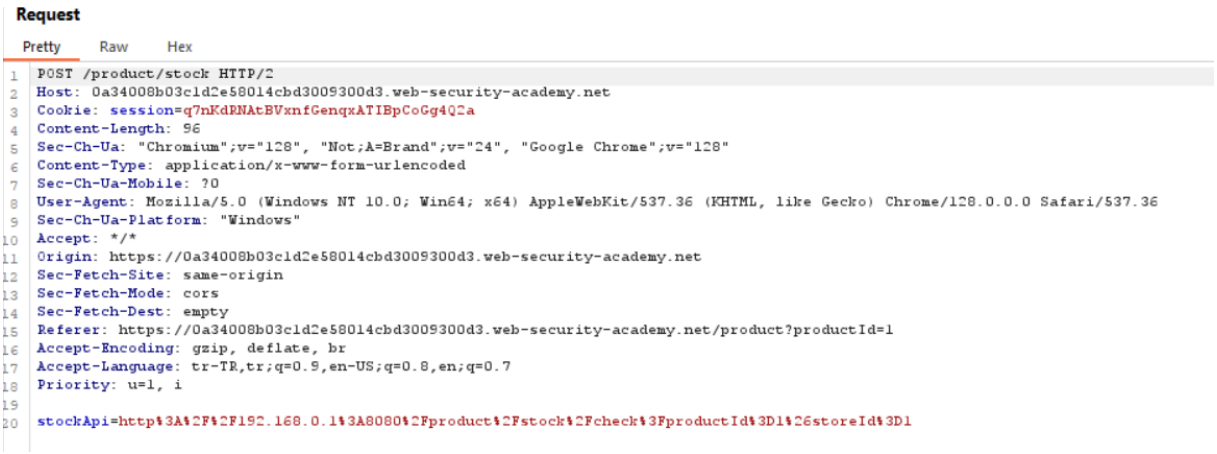
Server-Side Request Forgery (SSRF)

Lab: PortSwigger

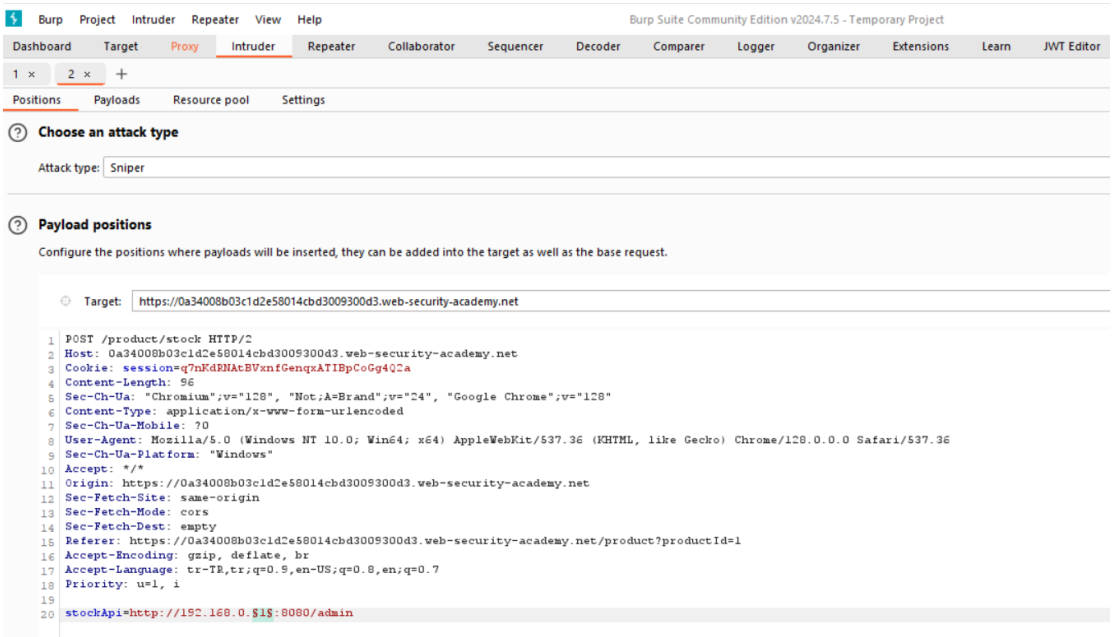
Senaryo: Başka bir back-end sisteme karşı temel SSRF

Çözüm Adımları: Bu laboratuvarın dahili bir sistemden veri çeken bir stok kontrol özelliği var.Laboratuvarı çözmek için, stok kontrol işlevini kullanarak dahili 192.168.0.X aralığı 8080 portunda bir yönetici arayüzü için tarayın, ardından carlos kullanıcısını silin.

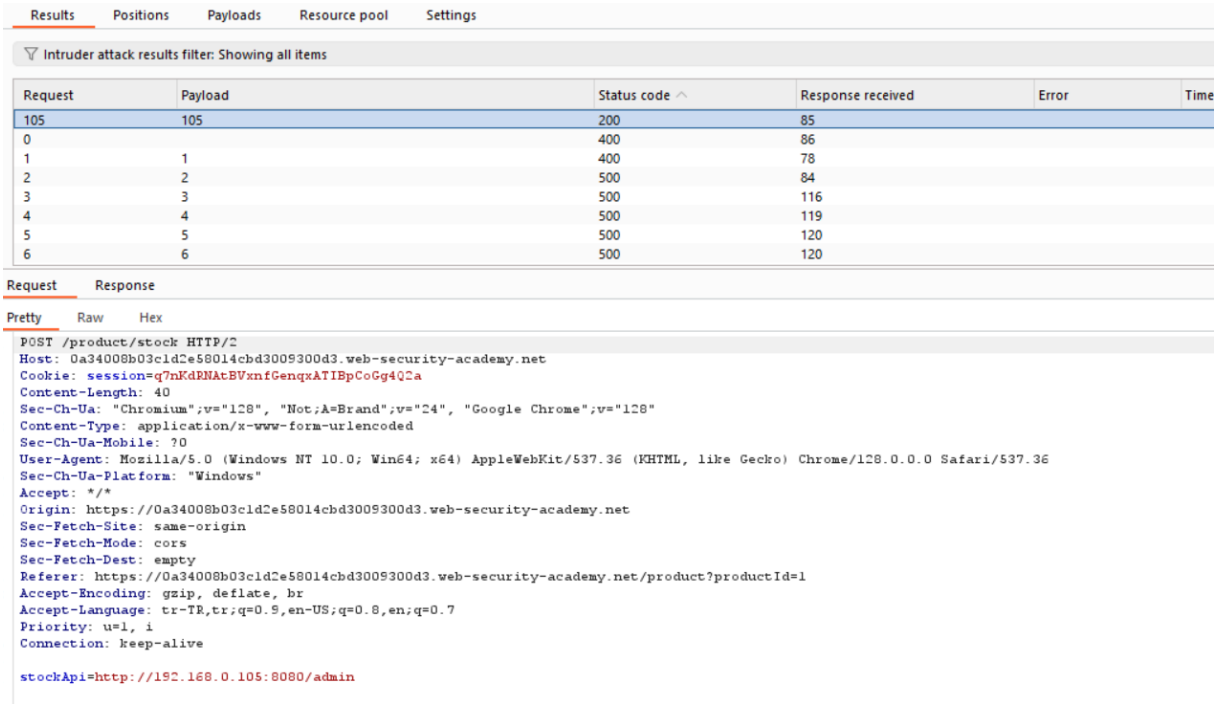
Öncellikle web sitesinde stok kontrolü yapan sayfadaki isteği Burp Suite ile request değerini inceledim.



Bu laboratuvarda, dahili bir IP aralığında (192.168.0.X) çalışan bir yönetici arayüzüne (admin paneli) erişmeniz gerekiyor. Yönetici arayüzünün 8080 portunda çalıştığını biliyoruz.



Burp Suite Intruder kullanarak, **192.168.0.X:8080** IP aralığını brute force ile tarayarak doğru URL'yi buluyoruz.



Doğru URL'yi (admin panelini) bulduktan sonra, Burp Suite'teki stok kontrol isteğinde stockApi parametresine bu URL'yi veriyoruz ve isteği forward ederek sunucuya gönderiyoruz.

Admin paneline erişim sağladıktan sonra, **carlos** kullanıcısını siliyoruz ve laboratuvarı başarıyla tamamlıyoruz. **(http://192.168.0.105:8080/admin/delete?username=carlos)**