LAB: BASIC SSRF AGAINST ANOTHER BACK-END SYSTEM

https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-backend-system

GÖREV:

Temel SSRF

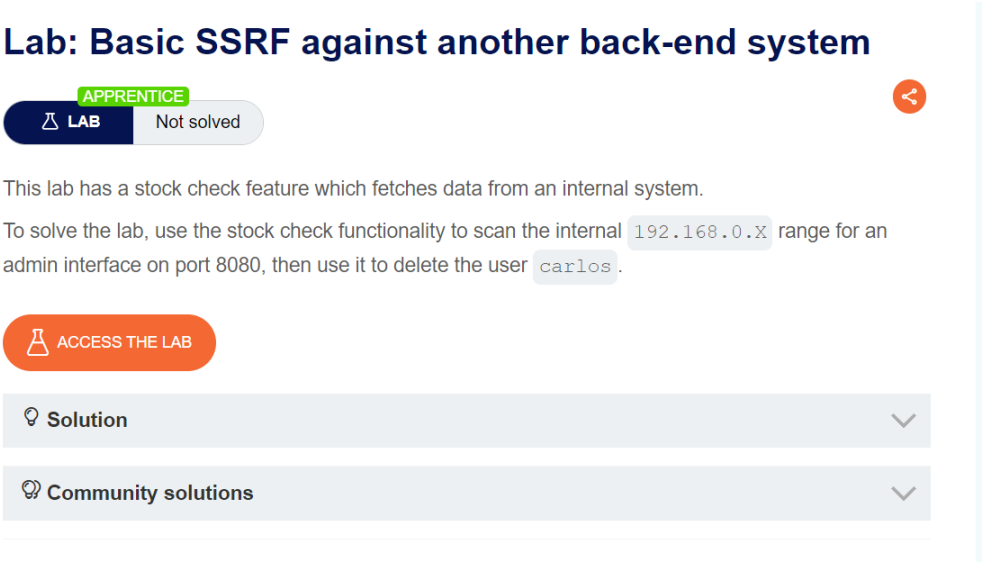
AÇIKLAMA:

Bu lab, dahili bir sistemden veri getiren bir stok kontrol özelliğine sahiptir.

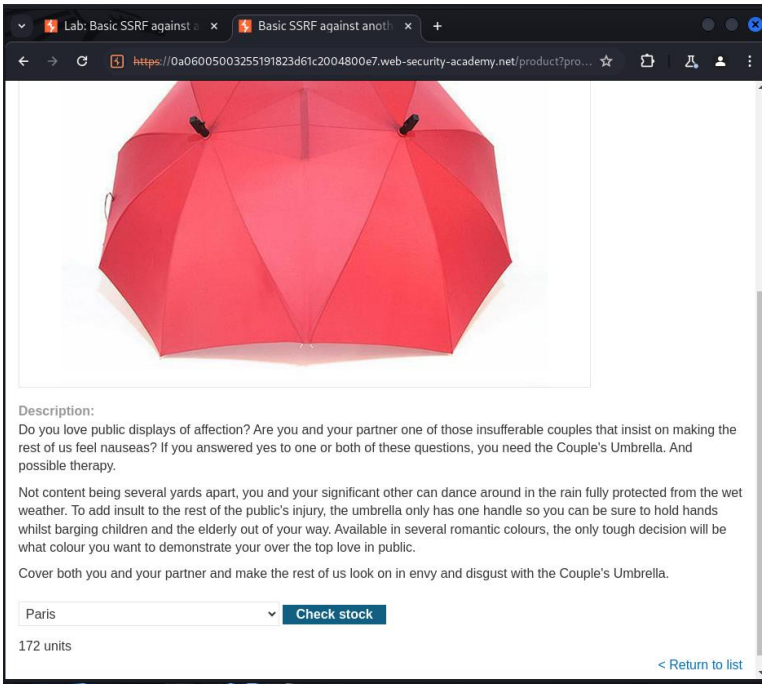
Lab'ı çözmek için, 8080 portunda bir yönetici arayüzü için dahili 192.168.0.X aralığını taramak için stok kontrol işlevini kullanın, ardından bunu kullanarak carlos kullanıcısını silin.

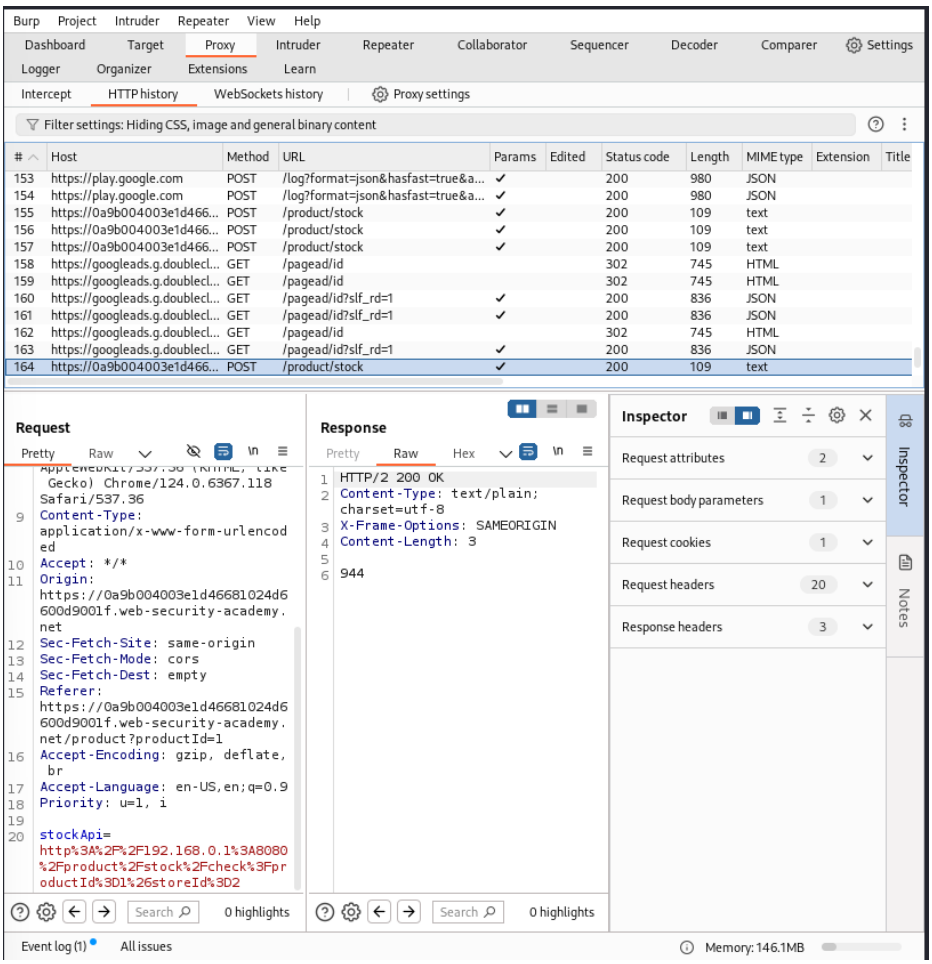
ÇÖZÜM:

Laboratuvara erişimi başlatıyoruz.

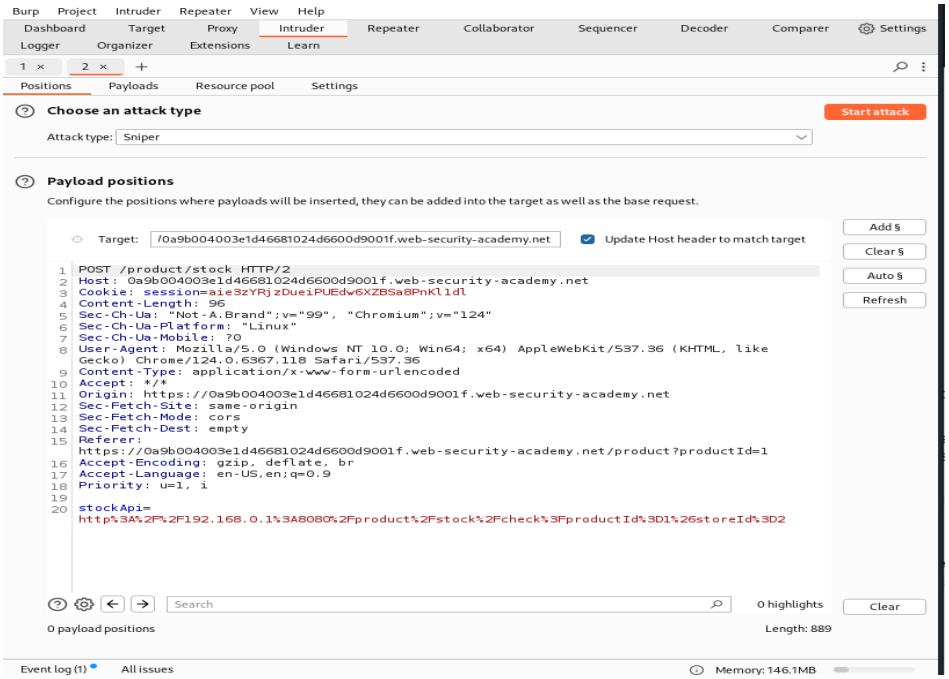


İlk adım olarak "Stok kontrolü"ne tıklayın, Burp Suite'te isteği yakalayıp Burp Intruder'a gönderilmelidir.



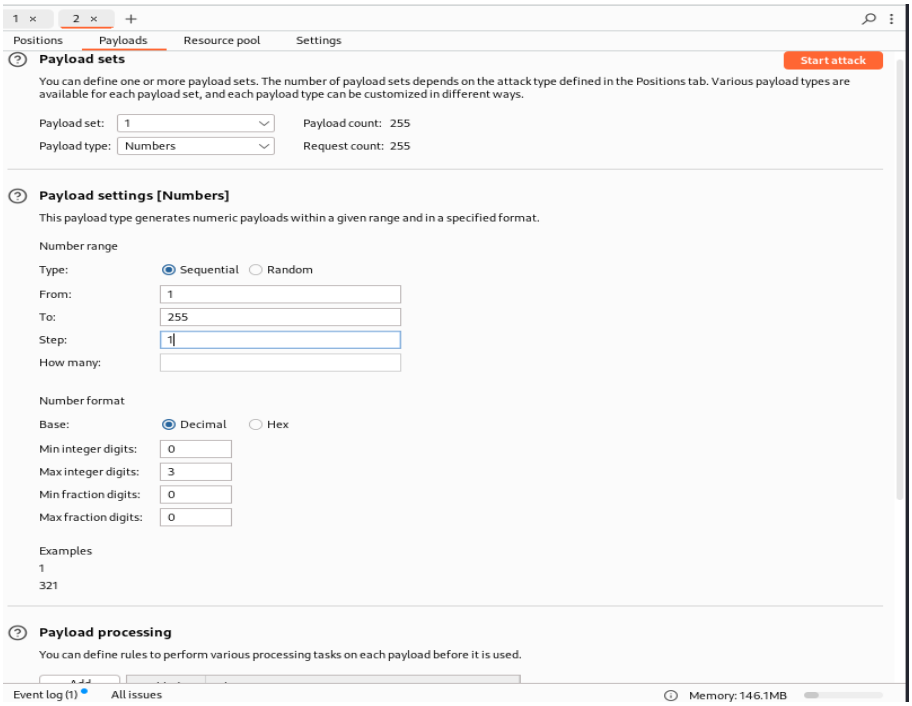


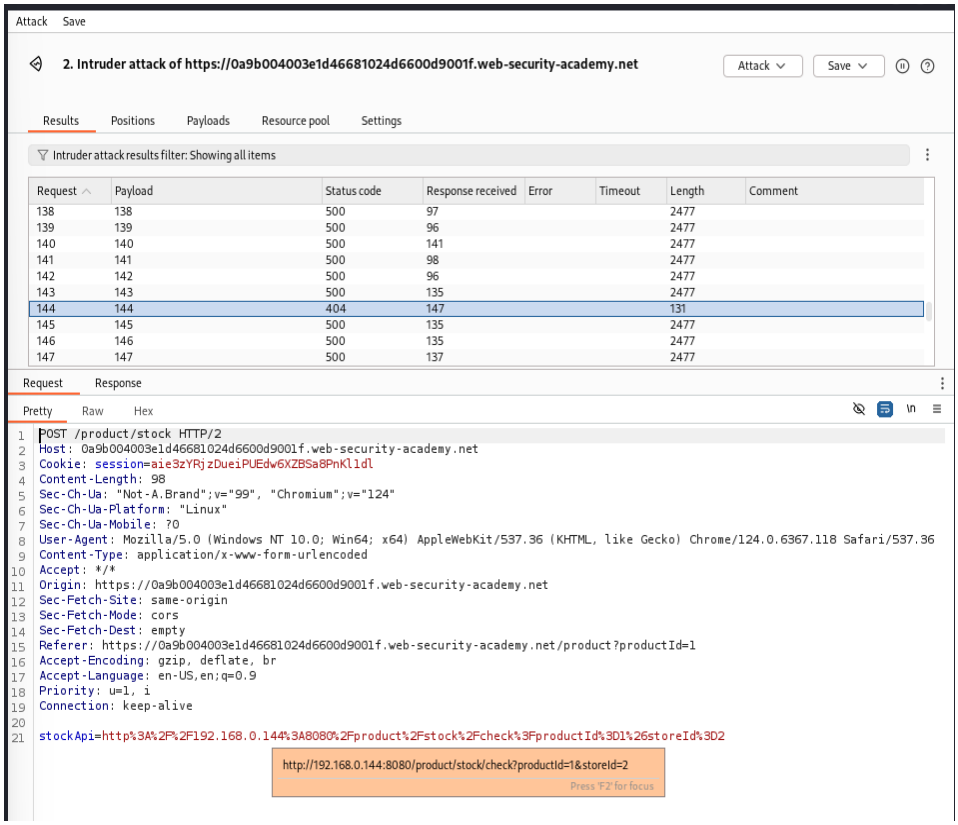
stockApi parametreyi http://192.168.0.1:8080/adminIP adresinin son sekizlisini (sayı 1) vurgulayacak şekilde değiştirin ve "Ekle"ye tıklayın.



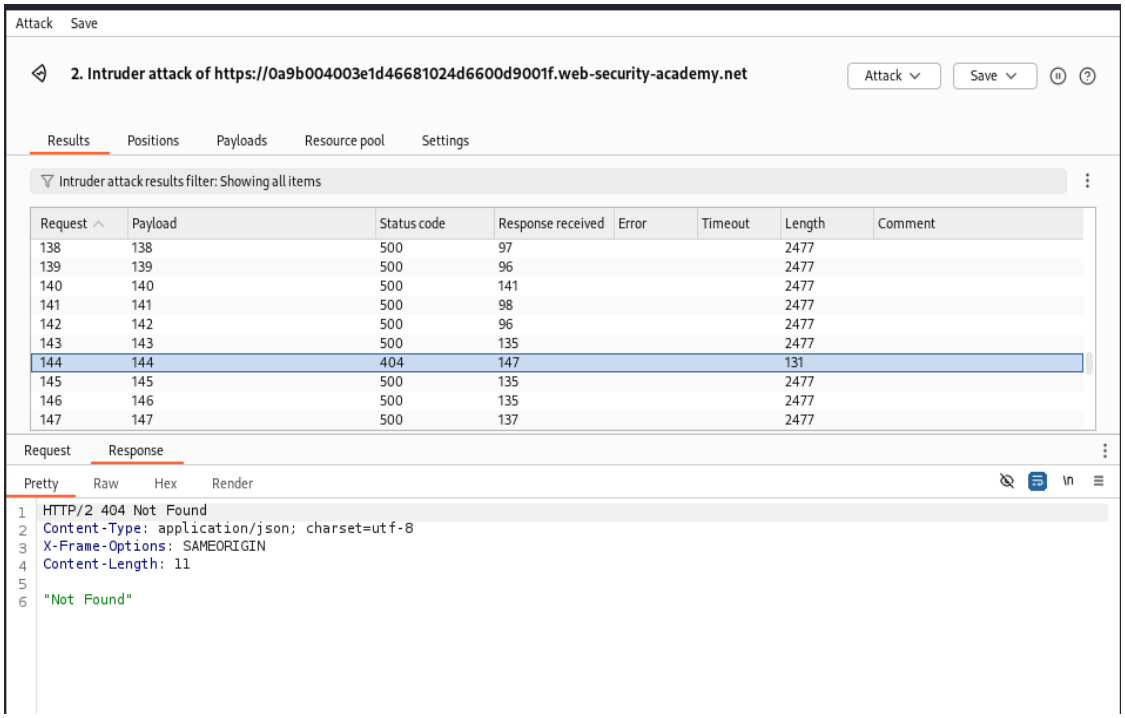

```
stockApi=
http%3A%2F%2F192.168.0.§1§%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D2
```

Payload set ve type değerlerini düzenlememiz gerekmektedir.

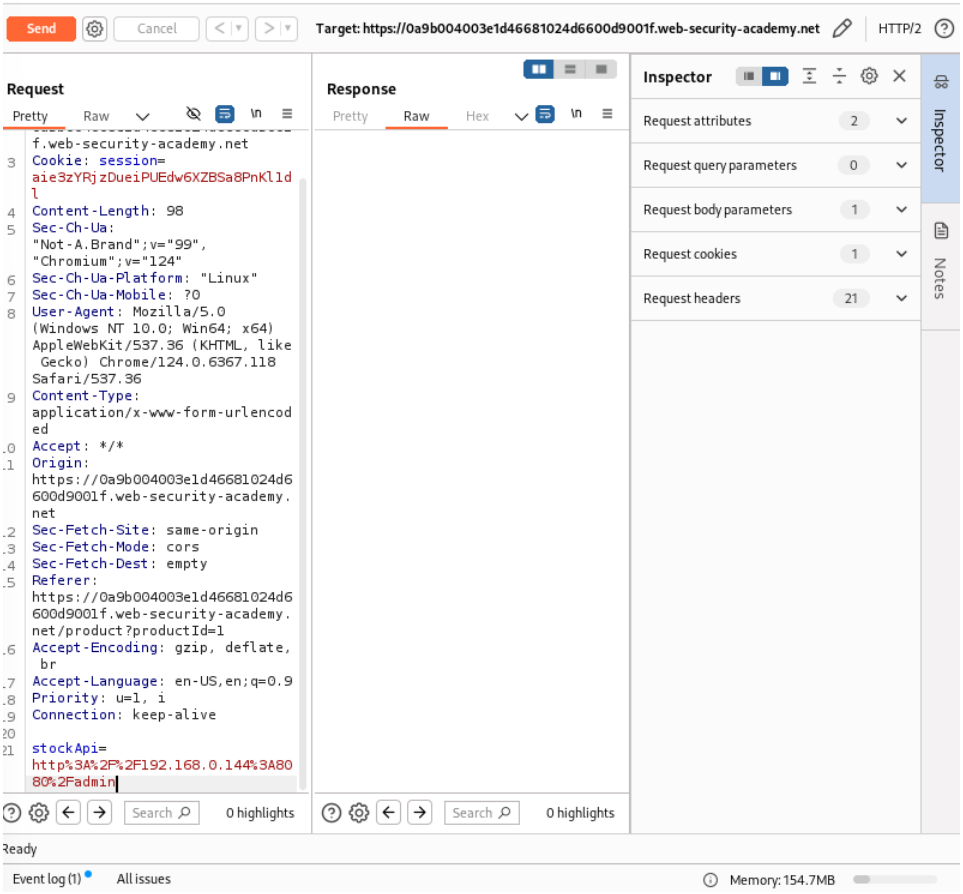




Status Code da “Not Found” bulmamız gerekmektedir.

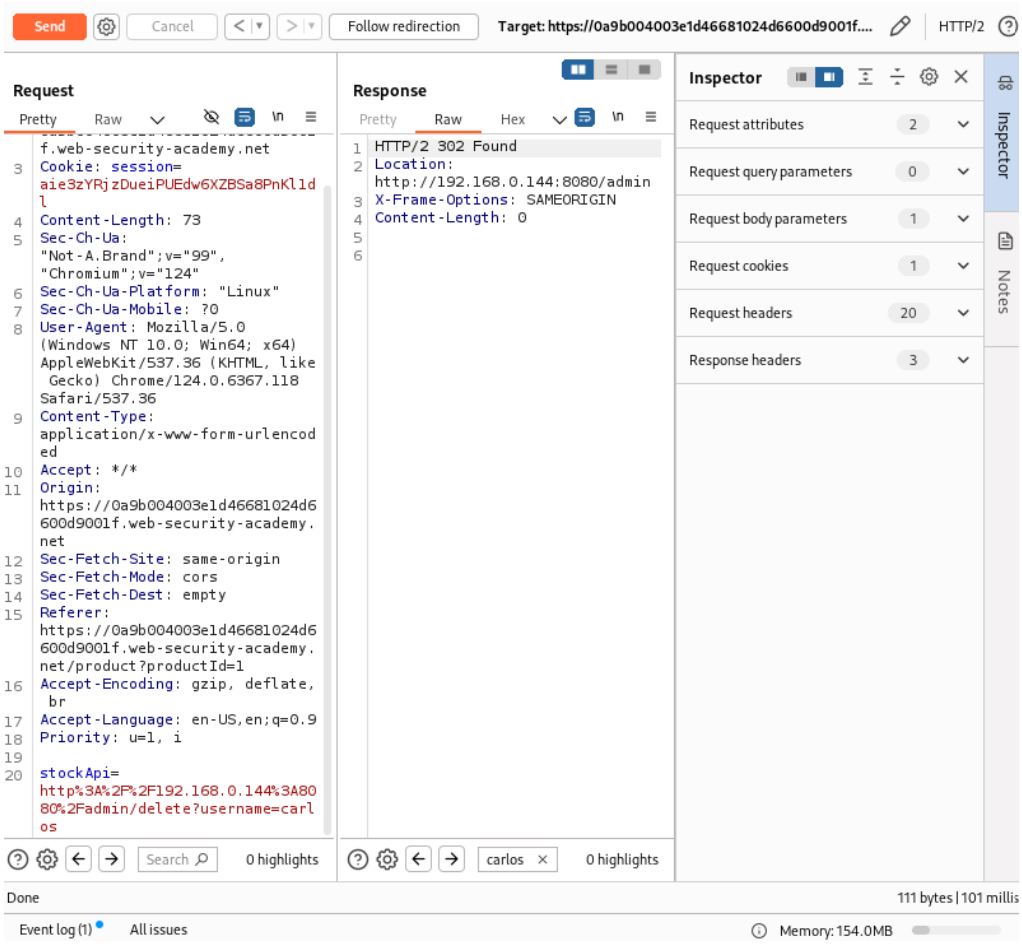


Bu isteği bulup “sent to repeater” yapılması gerekmektedir.

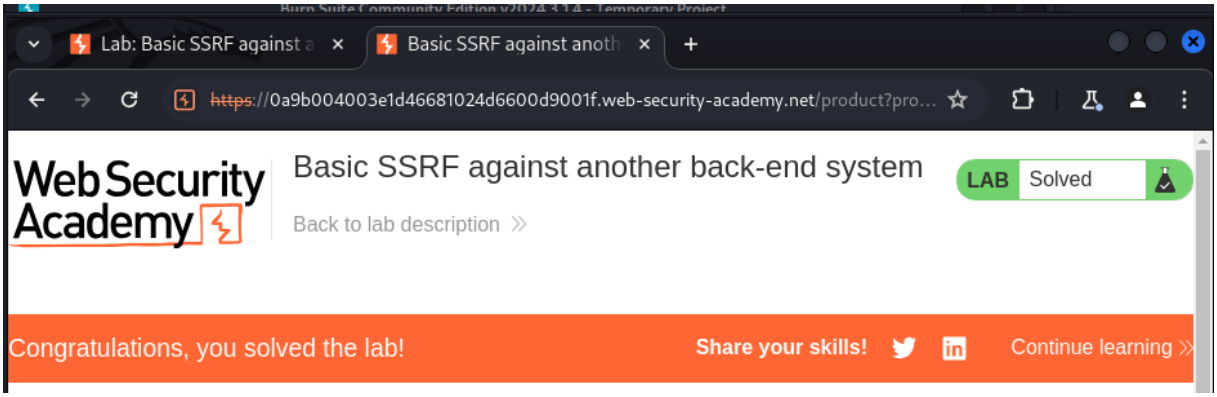


stockApi:/admin/ yazıp carlosu aramamız gerekmektedir.

stockApi değerini admin/delete?username=carlos olarak düzenlememiz gerekmektedir.



Gerekli düzenlemeyi yaptıktan sonra “send” butonuna basıp isteği gönderiyoruz.



Laboratuvarımızı tamamladık.

Şeyma Saylan