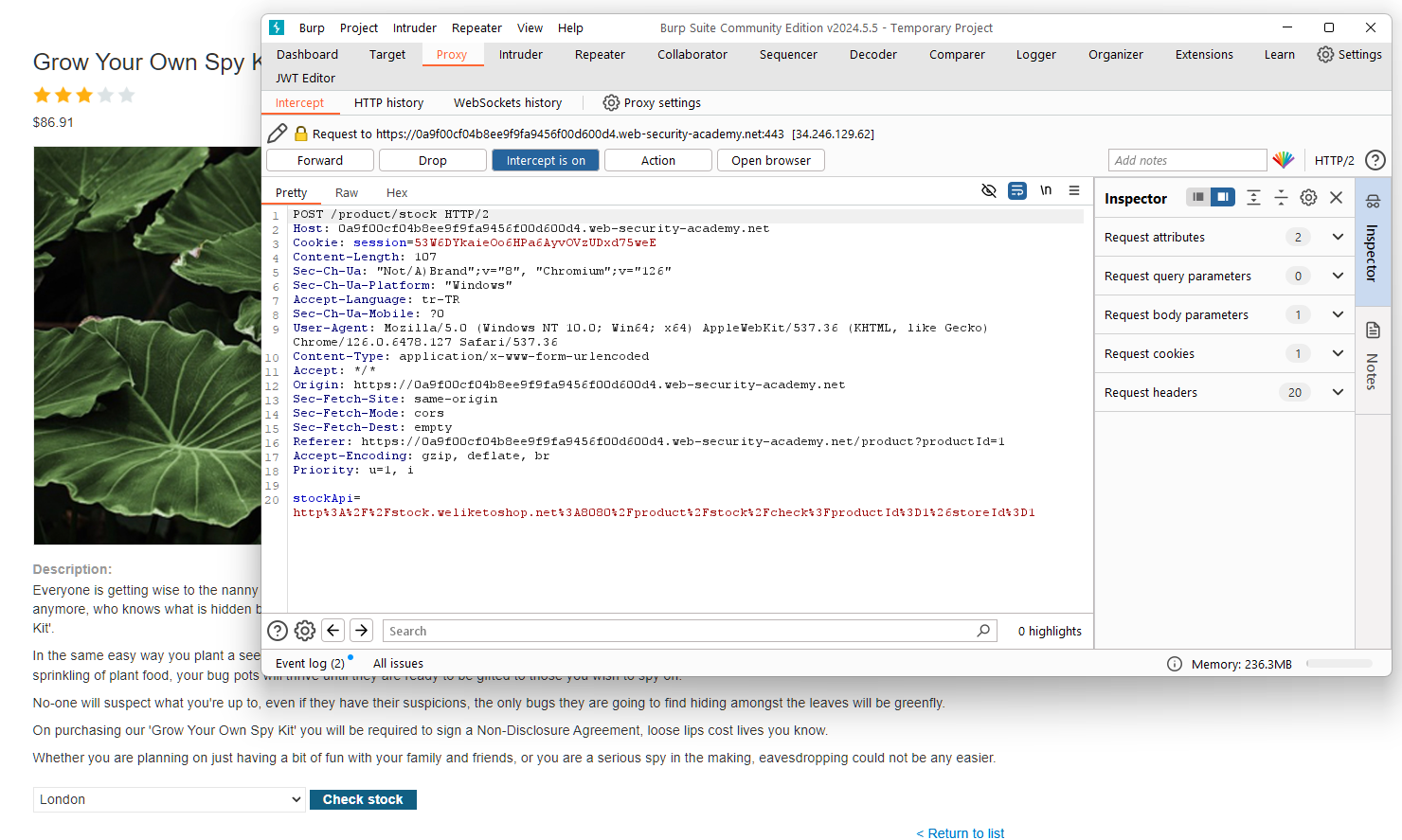
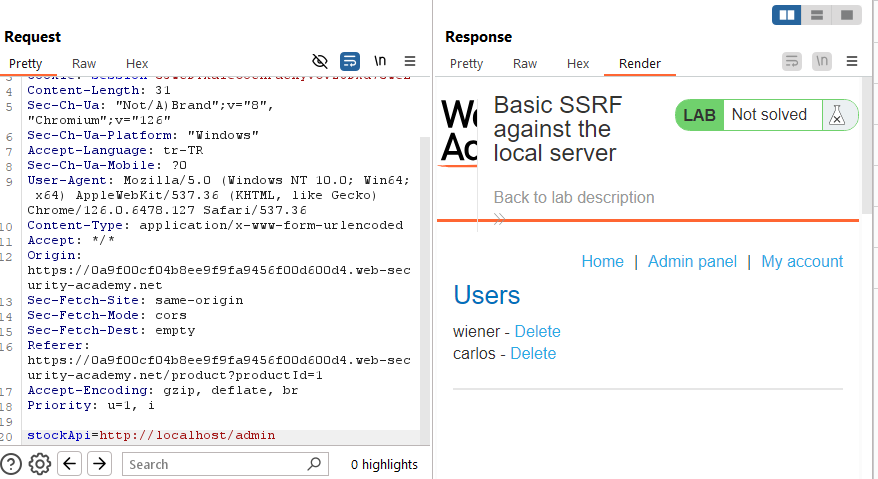
SSRF

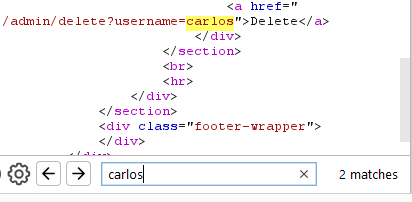
1-Lab: Basic SSRF against the local server(PortSwigger)

İlk olarak Api gönderilen bir sayfa aradım ve stock kontrol de buldum

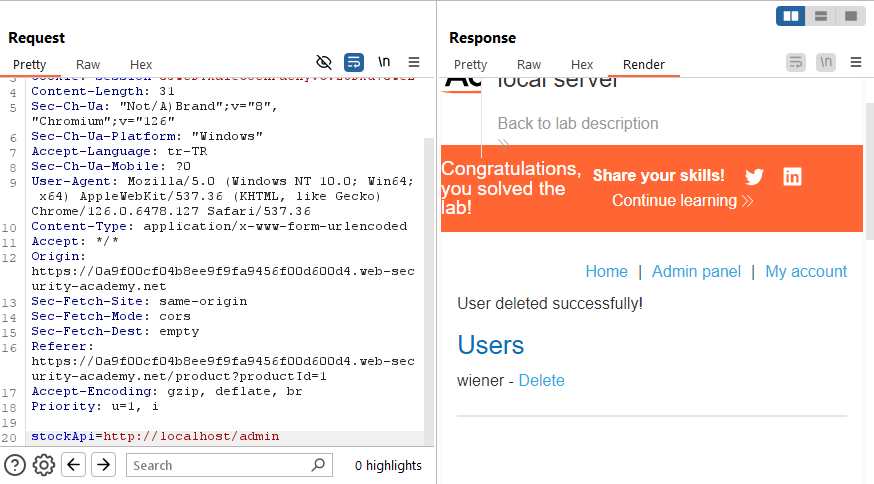


Sonrasında bu isteği repeatere gönderdim ve apiyi değiştirerek admin sayfasına girdim

Gelen sayfanın RAW kodunu inceleyerek kullanıcı silme adresini buldum ve repeater ile gönderdim

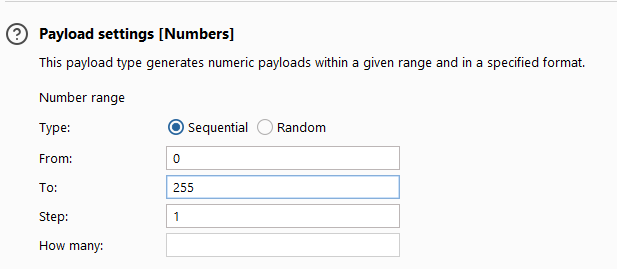


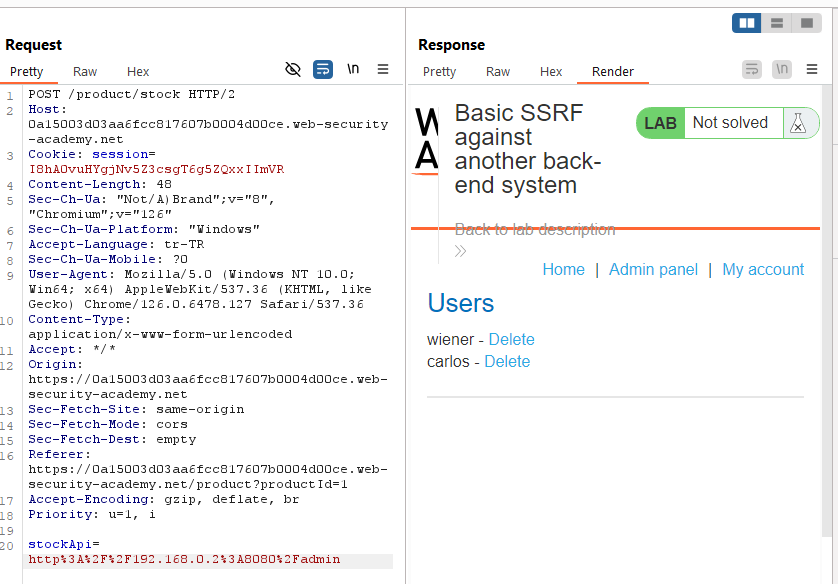
Sonrasında admin sayfasına döndüğümüzde silindiğini görüyoruz



**2-Lab: Basic SSRF against another back-end system(PortSwigger)**

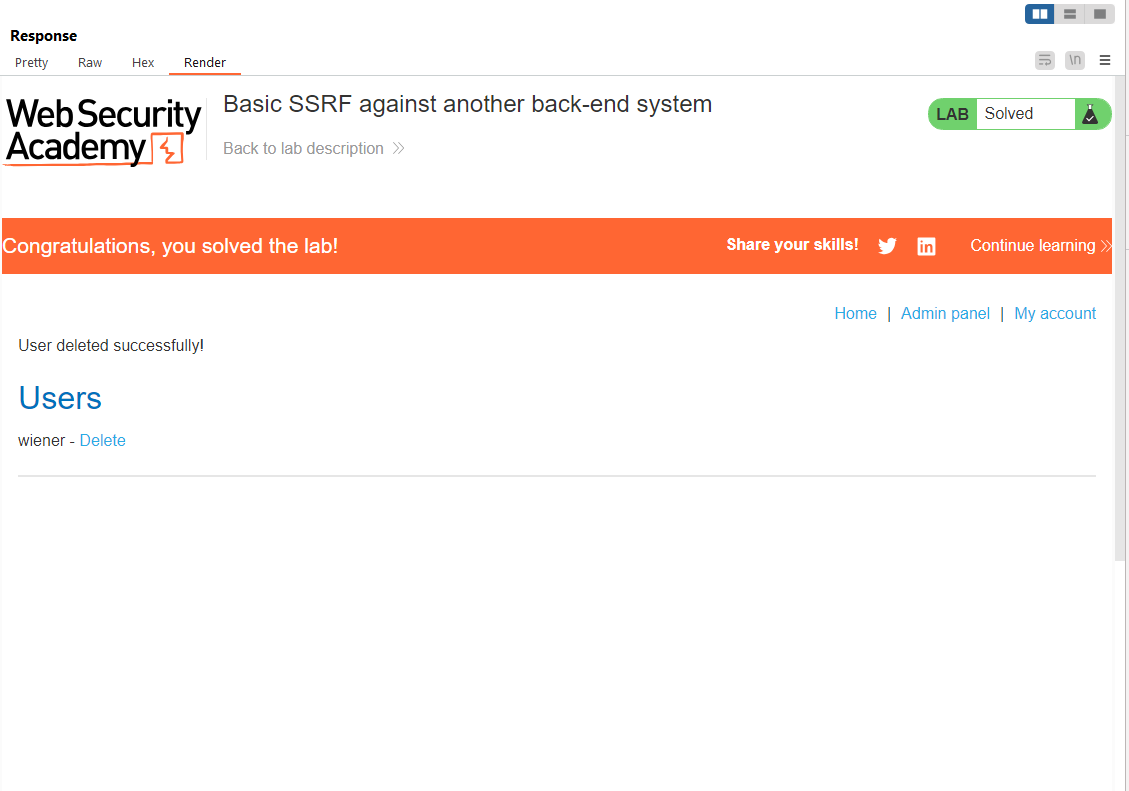
Api gönderilen sayfayı buldum önce sonra açıklamada verildiği üzere admin sayfasını bulmak için ıntrudere gönderdim



Brute force attıktan sonra farklı uzunluktaki sayfayı bulup inceledim

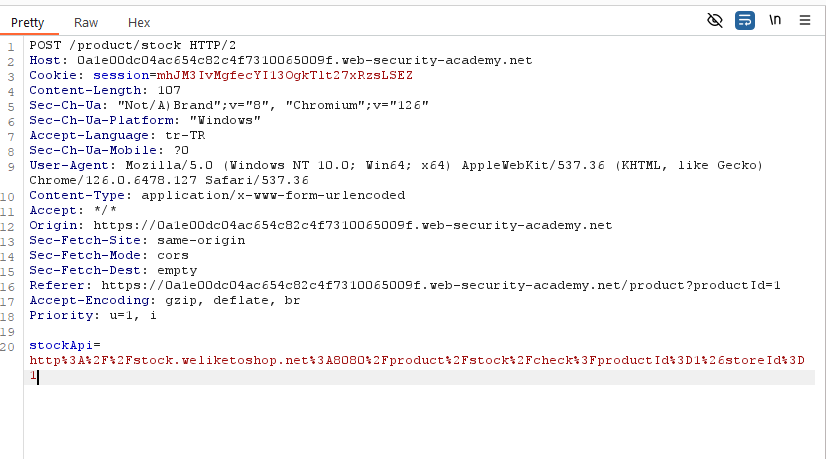
Raw kodunu inceleyerek Carlos silme apisini buldum ve sildim



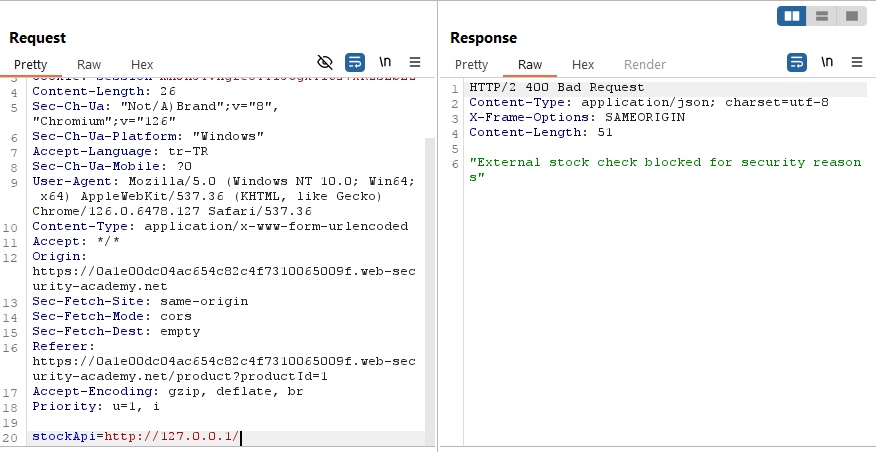


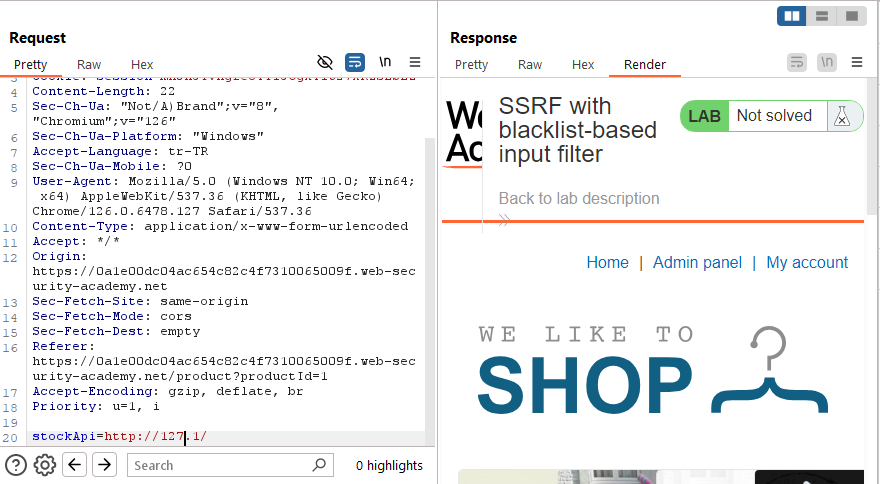
**3-SSRF with blacklist-based input filter**

İlk olarak api yakalıyoruz.

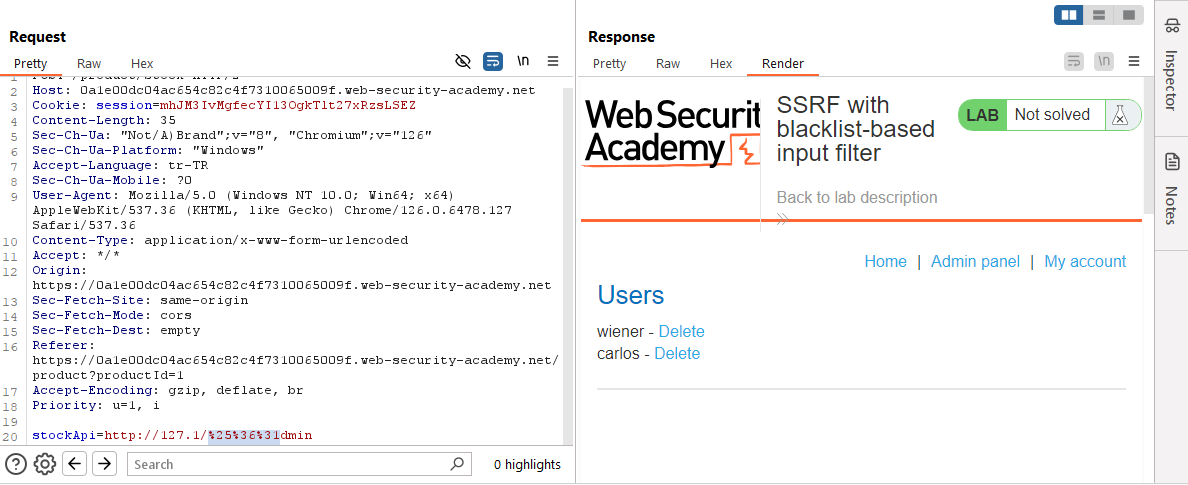


127.0.0.1 adresi black liste alındığı için 127.1 olarak deniyoruz

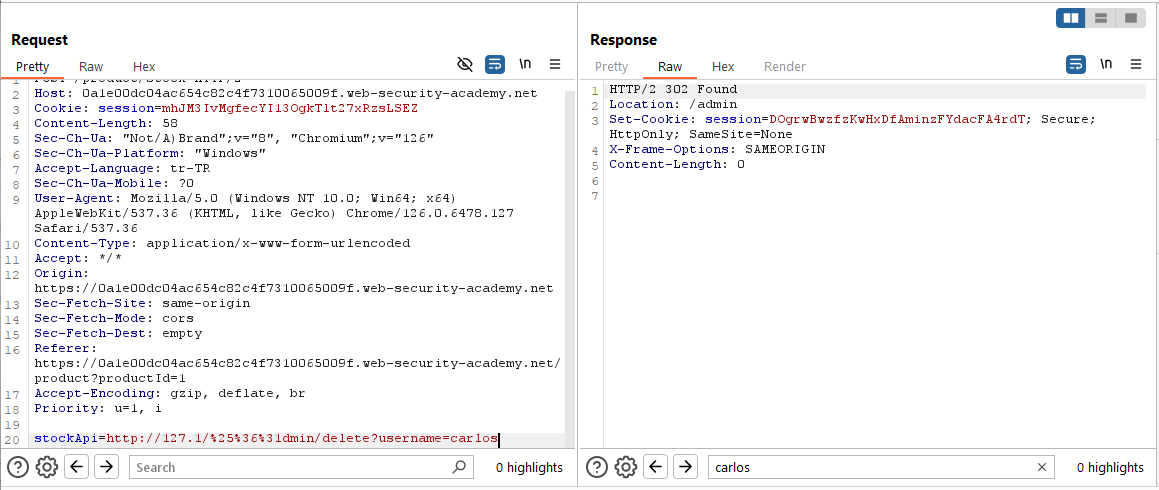


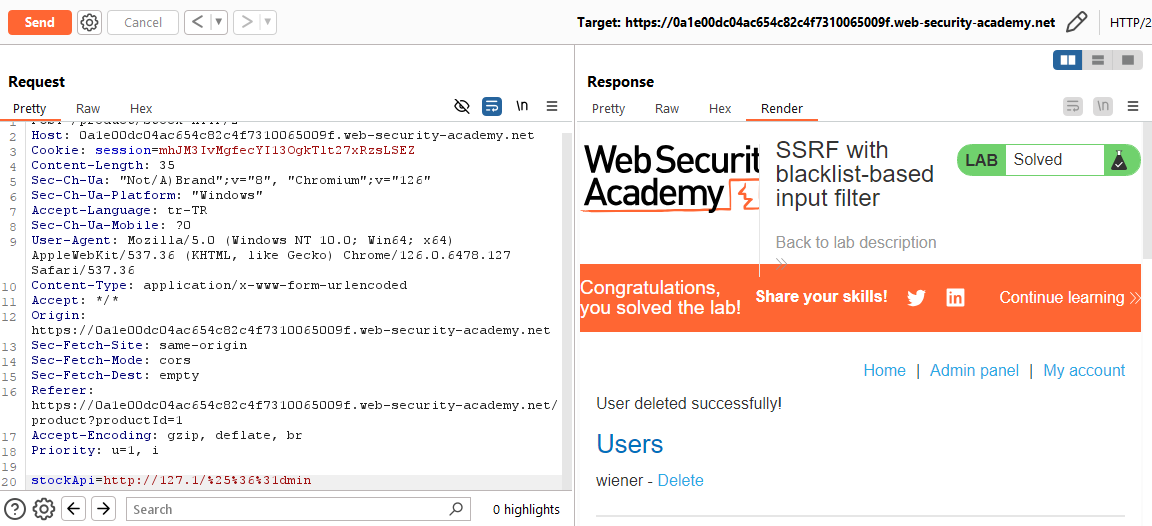


Bu şekilde denediğimiz de giriş yapabiliyoruz. Cevap olarak dönen sayfanın raw kodundan admin sayfasının adresini bulup girmeyi deniyoruz, /admin olarak denediğimizde kara listeye alındığı için istediğimiz cevabı alamıyoruz a yı encode edip deneyerek sayfaya giriş yapıyoruz



Admin sayfasının raw kodunu inceleyerek carlosu siliyoruz

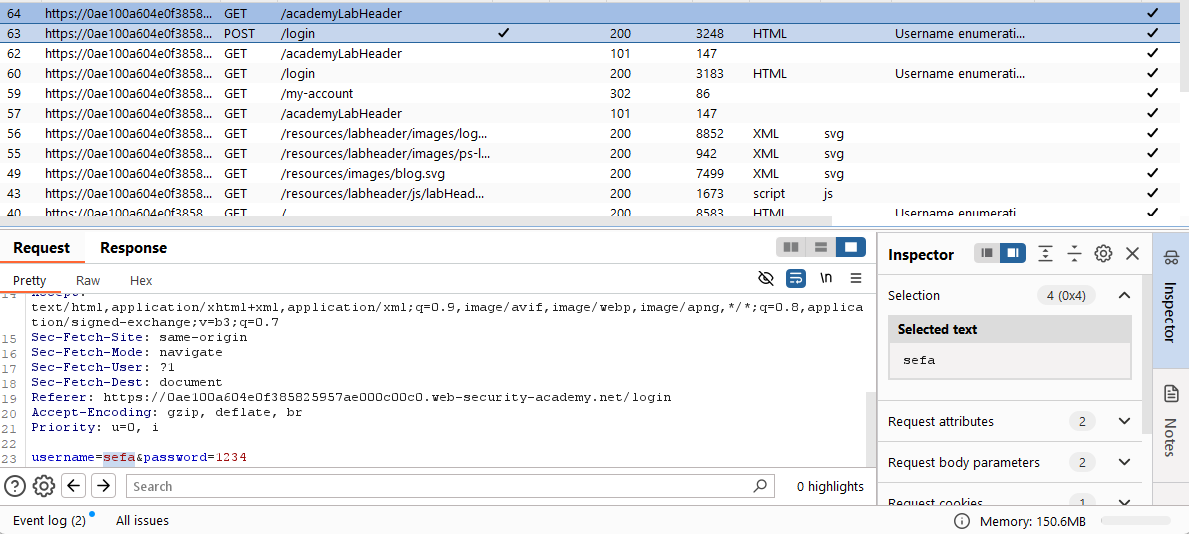


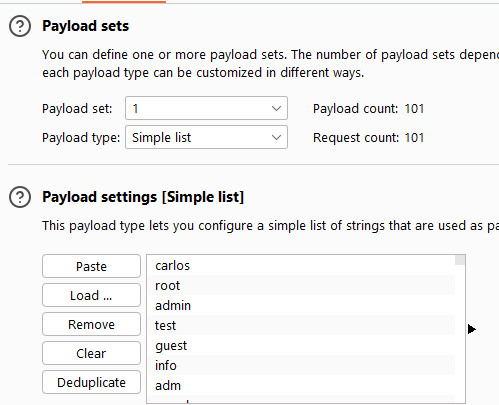


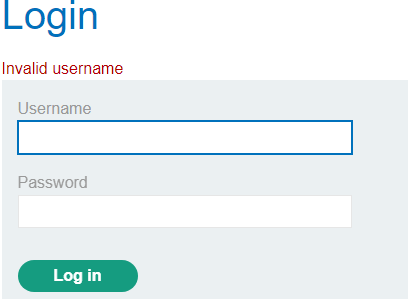
**Authentication**

**1-Username enumeration via different responses**

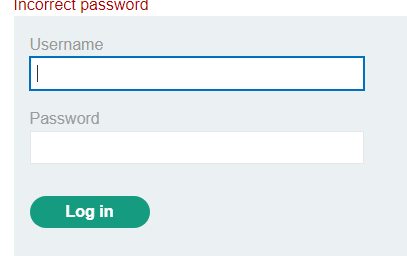
İlk olarak giriş yapma denemesi yaparak post isteğini yakalayıp ıntrudere gönderiyoruz ve payloadımızı kullanıcı adı kısmından gönderiyoruz çünkü kullanıcı adı yanlış olunca site bunu bize söylüyor







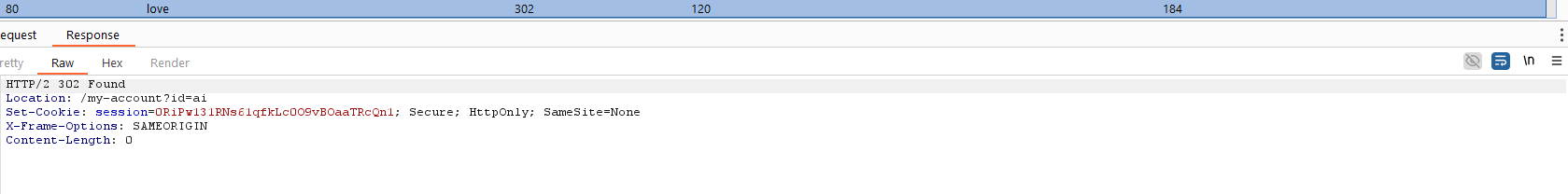
Doğru kullanıcı adı girdiğimizde de şifrenin yanlış olduğunu belirtiyor



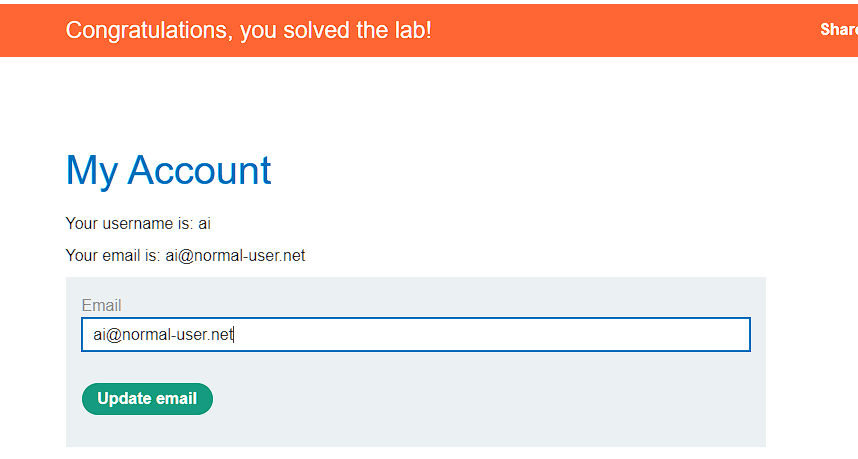
Kullanıcı adımızı ai olarak bulduktan sonra şifre kısmı için atack başlatıyoruz



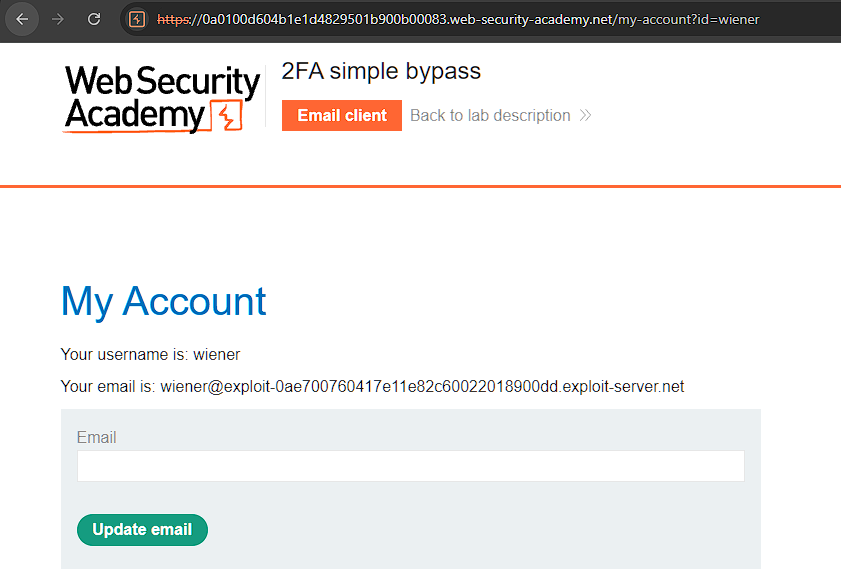
Şifremizi de love olarak buluyoruz

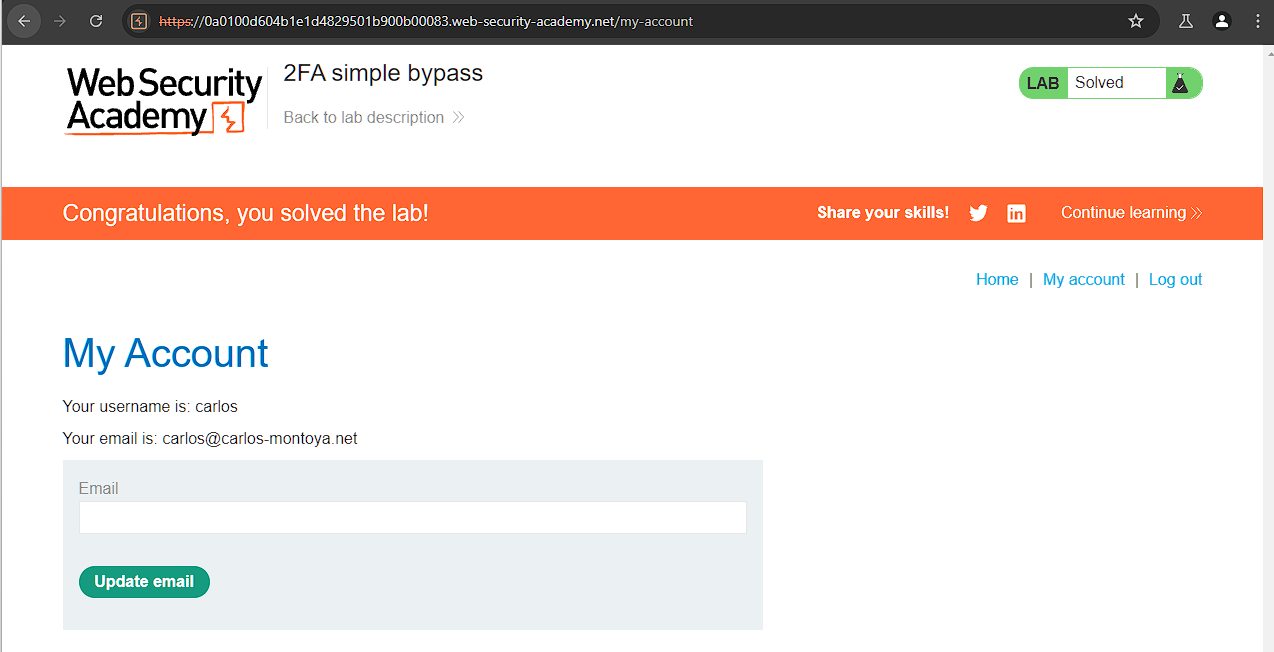


Bu bilgiler ile giriş yapabiliyoruz

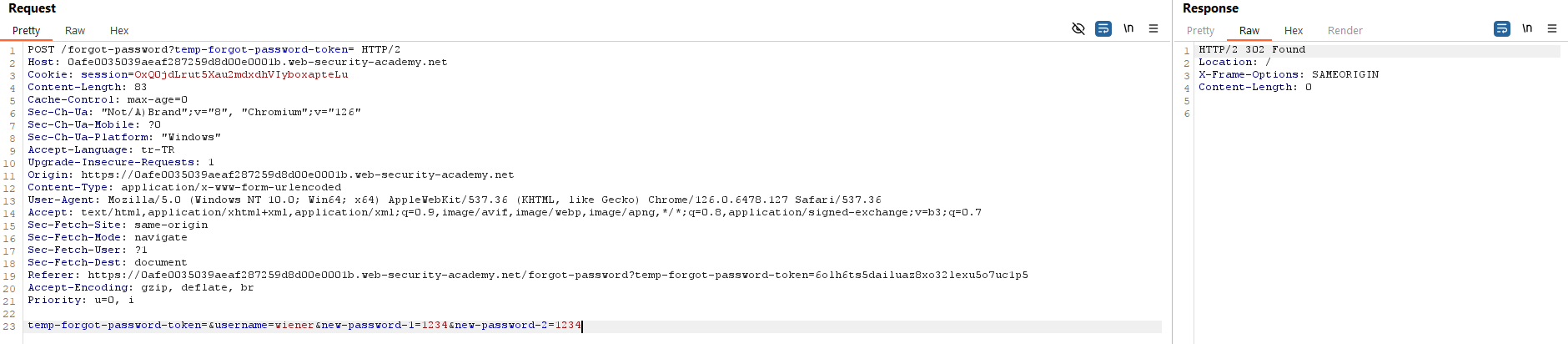


**2- 2FA basit baypas**

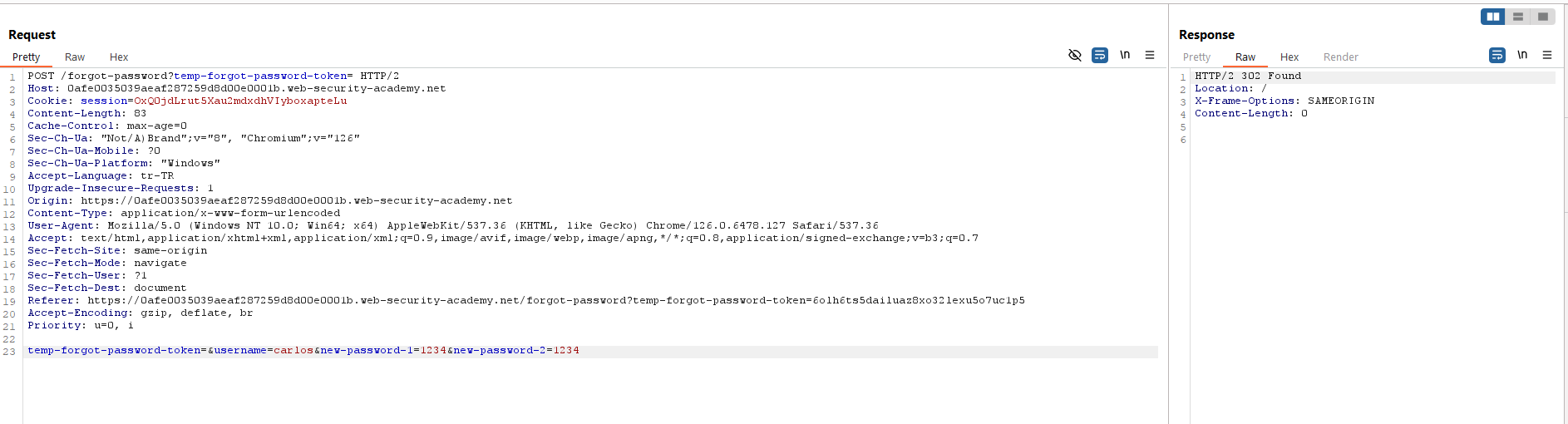
Bizim kimlik bilgilerimizin wiener;peter olduğu verilmiş ve Carlos un hesabına girmemiz isteniyor.Kendi hesabımıza girerken giriş için mail adresimize kod gönderiliyor.Bu sırada url kopyalıyoruz.

Hesabımızdan çıkış yapıp carlosun hesap bilgilerini giriyoruz.Sonrasında mail kısmında kod istediğinde kendi profilimizde kopyaladığımız url den ?id=wiener kısmını silerek yapıştırdığımızda giriş yapmış oluyoruz

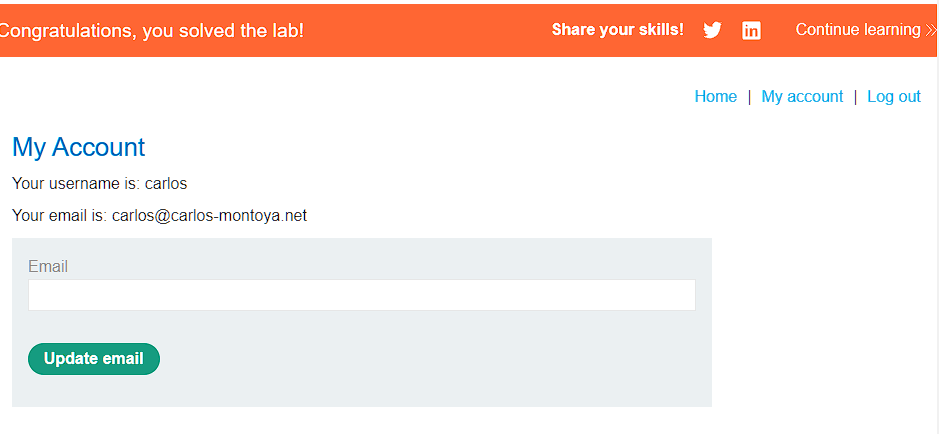
**3- Password reset broken logic**

İlk olarak parolamı unuttum kısmına tıklıyoruz ve kendi parolamızı maile gelen link ile değiştiriyoruz. Sonrasında http geçmişini incelediğimizde şifre değiştirme isteğinin token ile gönderildiğini görüyoruz ve tokenı sildiğimizde de şifreyi değiştirebiliyoruz

Buradan ismi Carlos yapıp carlosun şifresini değiştiriyoruz.



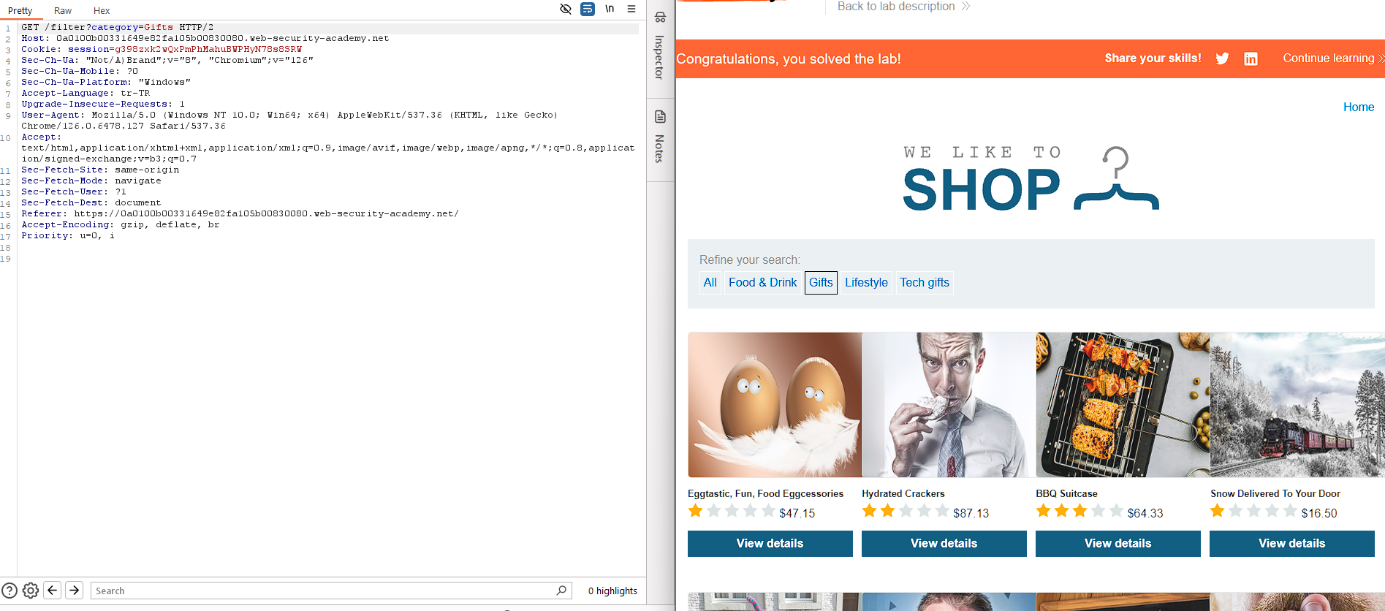
Ve giriş yapıyoruz



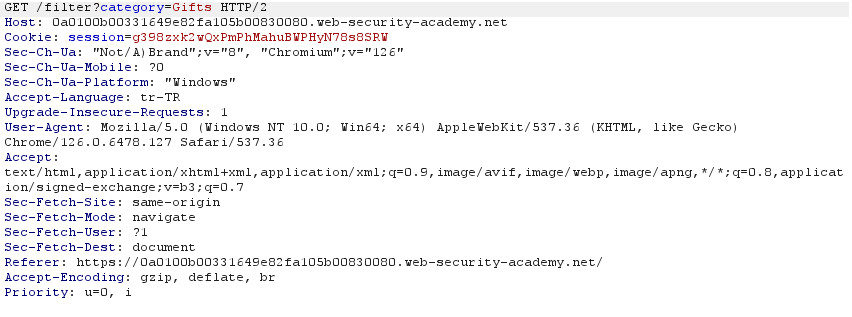
**Injection**

**1-SQL injection vulnerability in WHERE clause allowing retrieval of hidden data**

İlk olarak burp suit ile isteği yakalıyoruz

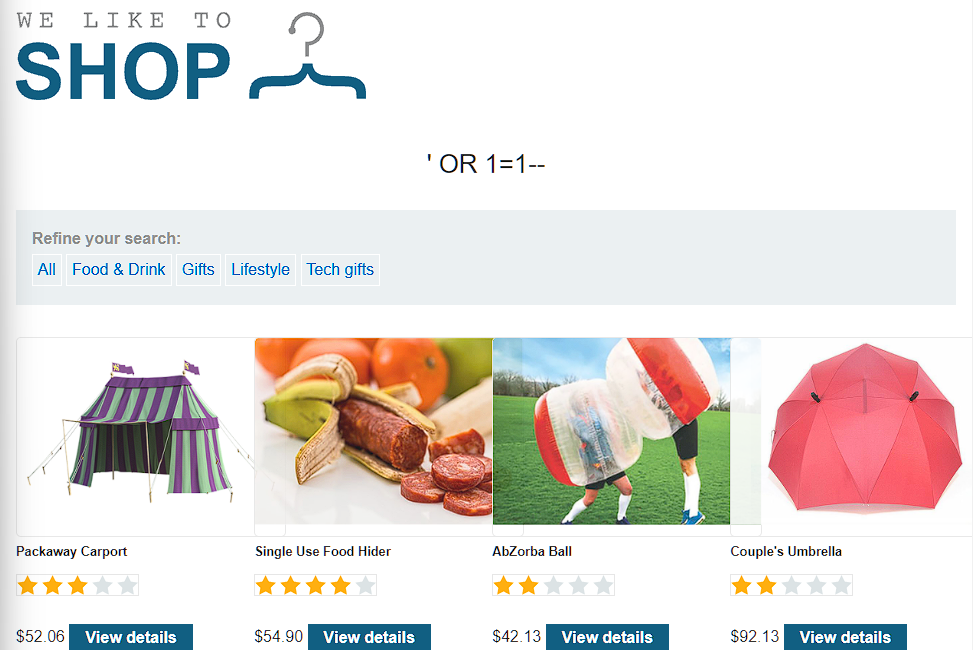


Yakaladığımız istekte kategori bilgisinin gönderildiğini görüp bu kısmı manipüle ediyoruz



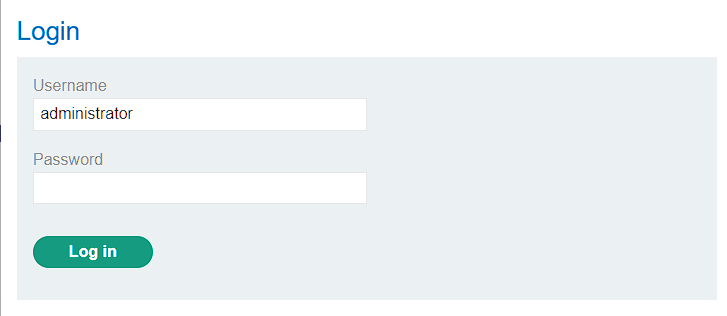


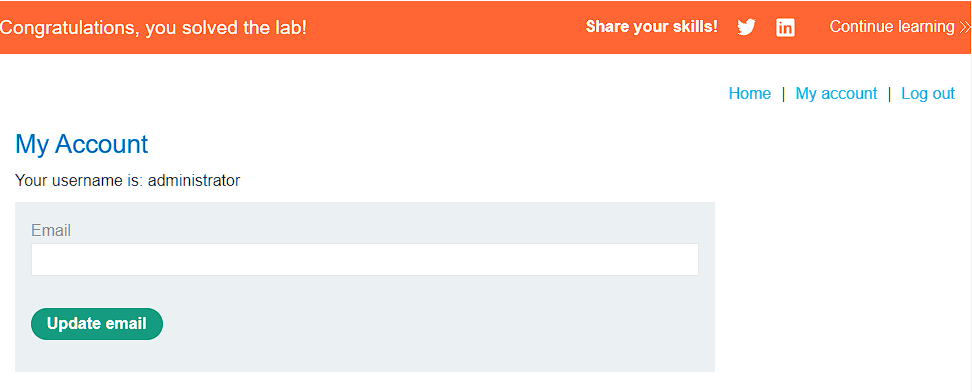
Bu isteği bu şekilde gönderdiğimiz de tüm ürünleri görebiliyoruz



**2-SQL injection vulnerability allowing login bypass**

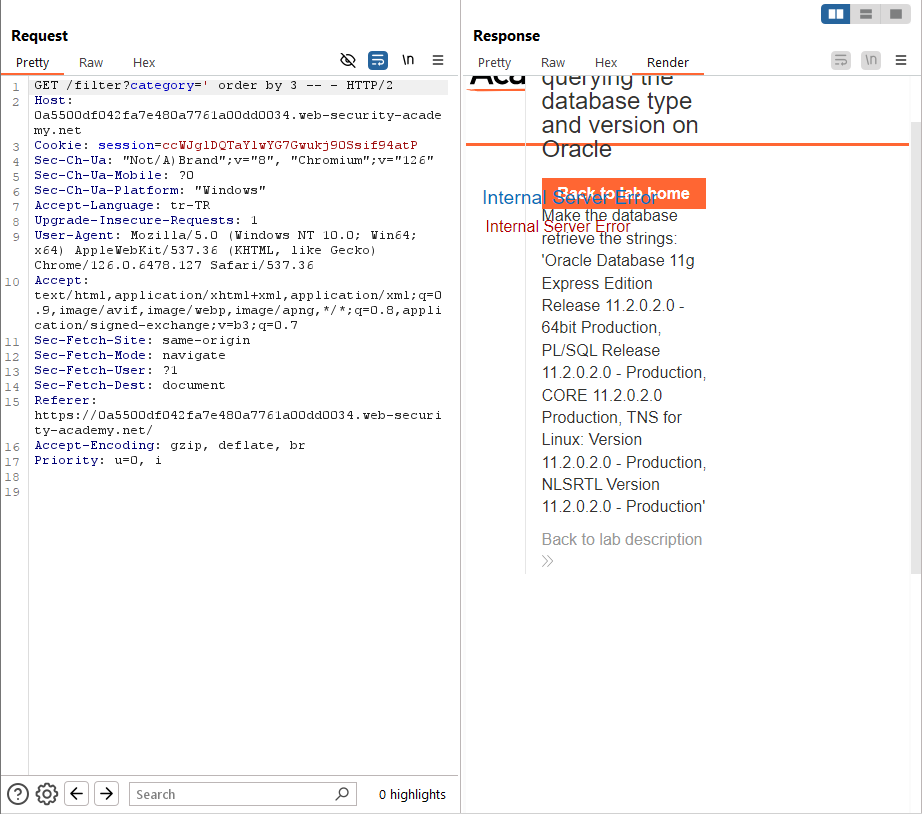
Administrator adlı kullanıcının hesabına girmemiz isteniyor bu sebeple kullanıcı adı kısmına administrator yazıp şifre kısmına ise ‘ OR ‘1’=’1 payloadını yazdığımızda giriş yapmış oluyoruz

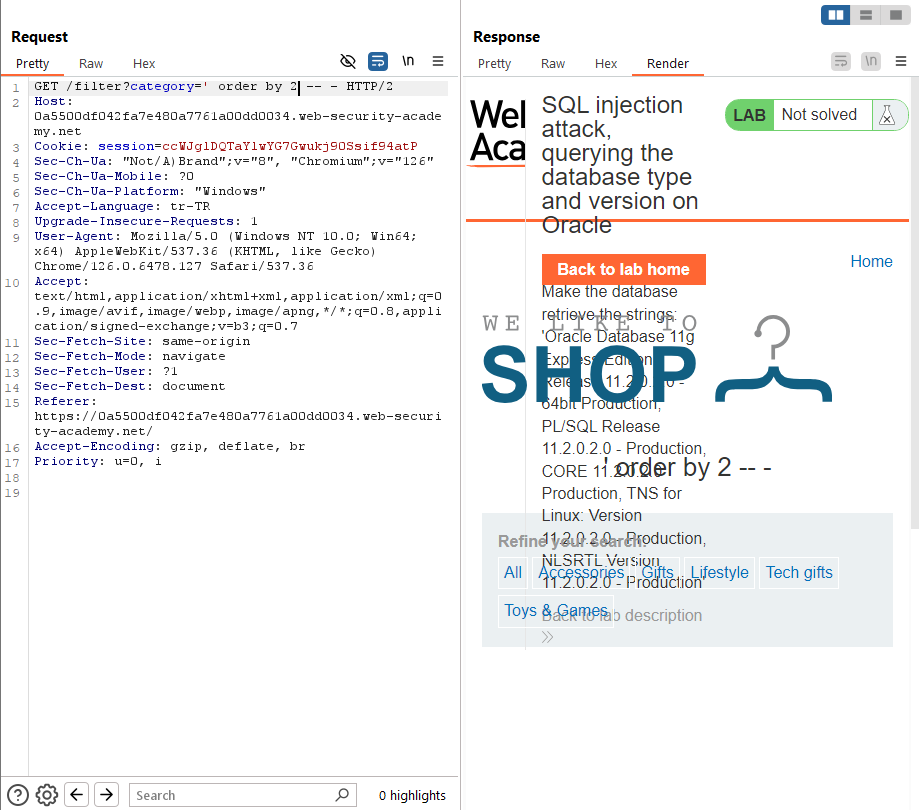


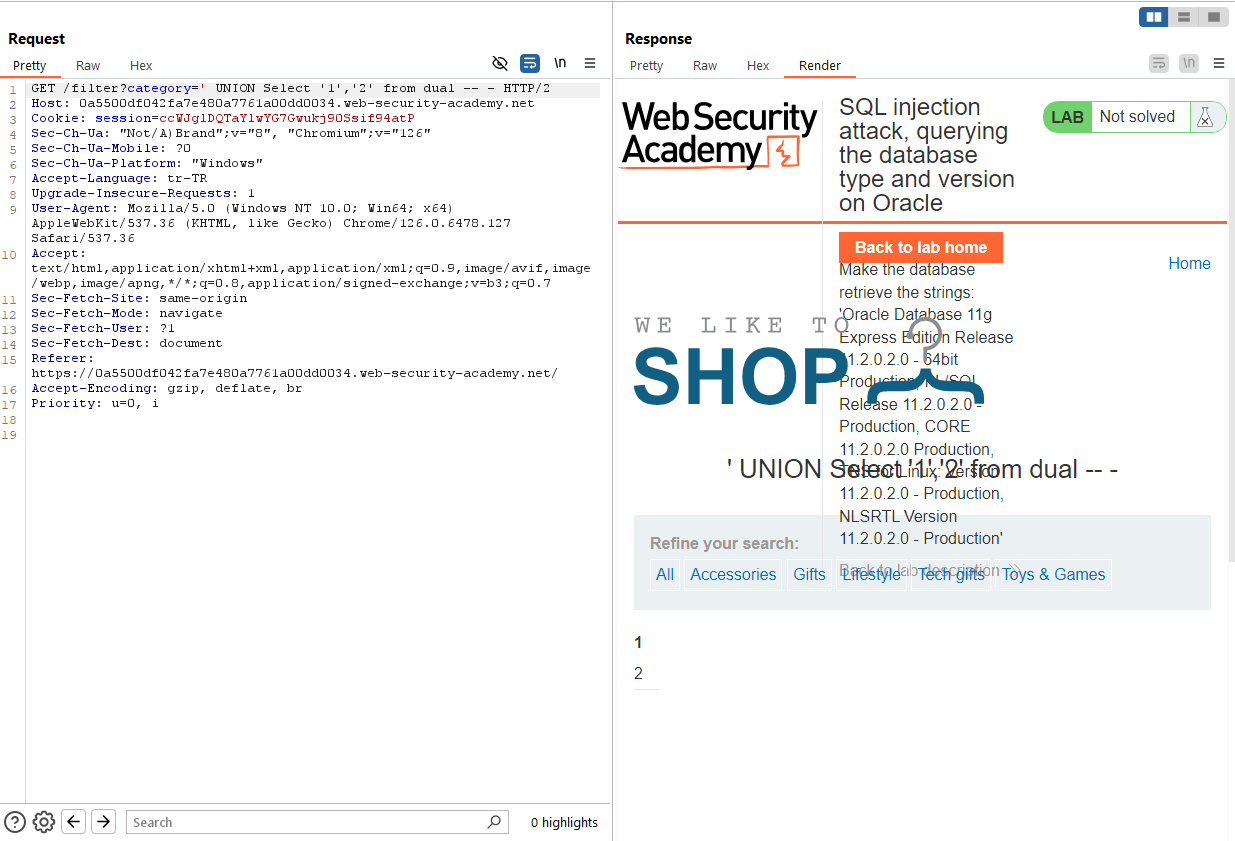
****

**3-**

İlk olarak burp suit ile isteği yakalıyoruz ve sutun sayısı öğrenmek için order by kullanıyoruz



Göründüğü üzere 2 adet sütun varmış



Verilerin geldiği yerleri de öğrendikten sonra veritabanı versiyonu öğrenebiliriz

