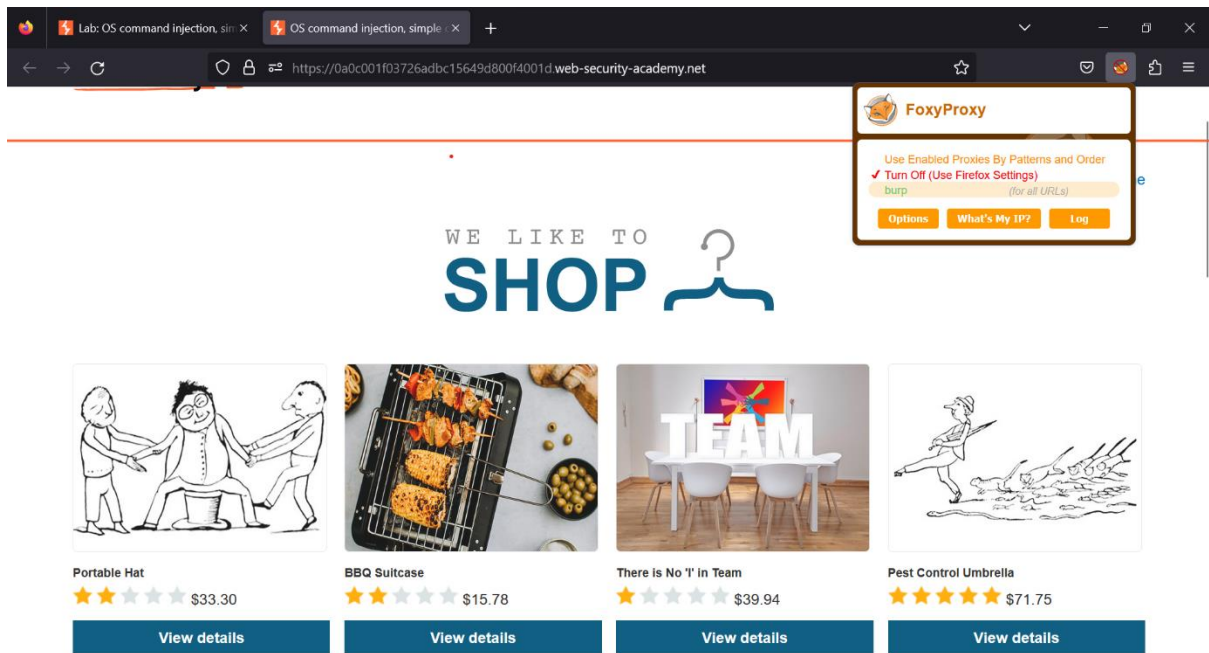
To solve the lab, execute the whoami command to determine the name of the current user.

Solution:

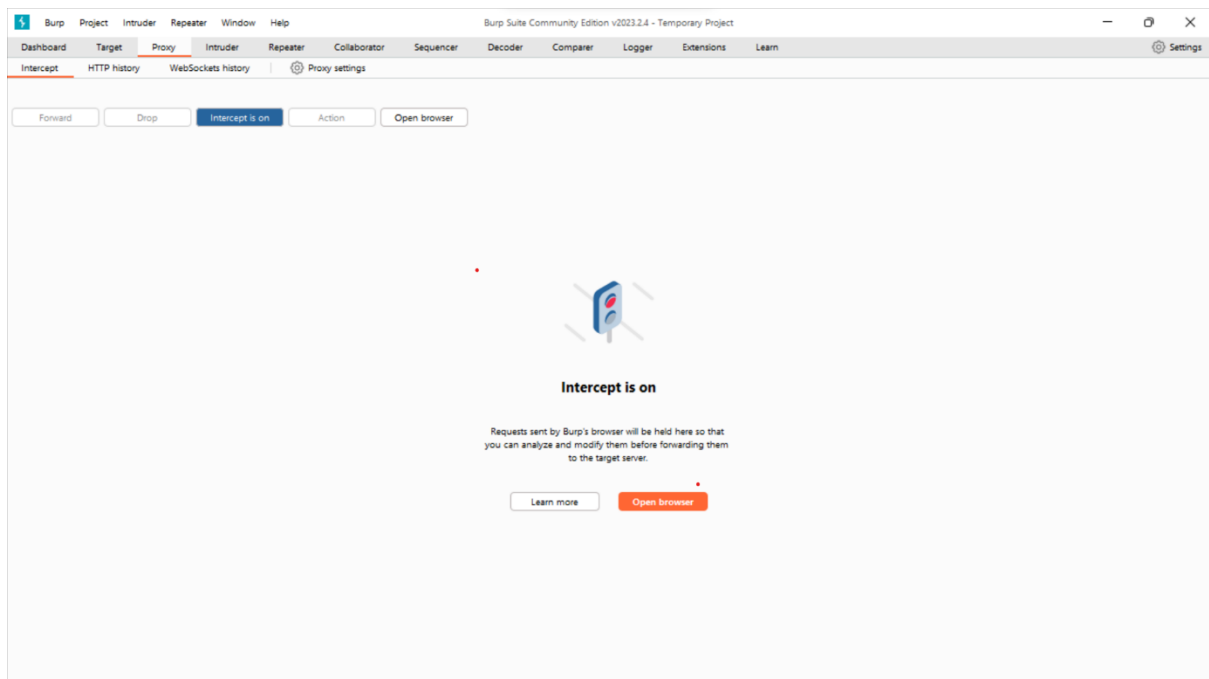
- Once the lab is accessed you will see a shopping site.



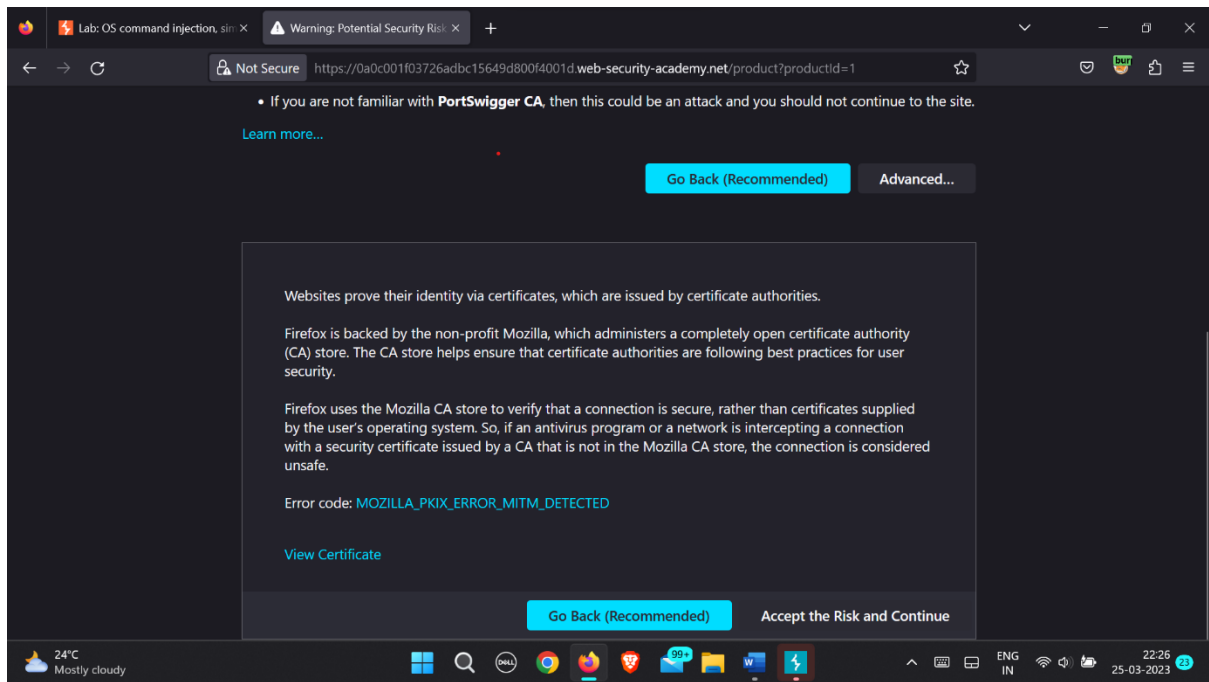
- We will be using foxy proxy and burp suite for this lab.
- Start your foxy proxy by clicking on the pinned extension in your Firefox browser.



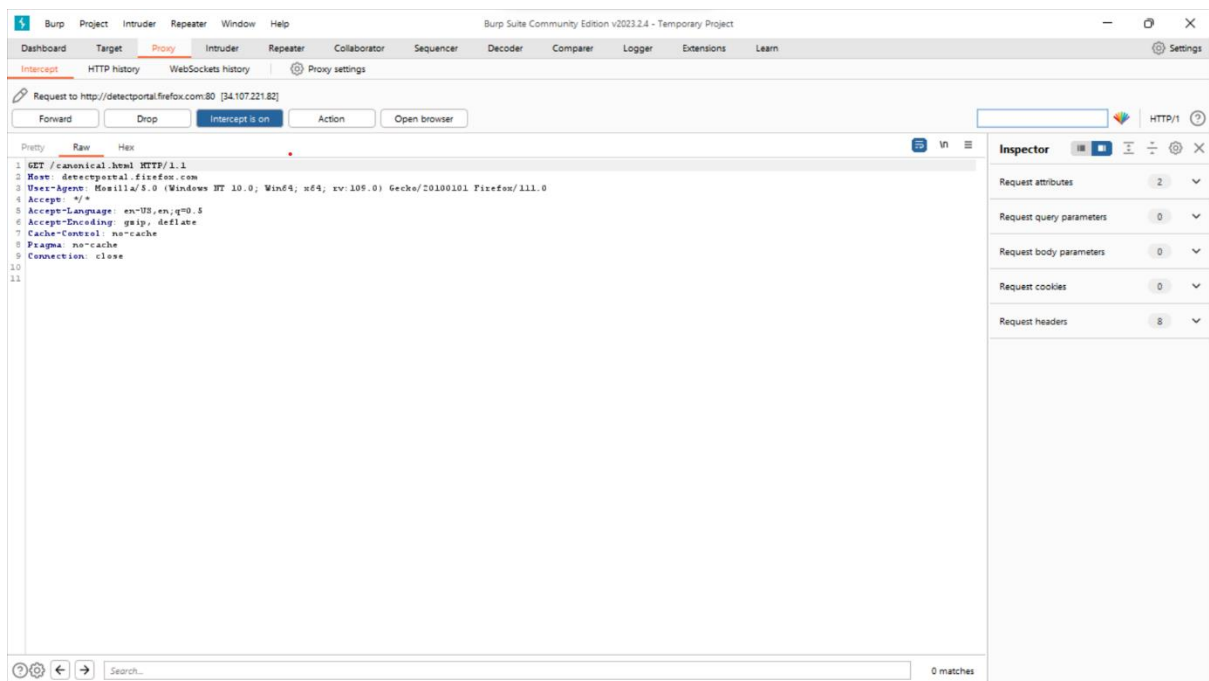
- Start your burp suite and go to proxy. Turn on the intercept.



- 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.

OS command injection, simple

https://0a27008e048604dac3a238100082002b.web-security-academy.net/product?productId=1

Description:

The days of finding your favorite lunch stolen from the fridge in the workplace are over. All manner of items can be hidden within the flesh of this single-use banana skin. Pop them in and seal it up, after all, no-one is going to pinch your banana, are they?

We have a dedicated team of banana eaters here at HQ in Arizona, all in need of boosting their potassium intake. We pride ourselves in being able to support the community and reduce waste by selling on the by-product to you.

No need to leave angry sticky notes all around the kitchen, no need to waste valuable resources by labeling all your foodstuffs anymore.

We are proud of our award-winning product which has earned us a number of small prizes for innovation, propelling us into the World Wide market. We can guarantee all of our bananas are eaten in Europe and the US, ensuring an ethically sourced product, leading to convenience and peace of mind for all of our customers.

We offer a 30-day money back guarantee providing the banana skin is returned to us in its original form, and must still be yellow.

London

[Return to list](#)

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

Request to https://0a27008e048604dac3a238100082002b.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open browser

Comment this item HTTP/2

Raw

```

1 POST /product/stock HTTP/2
2 Host: 0a27008e048604dac3a238100082002b.web-security-academy.net
3 Cookie: session=15d1gmsuao0fns8a1t4L6n03u3p48X
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/111.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0a27008e048604dac3a238100082002b.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 21
11 Origin: https://0a27008e048604dac3a238100082002b.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 productID=1&storeId=1

```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 1

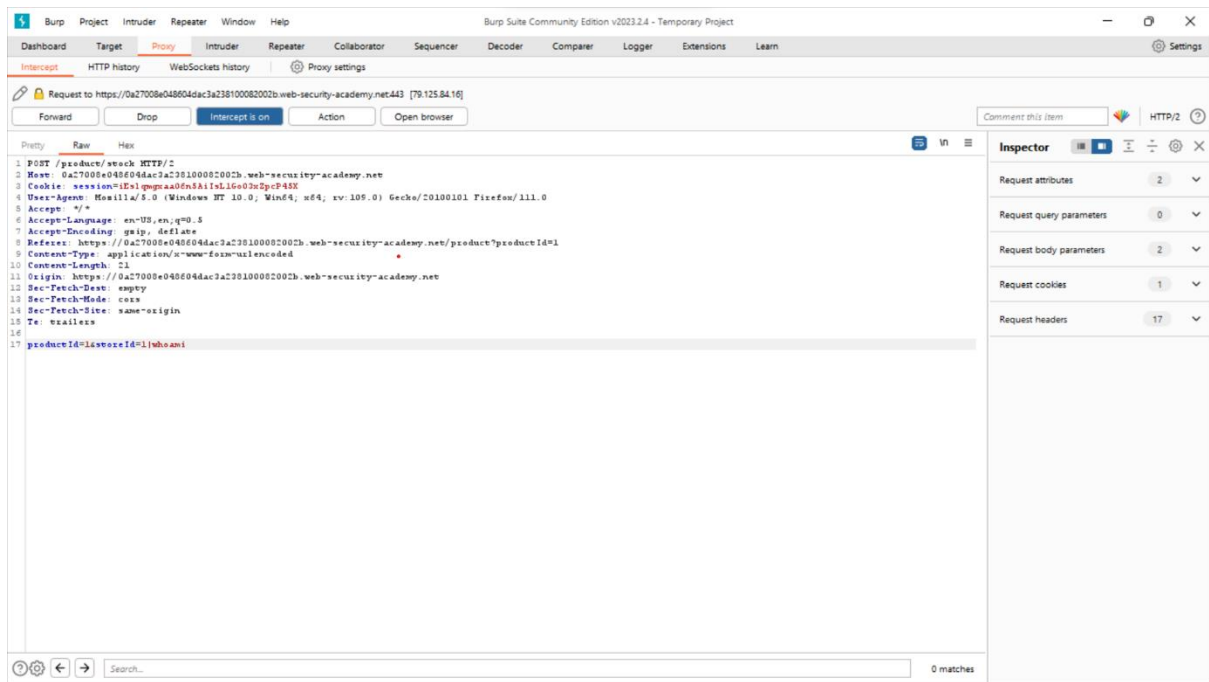
Request headers 17

0 matches

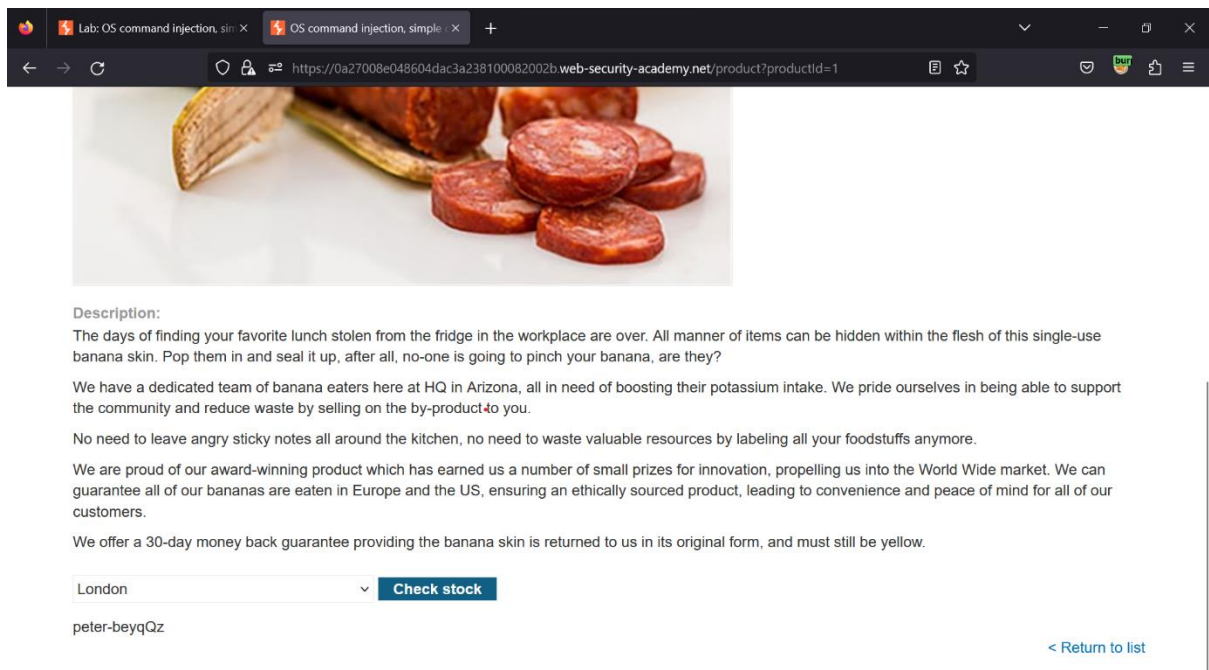
- The packet that requests for the stock option is captured on burpsuite. Change the stored parameter to:

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.