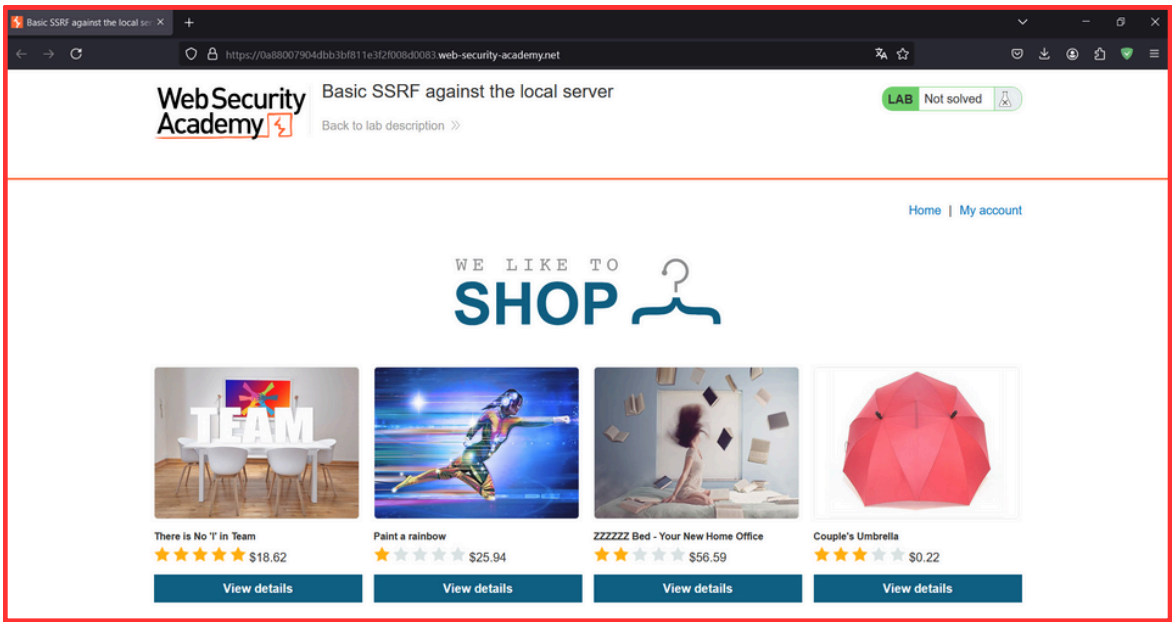
SSRF

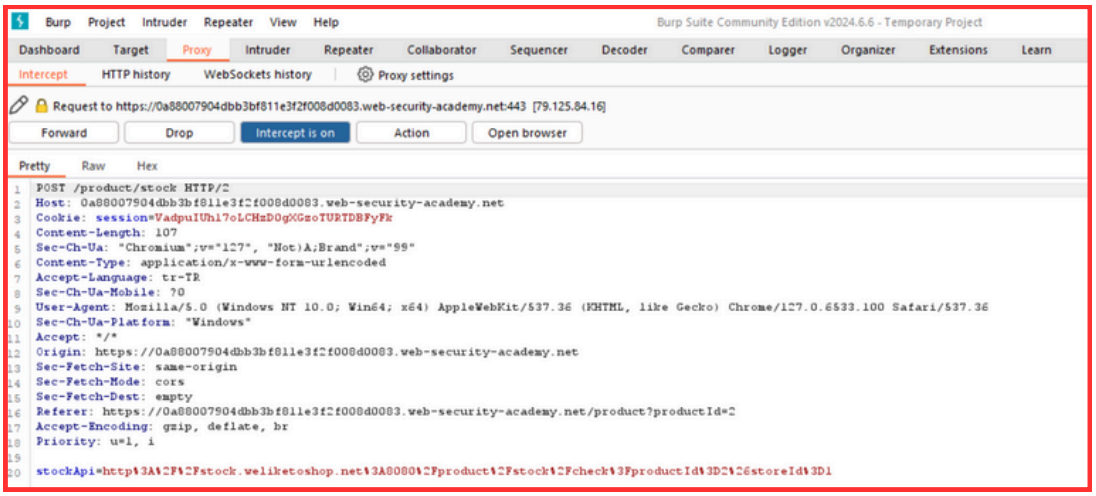
LAB 1

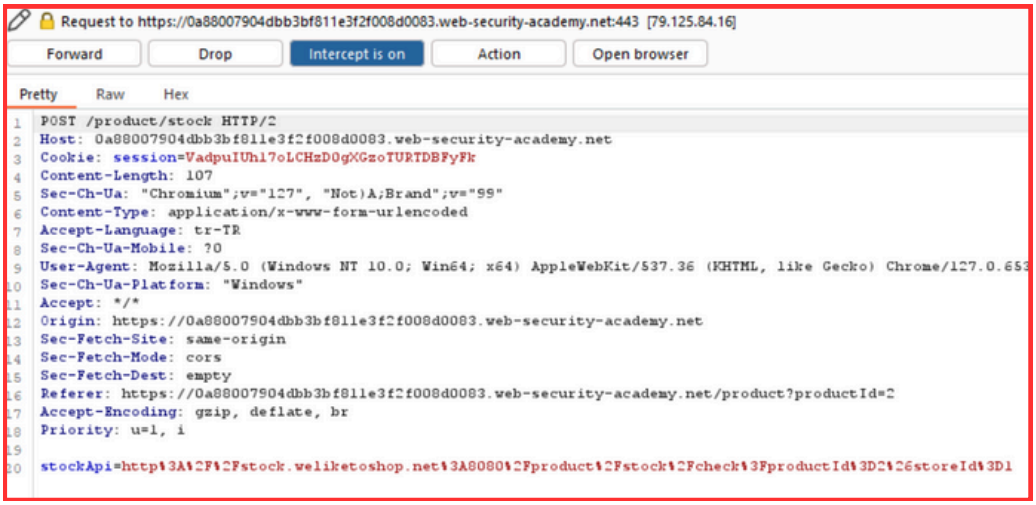
TARİH: 30.08.2024



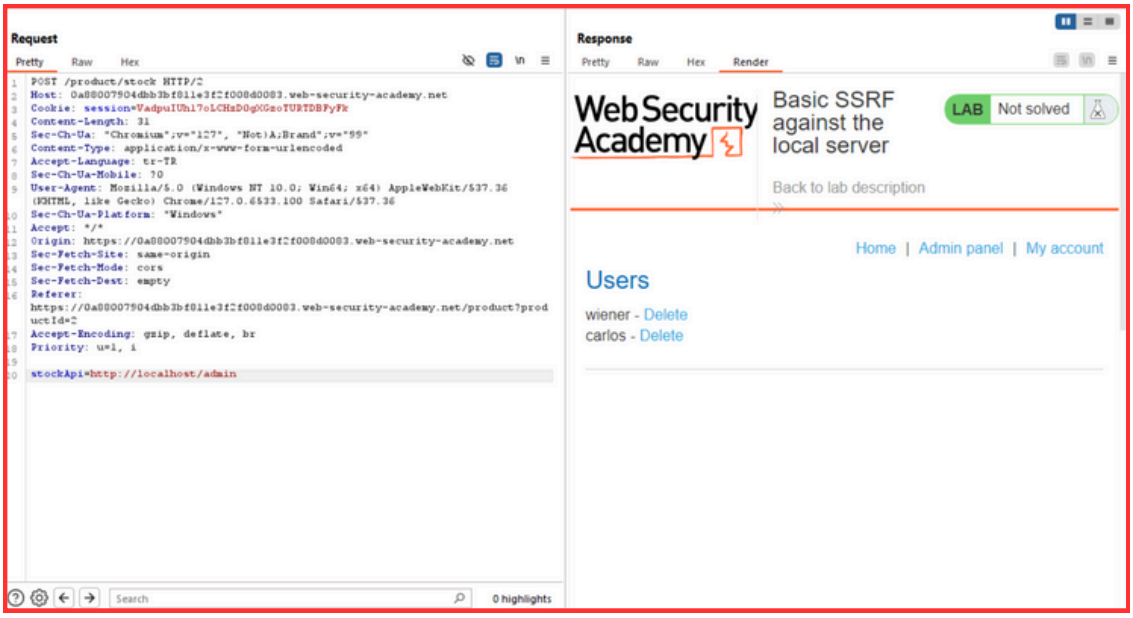
Bu lab içerisinde bizden, stok kontrol URL'ini değiştirip admin arayüzüne erişerek carlos adlı kullanıcıyı silmemiz isteniyor.

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. Bu paketi farklı şekillerde tekrar yollamak için BurpSuite içinde Repeater kısmına gönderiyorum.



Bu zafiyeti kullanarak http://localhost/admin adresine ulaşmamız belirtilmişti. Ben de stockApi parametresinde bu URL'i kullandım ve böylece admin sayfasına ulaştık burada carlos kullanıcısını silerek labı tamamlıyorum.