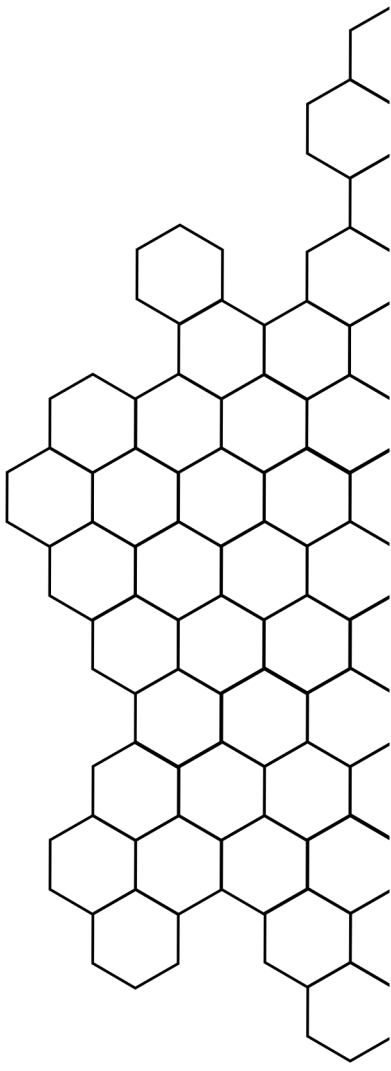
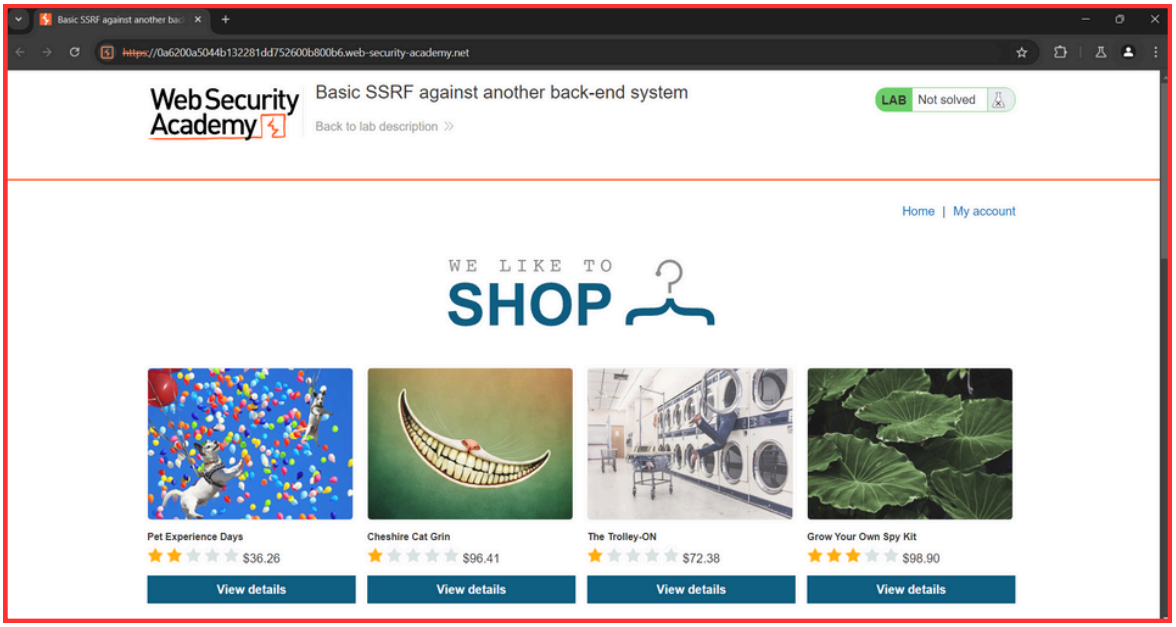
SSRF

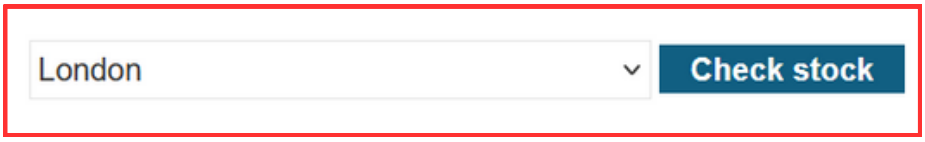
LAB 2

TARİH: 30.08.2024

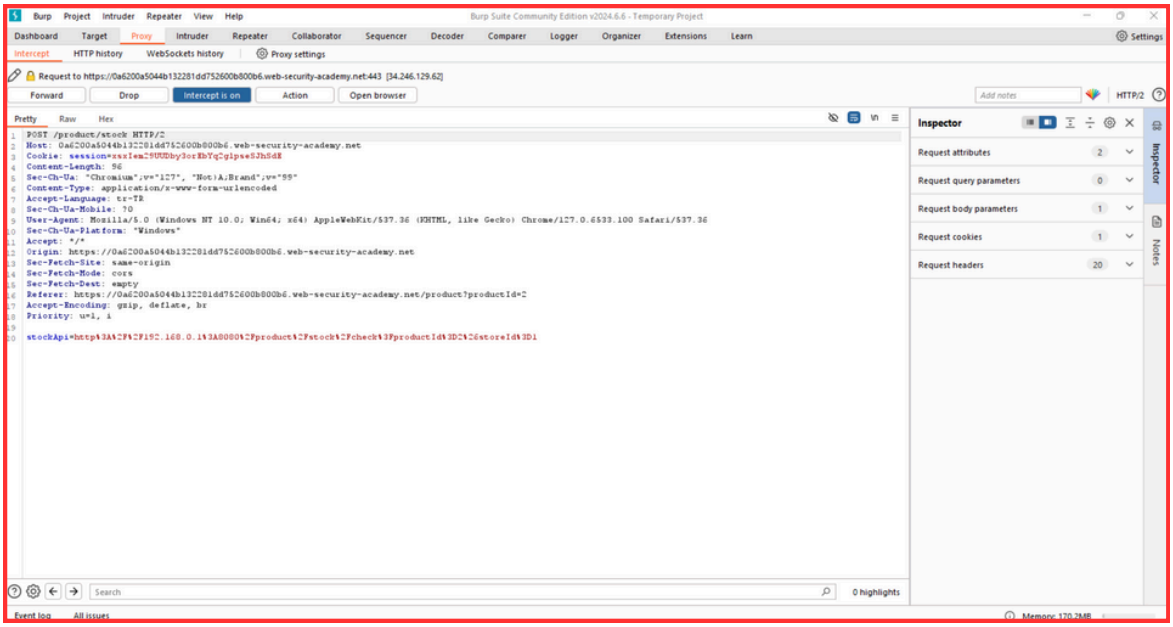


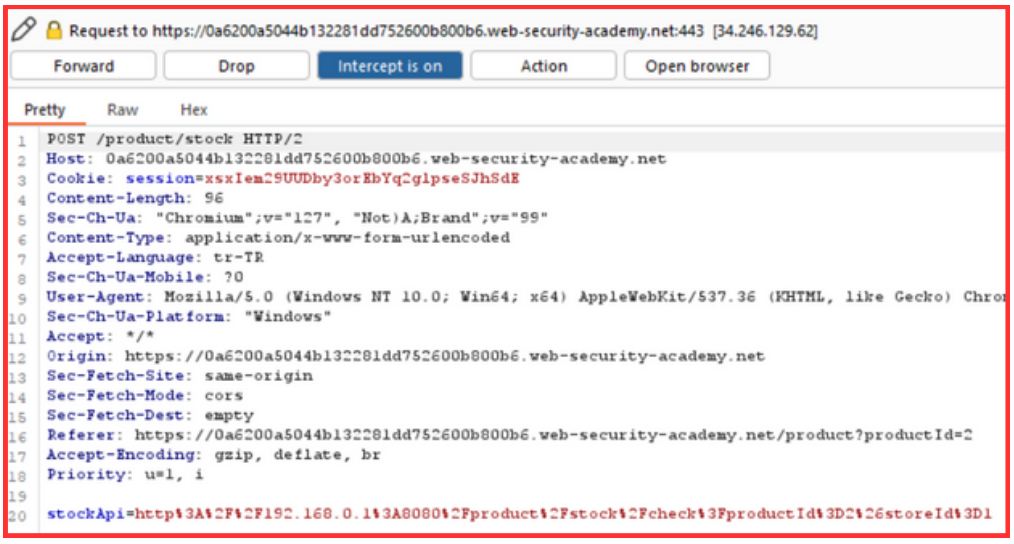


Bu lab için bizden stok kontrol işlevini kullanarak dahili sistemdeki 192.168.0.X aralığını tarayıp, 8080 portunda çalışan bir yönetici arayüzünü bulmamız ve ardından kullanıcı carlos'u silmemiz istenmektedir.

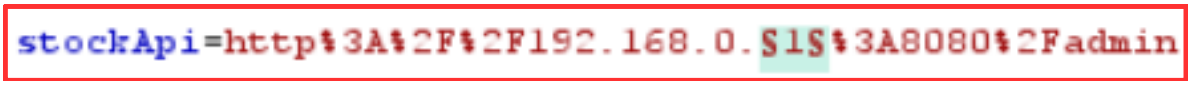


Burada ihtiyaç duyabileceğimiz için önce BurpSuite programını açtım. Ardından bir ürünün sayfasına giderek stok kontrol butonuna tıklayıp bu paketi BurpSuite üzerinde yakaladım.

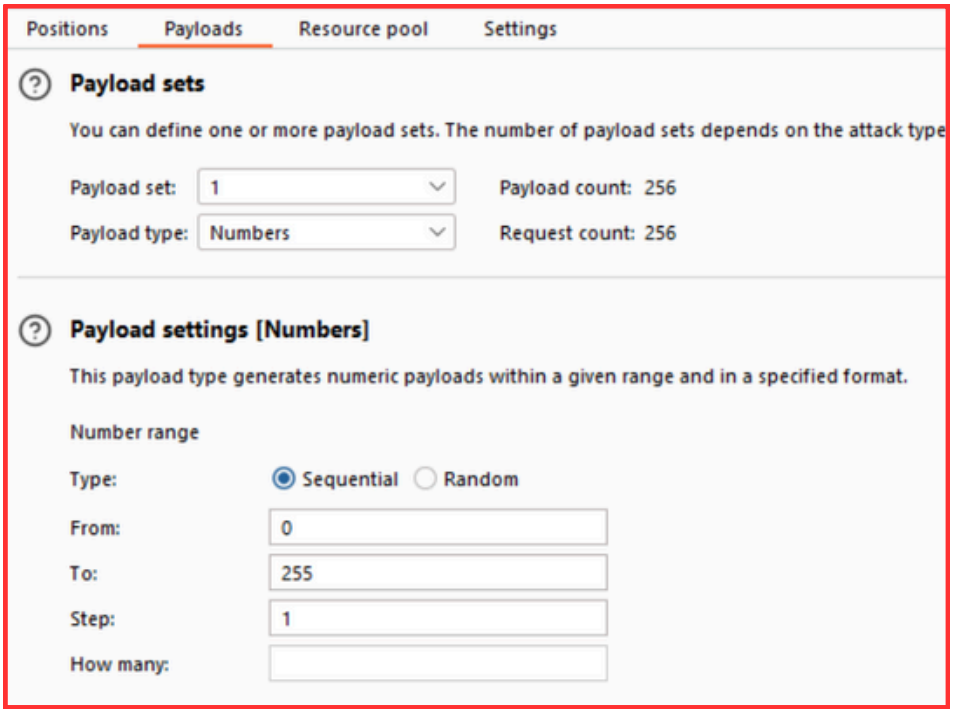




Yakaladığımız HTTP paketi içerisinde stockApi adında bir parametre bulunuyor. Bu parametre içinde bir URL verilmiş, muhtemelen aradığımız kısım burası. Buradaki IP'nin son kısmını değiştirip istenen taramayı gerçekleştiricem. Bunun için paketi Intruder'e gönderdim.



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.

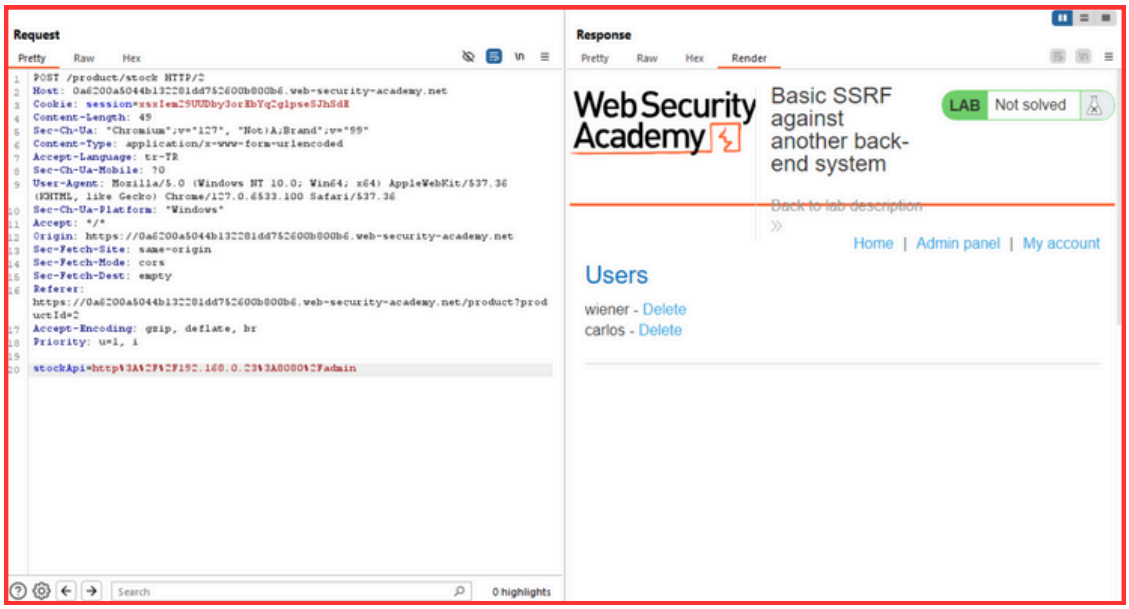


Request	Payload	Status code	Response received
24	23	200	150
0		400	84
2	1	400	88
15	14	500	80
21	20	500	80
22	21	500	80
27	26	500	80
4	3	500	81
8	7	500	81
3	2	500	82
16	15	500	82
28	27	500	82
11	10	500	83
20	19	500	83
32	31	500	84

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.



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