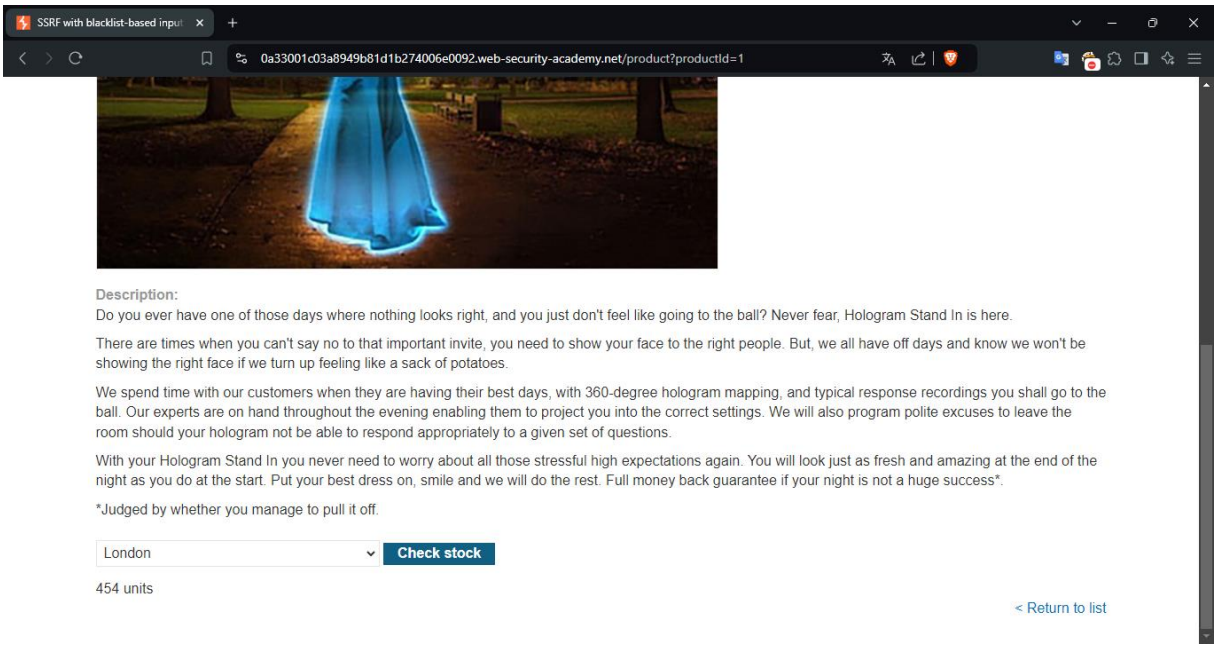
Sercer-Side Request Forgery (SSRF)

LAB_1: SSRF with blacklist-based input filter

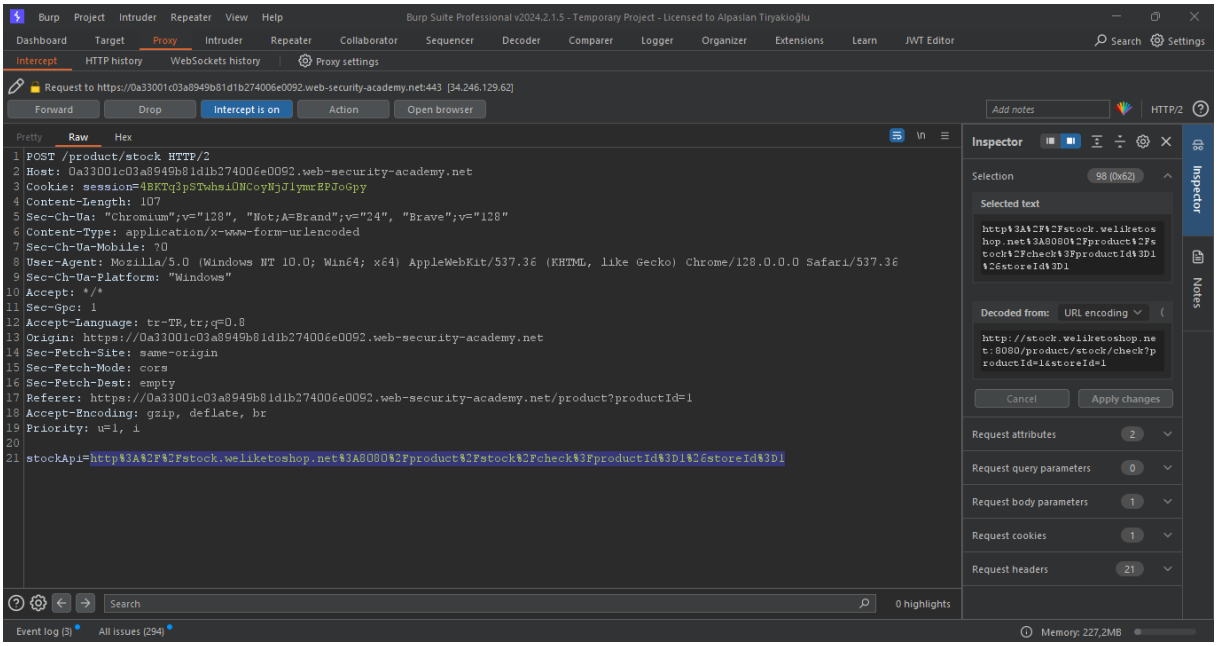
Bu laboratuvarda dahili sistemle iletişim kurup stok kontrol işlemi yapan bir fonksiyonu bulunmaktadır. *https://localhıst/admin* sayfasına gidip *carlos* isimli kullanıcının silinmesiyle laboratuvar çözüme ulaşacaktır.

Bu açıklamamaları okuduktan sonra laboratuvara giriş yapıyorum. Stok kontrol fonksiyonunu test etmek için site içerisindeki ürünlerin bir tanesine giriş yapıp fonksiyonu çalıştırıyorum.

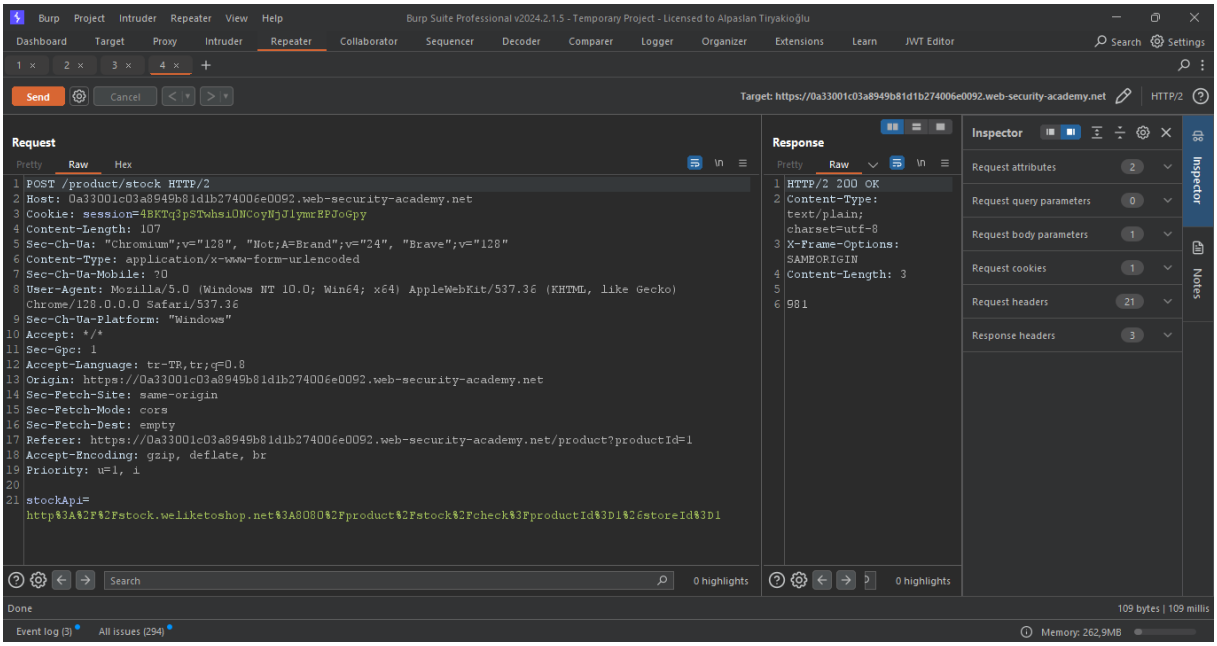


Görüldüğü gibi altta stok çıktısı beliriyor.

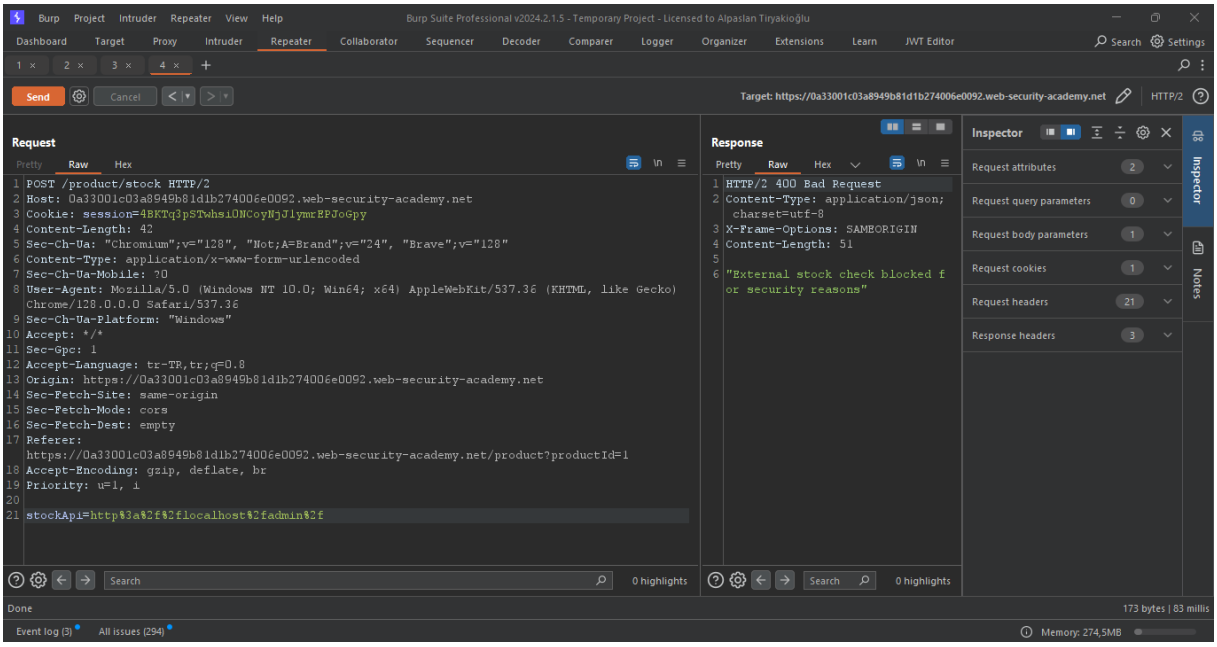
http paketini inceleyip nereyi manipüle edebiliriz buna bakalım.



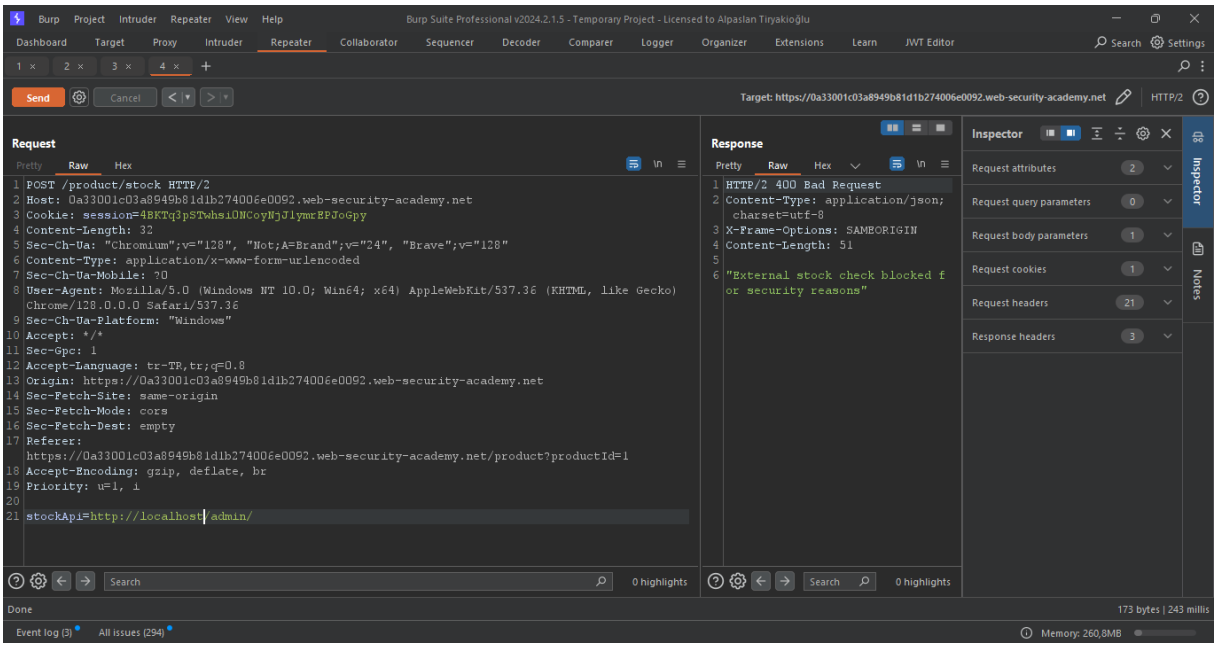
Tek pakette işlem gerçekleşiyor ve bariz şekilde URL'yi görebiliriz. Ancak burada URL encoding işlemi uygulanmış. İlk bakışta anlaşılıyor. Eğer anlayamazsak merak ettiğimiz kısmı seçip sol taraftaki Inspector kısmından akıllı çözüme ulaşabiliriz. Bu paket üzerinde çalışacağımız için repeater aracına gönderip işlemlere başlıyorum.



Rahat görme ve işlem yapmak için bu şekilde ayarladım. İlk başta direkt olarak admin sayfasına gitmeye çalışalım.

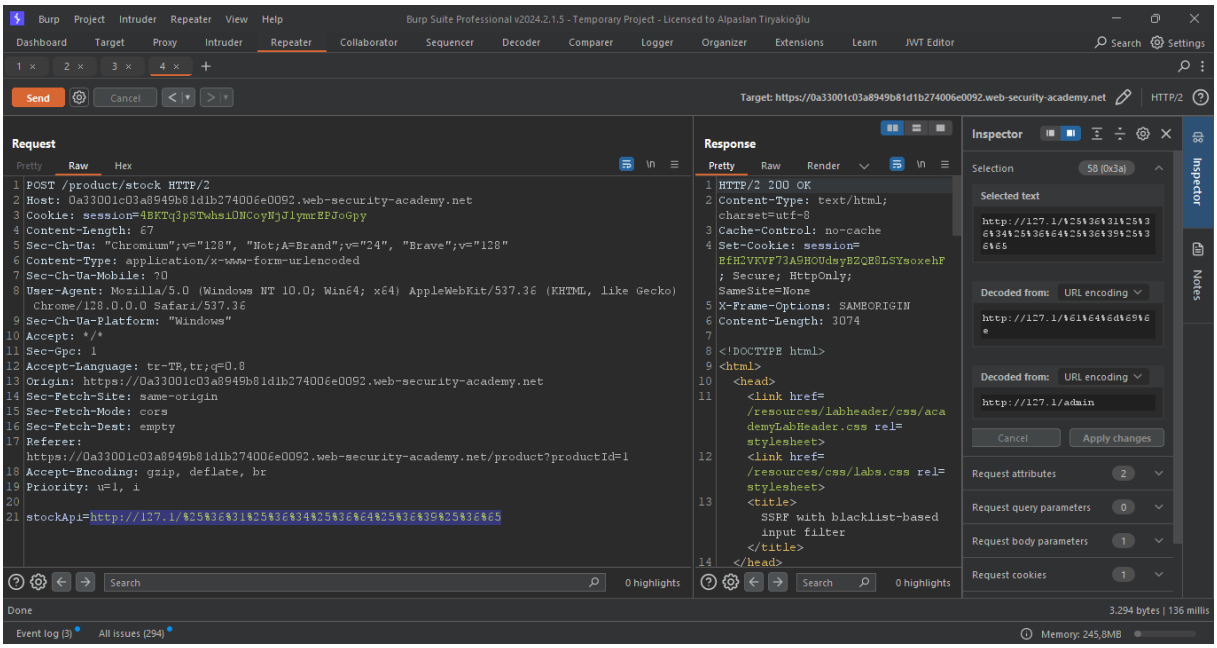


HTTP 400 hatasını döndürdü. URL encoding yapmamıza rağmen. Localhost'a gitmek için kullanabileceğimiz farklı adreslerde mevcut. 127.0.0.1, 127.1; bunlar localhost'a gitmek için kullanılabilir ancak bunlarda da herhangi bir etki alamadım. URL encoding kullanmadan gitmeyi deneyelim.

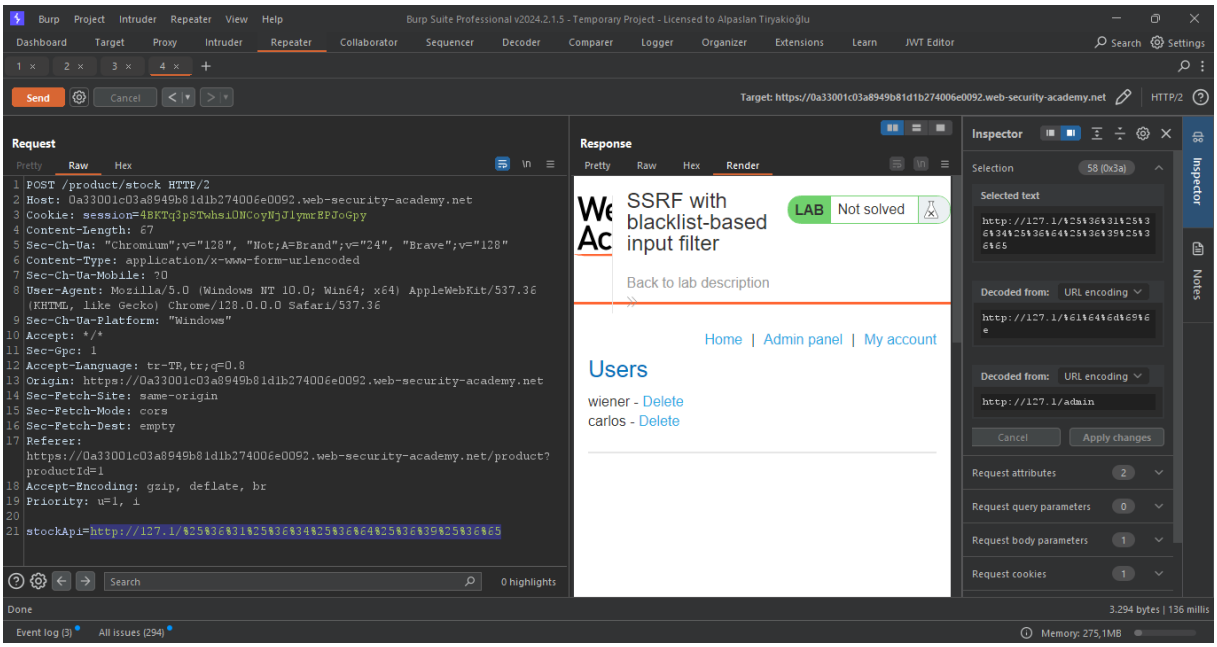


Burada da herhangi bir değişiklik göremedik.

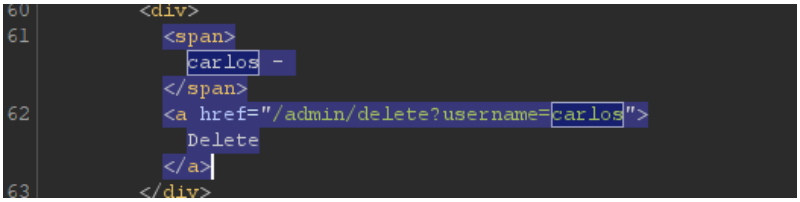
Dikkat çeken bir durum, site kaynak kodlarında iki adet JS kodu kaynak gösterilmiş. Bir tanesi stok kontrolünü ekrana basıyor bir tanesinde ise URL encoding ile ilgili komutlar yazıyor. Gitmek istediğimiz adreste url encoding yapmayı denemek çözüm olabilir.



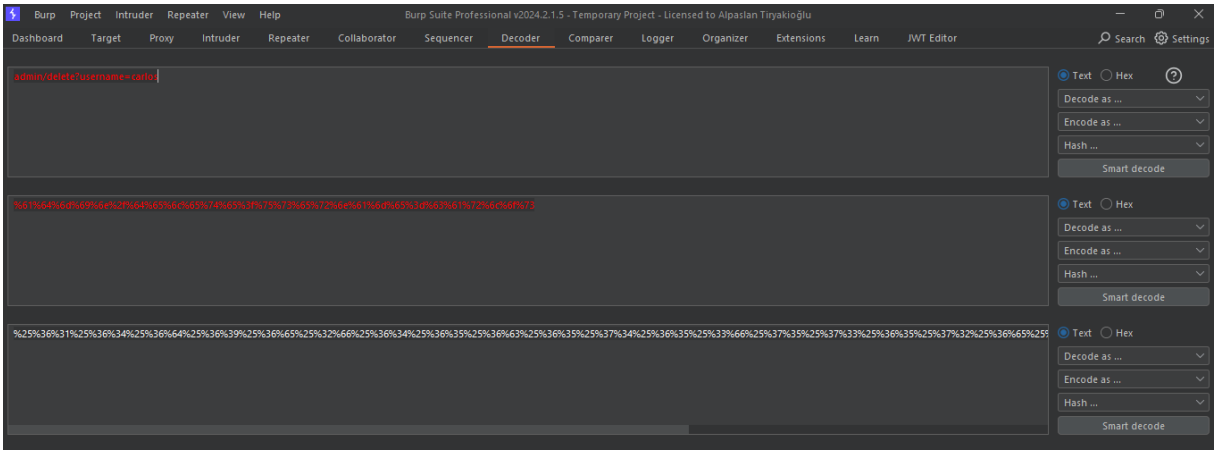
Evet son yakaladığımız ipucu ile bir kere URL encoding yaptım ve sonuç değişmedi. Mantıken de 1 kere şifrelersem çözümlendiğinde cleartext olacak. Şifreli şekilde gitmesi için iki kere encode etmemiz gerekli. Bunu yaptıksan sonra yüklenen sayfanın render almış haline bakalım.



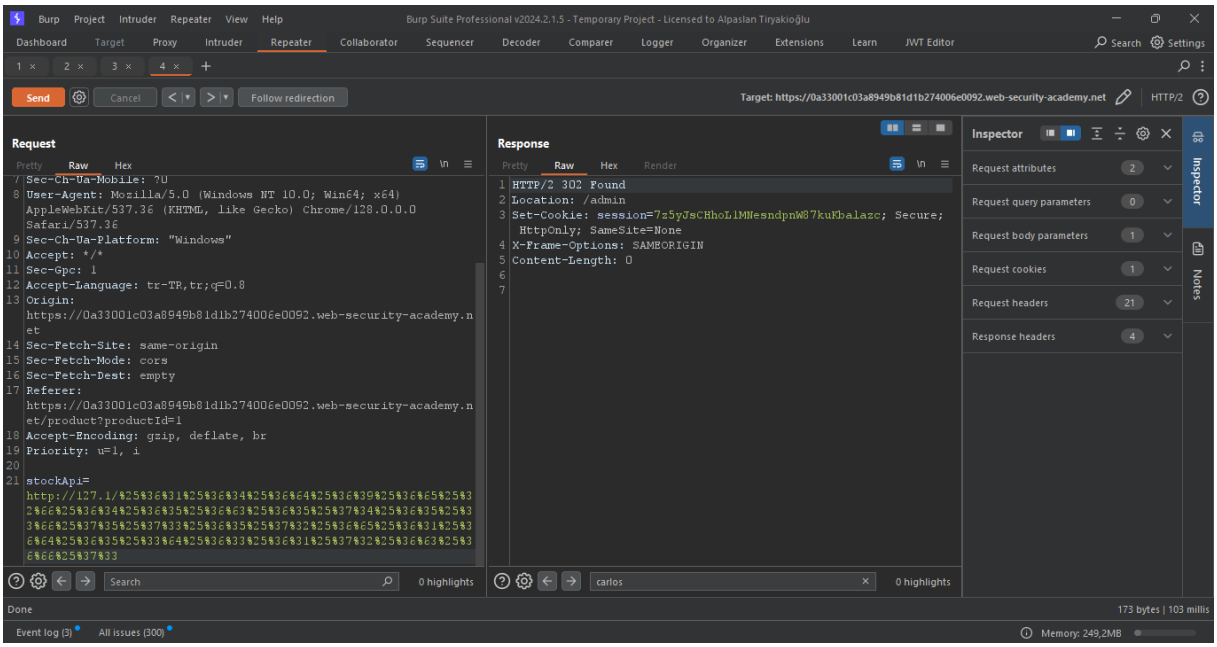
Görüldüğü gibi admin paneline erişim sağlanmış. Kaynak kodundan carlos kullanıcısının delete fonksiyonunun nasıl çalıştığına bakalım.



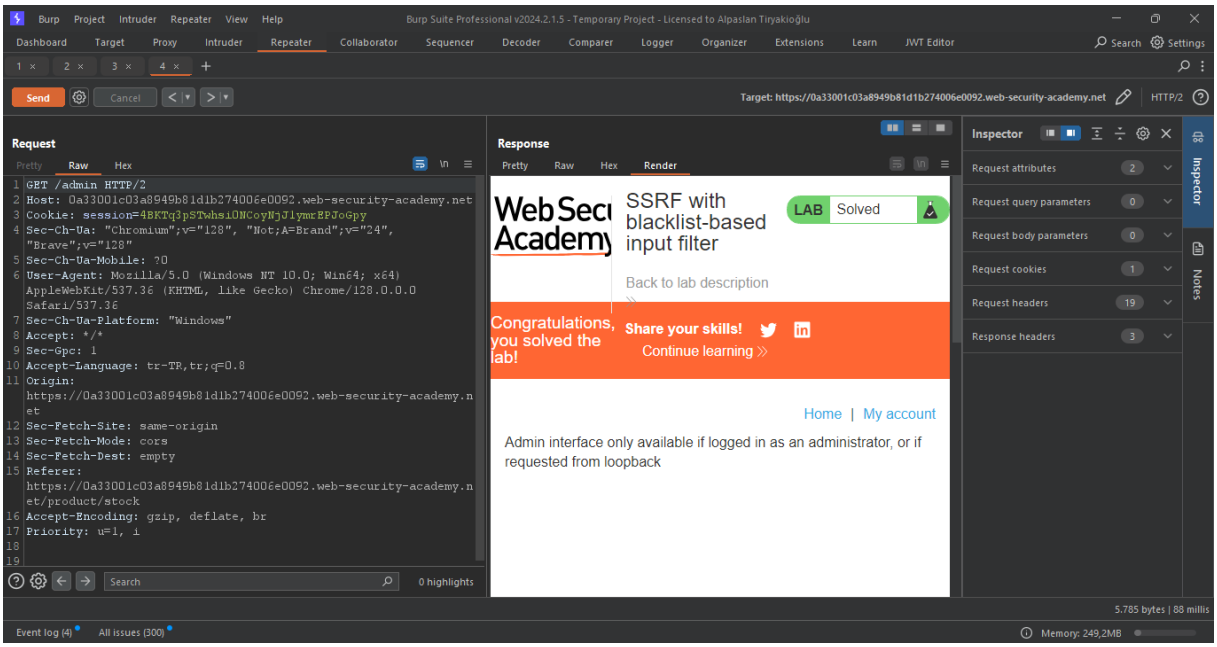
Bu parametreyi ve adres gittiğimiz istismar ettiğimiz adresin sonuna eklediğimizde işlemin tamamlanmış olması gerek.



Decoder aracında path kısmını iki kere encoding işleminden geçirdim. Ve artık paketi gönderebiliriz.



Delete fonksiyonundan sonra yönlendirme olarak /admin adresi verildiği için buraya gitmemiz için paket döndürüyor. Sol üstten follow redirection seçeneğine basarsak yönlendirmenin nereye gittiğini görebiliriz.



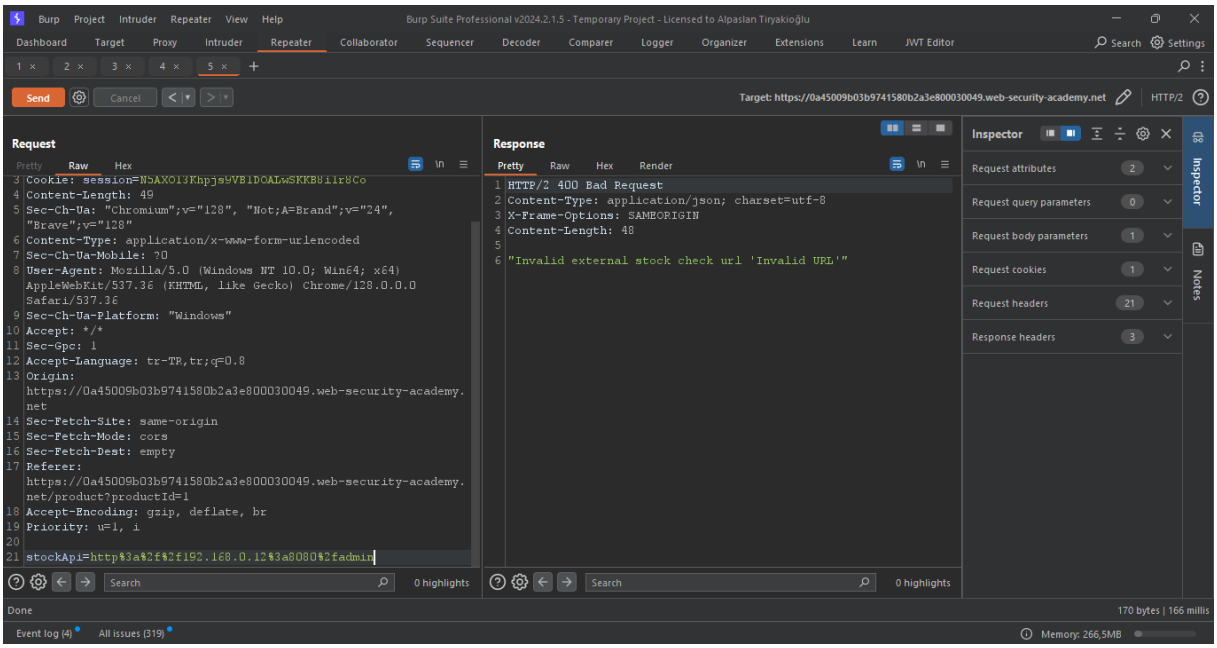
Yönlendirme sonucunda işlemin başarıyla tamamlandığını görebiliriz. Ancak tabi ki hata mesajı da bulunmakta. Admin yetkilerine sahip olmadığım için bu hatayı aldım ama SSRF zafiyetini istismar ederek istediğim işlemi gerçekleştirdim.

LAB_2: SSRF with filter bypass via open redirection vulnerability

Bu laboratuvarda dahili sistemle iletişim kurup stok kontrol işlemi yapan bir fonksiyonu bulunmaktadır. Stok kontrolü yaparak *http://192.168.0.12:8080/admin* adresine giderek *carlos* kullanıcısının silinmesi gerekiyor.

Stok kontrol fonksiyonu yalnızca yerel uygulamaya erişimle sınırlandırılmıştır bu nedenle başka bir yönlendirme bulmanız gereklidir.

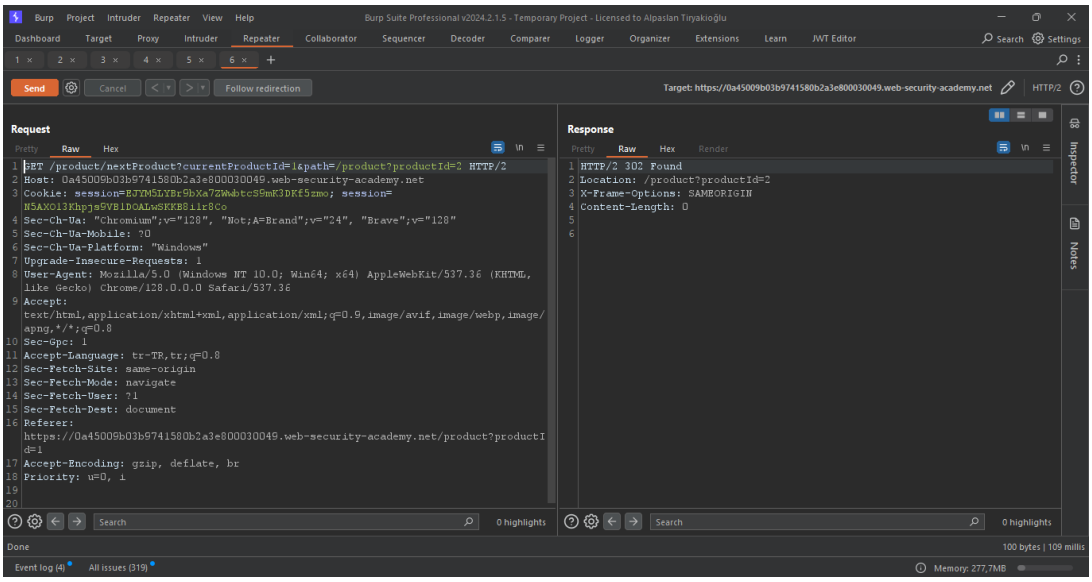
Laboratuvar açıklamalarını okuduktan sonra öncekinde olduğu gibi direkt stok kontrolü parametresinden işlem yapamayacağız anlaşılan. Yine de deneyip aldığımız hataya bakmak gerekir.



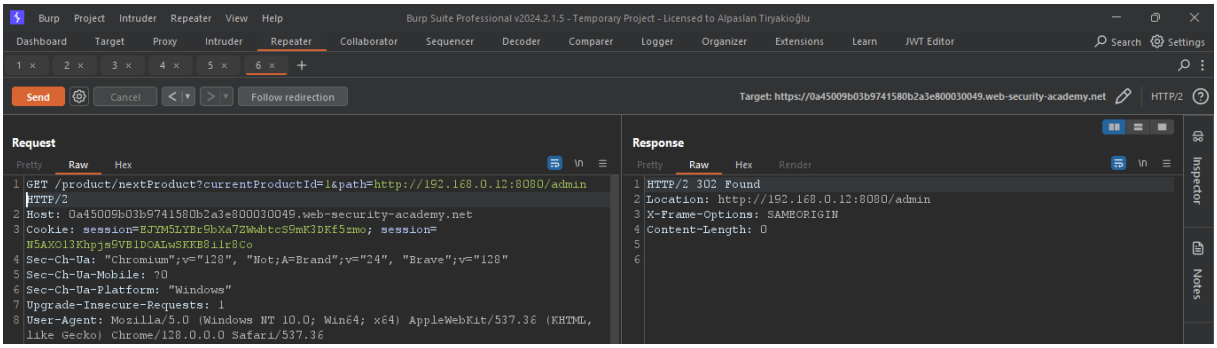
Gördüğümüz gibi denediğim farklı yöntemlerle de erişim elde edemedik. Site içerisinde gezmeye başlayalım.

Alt kısımda bazı yönlendirmeler bulunmakta. Site içerisinde direkt olan yönlendirmeleri bulmak için kaynak koduna da bakabiliriz.

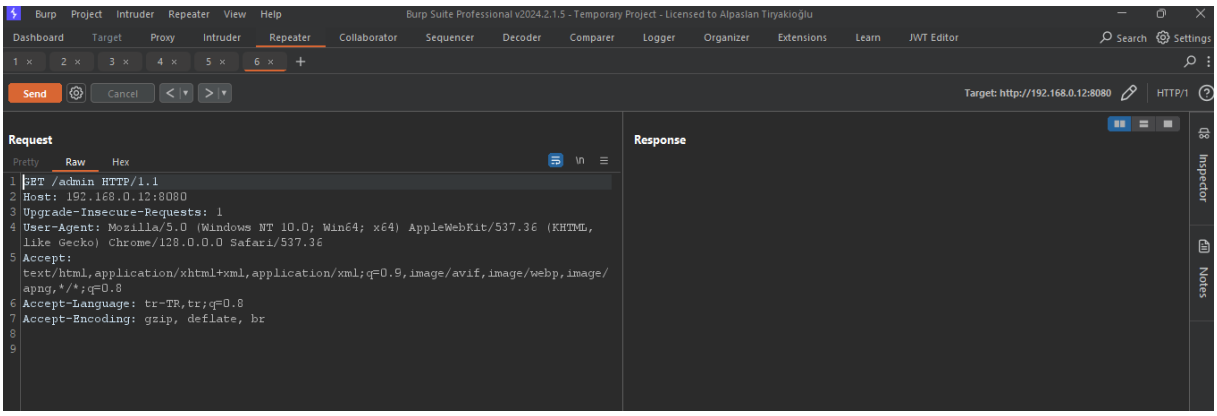
Buradaki kodda "*return to list*" bağlantısının "/" dizinine gittiğini, "*next product*" bağlantısının ise *"/product/nextProduct?currentProductId=1&path=/product?productId=2"* adresine gittiğini görüyoruz. Burada açıkça bir path ve yönlendirme mevcut. Butonu denediğimde de çalıştığını keşfettim. Bunu Burp Suite ile açıp deneyelim.



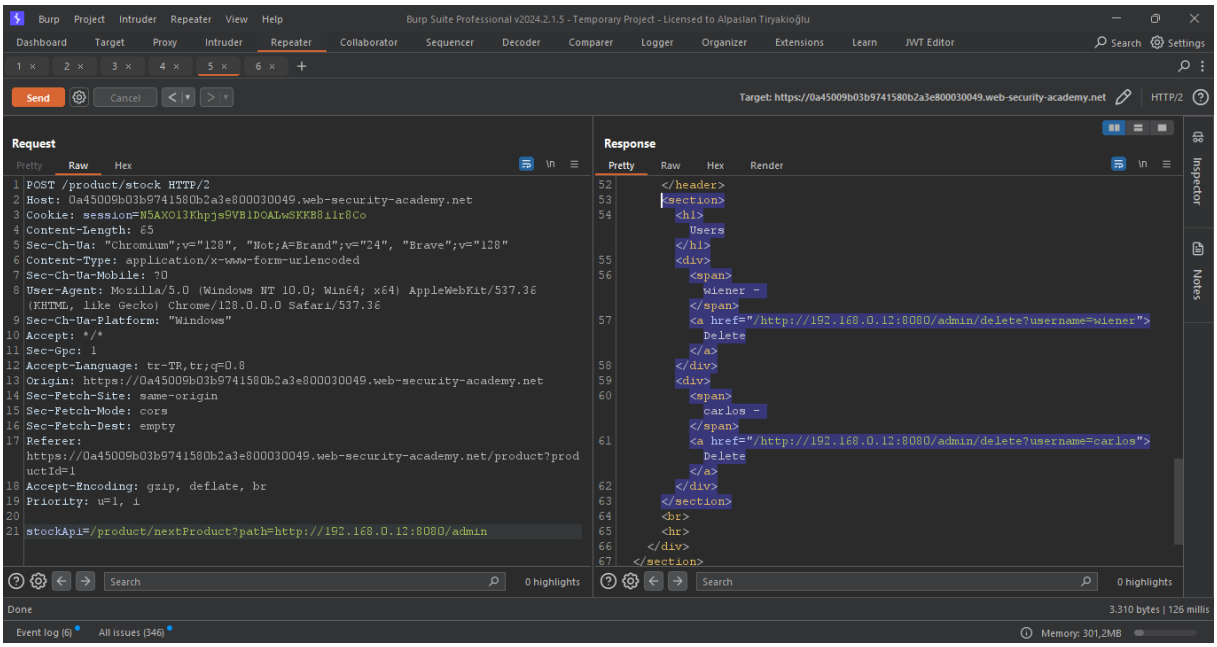
Yönlendirme ile bir yere gittiğini artık gerçekten tescillemiş olduk. Artık bu konumda işlemler yapabiliriz. Gitmemizi istediği adresi direkt olarak buraya koyup deneyelim.



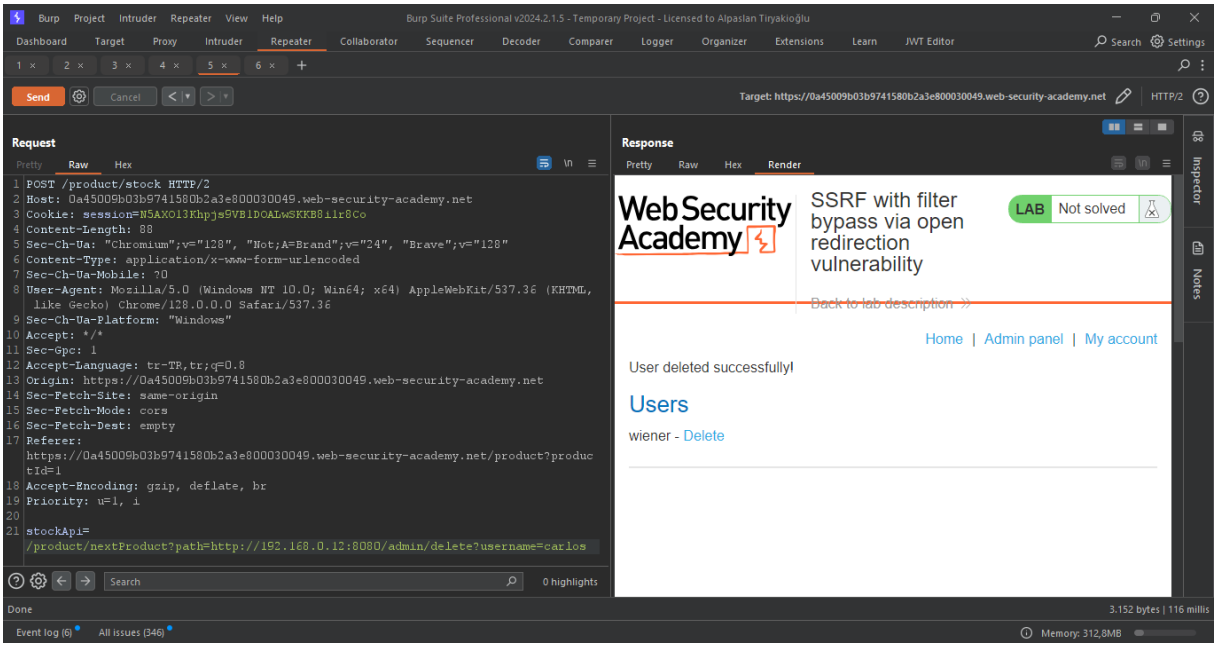
Yönlendirme olduğunu gördük. Follow redirection diyerek gittiği konumu doğrulayalım.



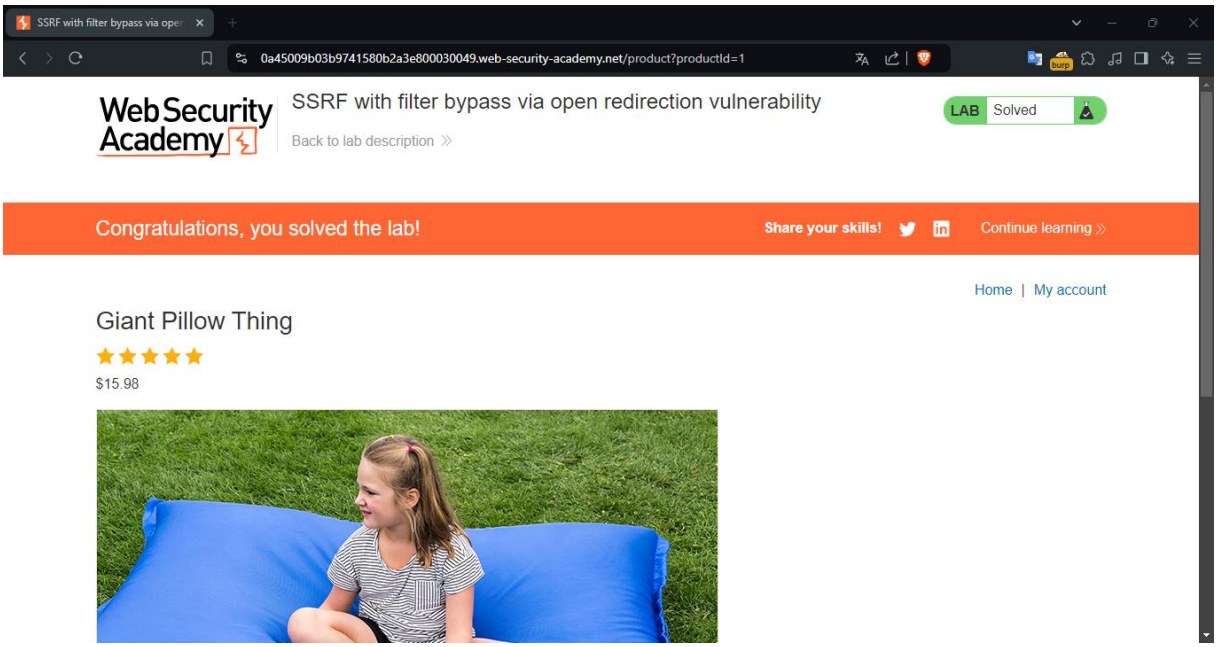
Direkt olarak buraya erişimim sağlayamıyoruz. Buradaki yönlendirmeyi başka bir yerde kullanmak mantıklı olabilir. Örneğin StokApi paketindeki değişkene değer olarak buradaki path'i vermek işe yarayabilir. Sonuç olarak ilk yönlendirme sunucu içinde olacak. Bu yüzden başarılı olabiliriz.



Önceki pakete geçip aldığımız path'i biraz değiştirdim. Mevcut ürün ID'sini sildim ve sadece path kalacak şekilde adresi ayarladım. Direkt olarak kaynak kodundan admin sayfasına eriştiğimizi görebiliriz. Bundan sonra kalan tek işlem kullanıcıyı silmek tıpkı diğer laboratuvarda olduğu gibi.



Silme işlemi başarıyla gerçekleşti.



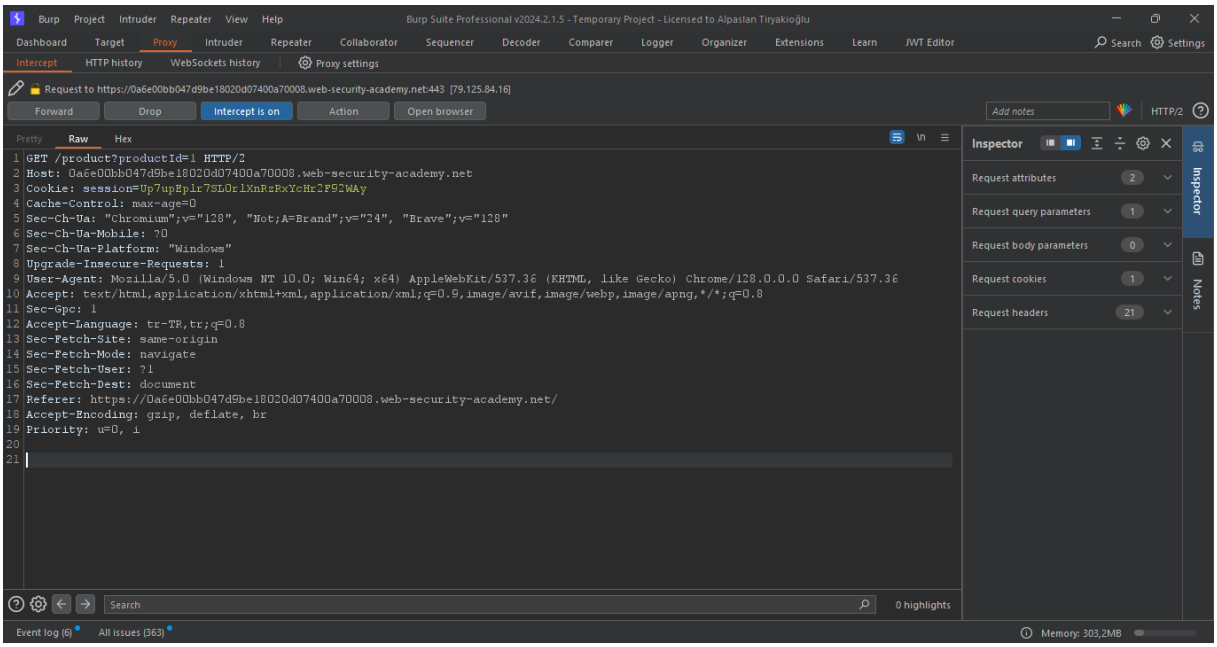
Tarayıcıda da bu şekilde görebiliriz.

LAB_3: Blind SSRF with out-of-band detection

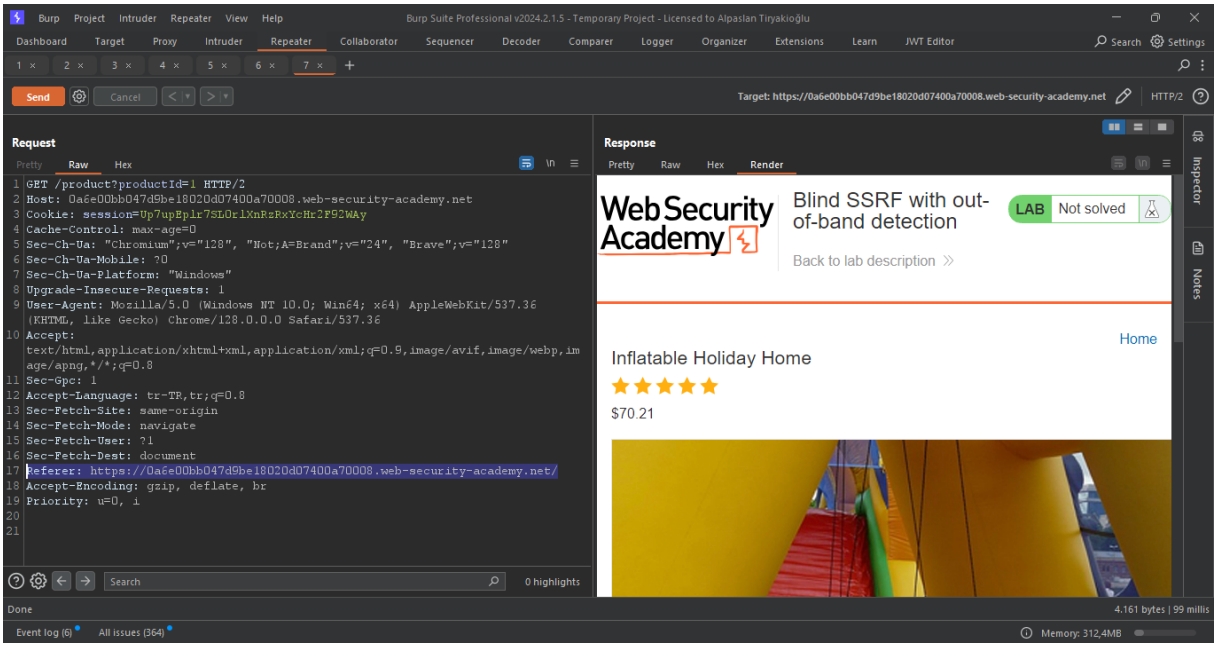
Bu site, bir ürün sayfası yüklendiğinde *Referer* başlığında belirtilen URL'yi getiren analiz yazılımını kullanır. Bunu çözmek için genel Burp Collaborator sunucusuna http isteği göndermesi gerekli.

Bunun için hem ücretsiz hem de ücretli Burp Suite sürümlerinde kullanabiliriz.

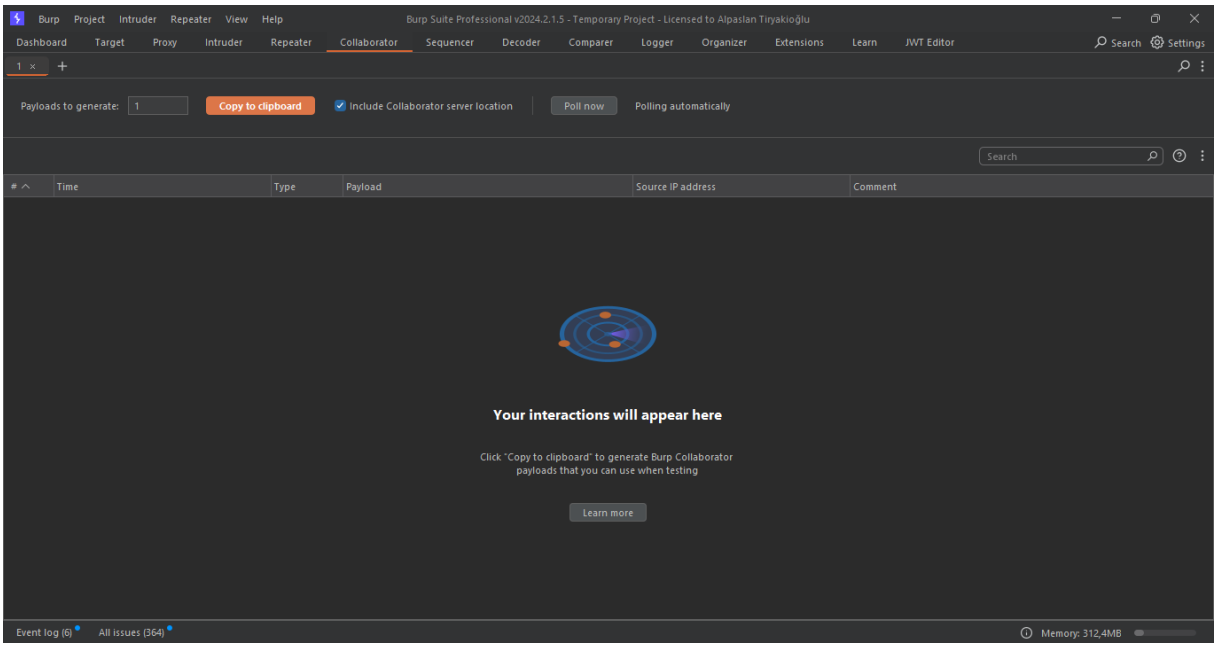
İlk açıklamalarda ürün sayfası yüklendiğinde gerçekleşen bir olaydan bahsediyor bu yüzden bir ürüne giderken direkt olarak http paketlerine bakacağız.



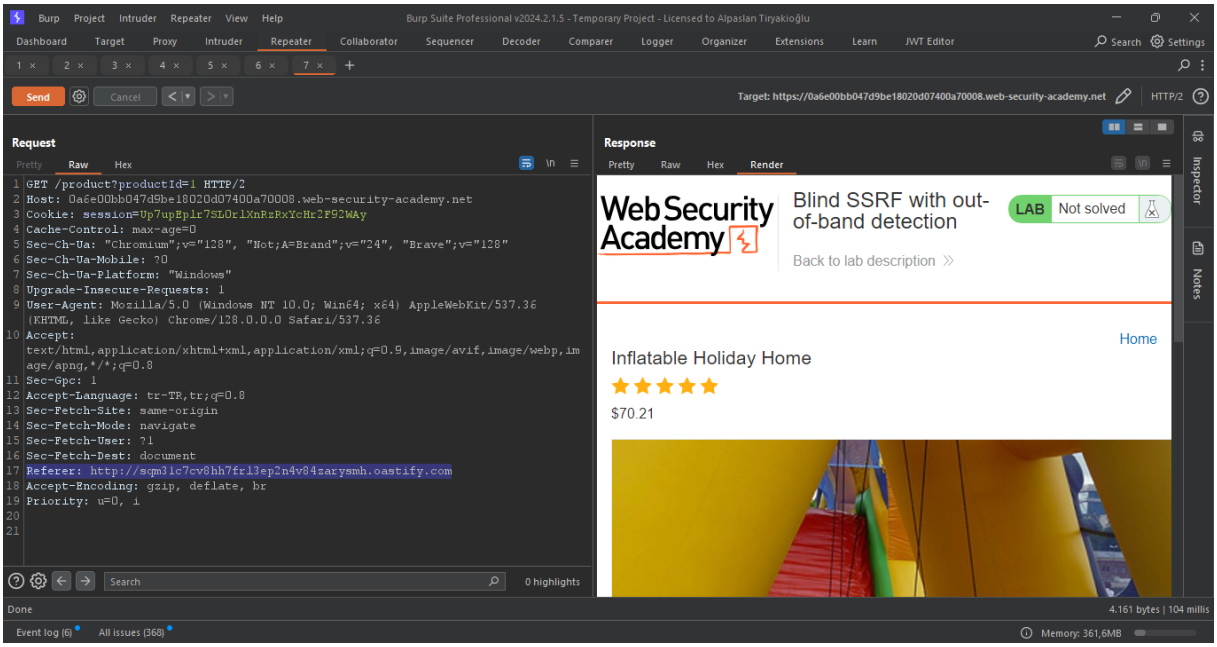
İki paket ile sayfa yükleniyor. Bizi ilgilendiren bu olduğu için bununla çalışıyorum. Repeater aracına atıp hemen başlıyorum.



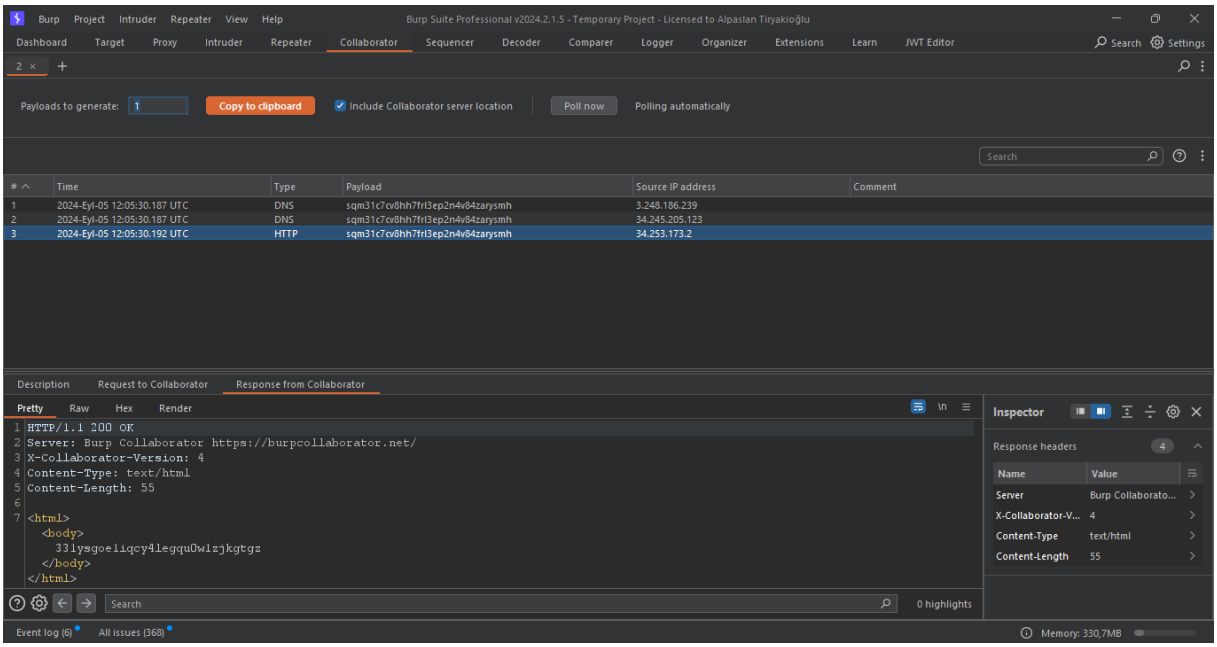
Buradaki Referer başlığı ile denemelerimiz yapmamız gerekiyor. ilk olarak Colloborator sunucusunu başlatıyorum.



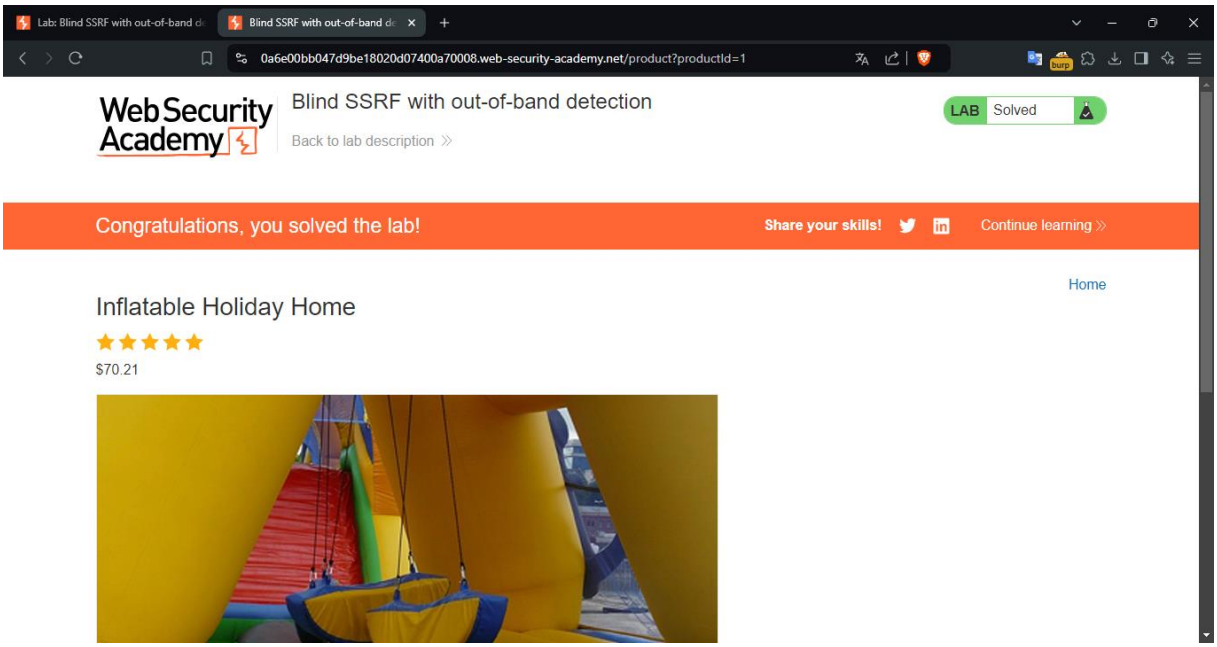
Collaborator sekmesine geldikten sonra "*Copy to clipboard*" butonuna bastığımızda adresi çalıştırmaya başlıyor ve otomatik olarak gelen istekleri yakalamaya başlıyor.



Burada göründüğü gibi esik değeri silip buraya yenisini yerleştirdim ve paketi gönderdim.



Collaborator içinde “Poll now” dedikten sonra gelen istekleri buradan görebiliriz. ben HTTP isteğinin cevabını görüntüledim. Bu sırada laboratuvar ekranına gelirsek zaten çözümlendiğini görebiliriz.



Bu laboratuvarı da çözümlemiş bulunmaktayız.