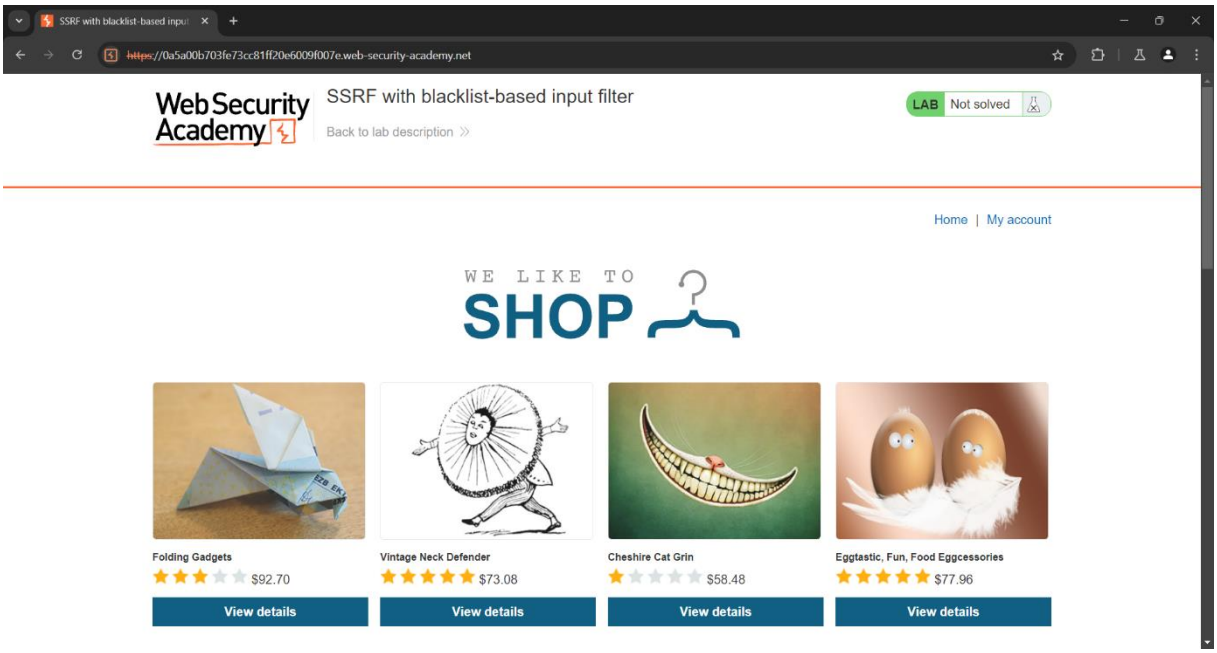
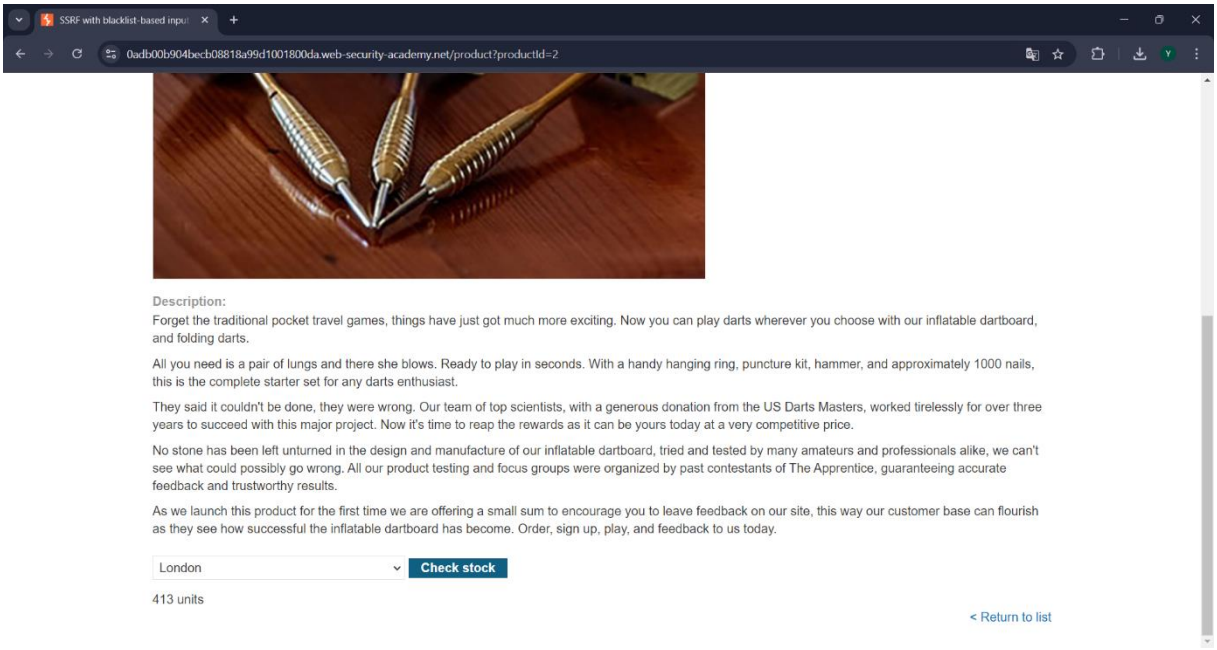
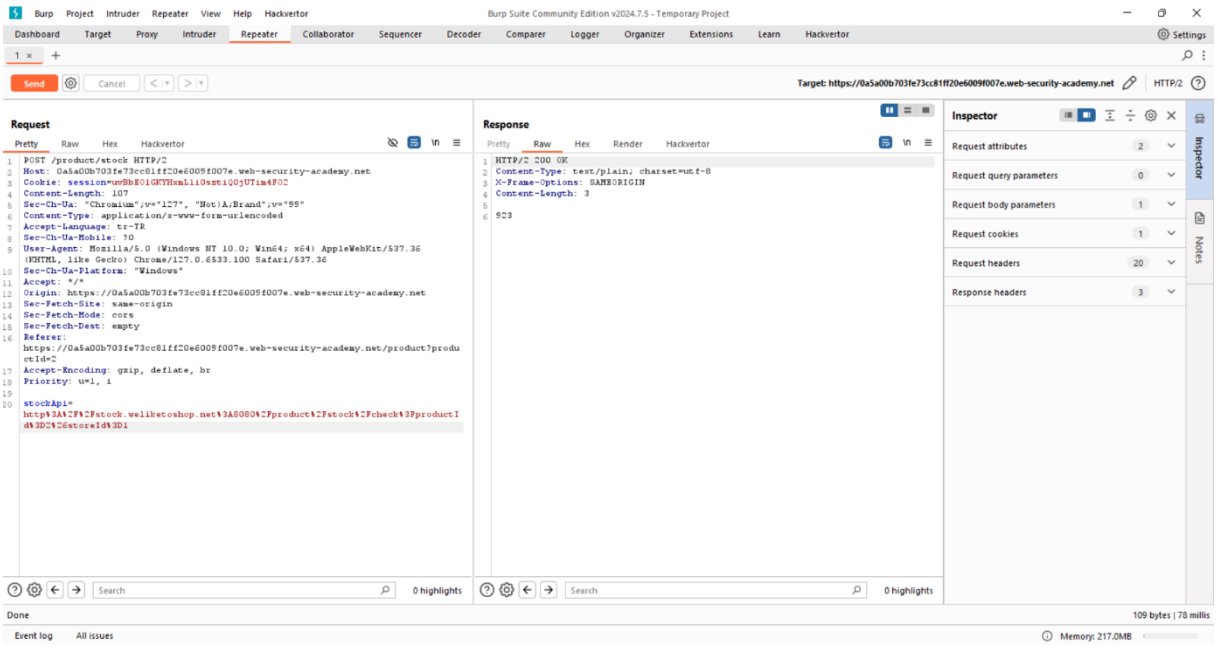
Portswigger Lab: SSRF Write-Up



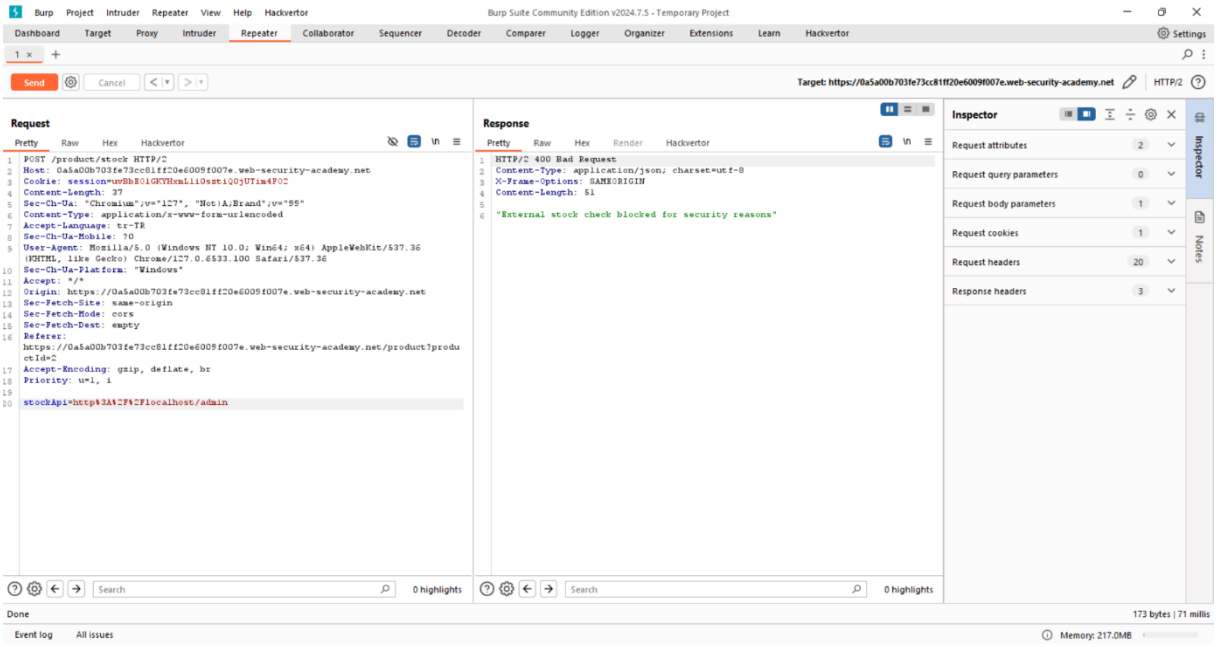
Bu sitemizin anasayfası, burada ssrf ile Carlos adındaki kullanıcıyı silmemiz isteniliyor. Bunun için ilk adım sunucu ile etkileşim kurulabilecek bir yer olmalı. Bunun için ürünlerin detaylarına bakalım.



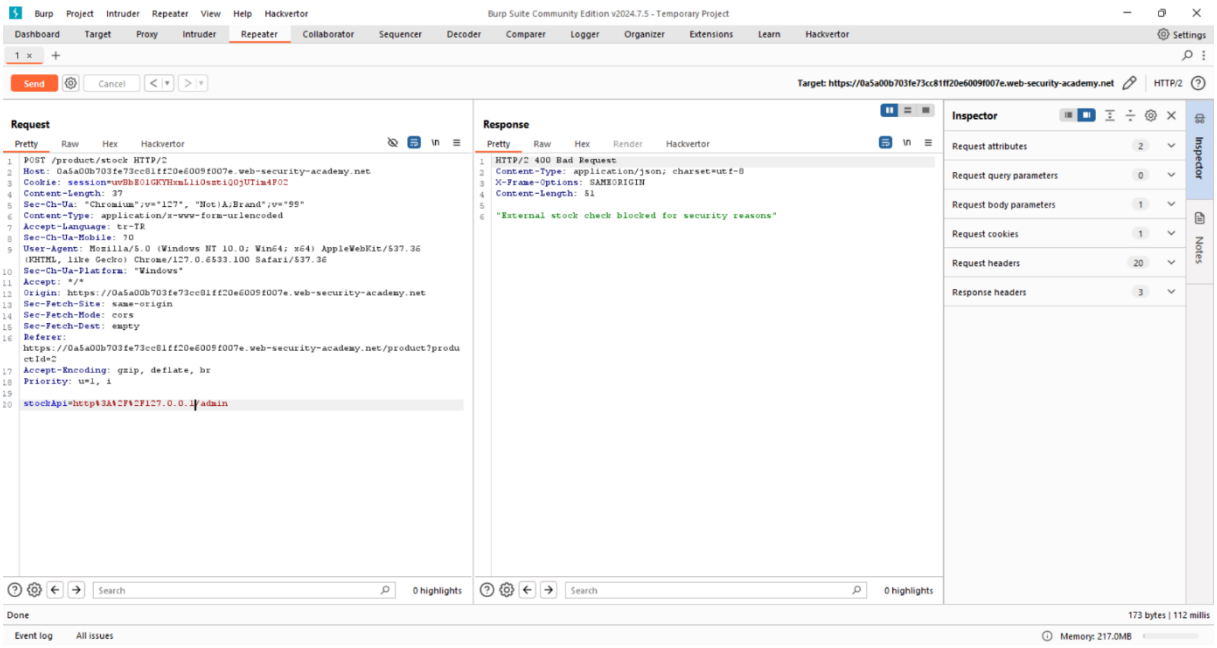
Rastgele bir ürün seçtim ve bu ürünün altında stok kontrol butonu vardı. Bunu burp suite ile takibe alalım.



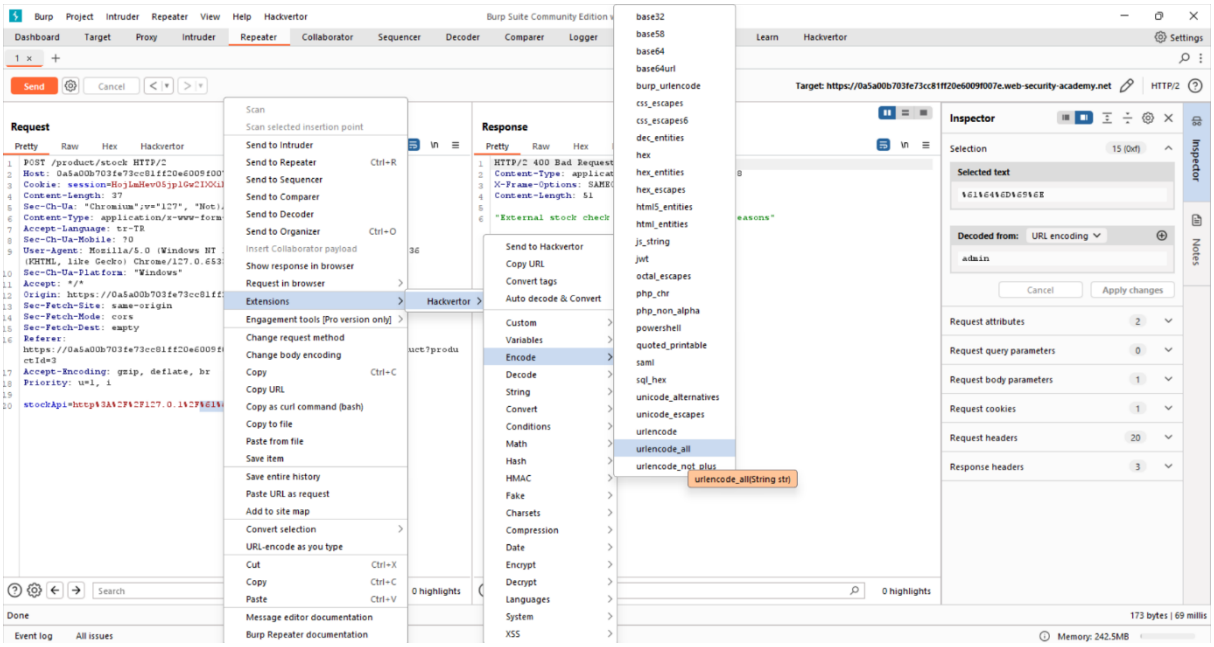
Karşımıza stockapi diye bir parametre çıktı bununla oynamaya başlayalım.



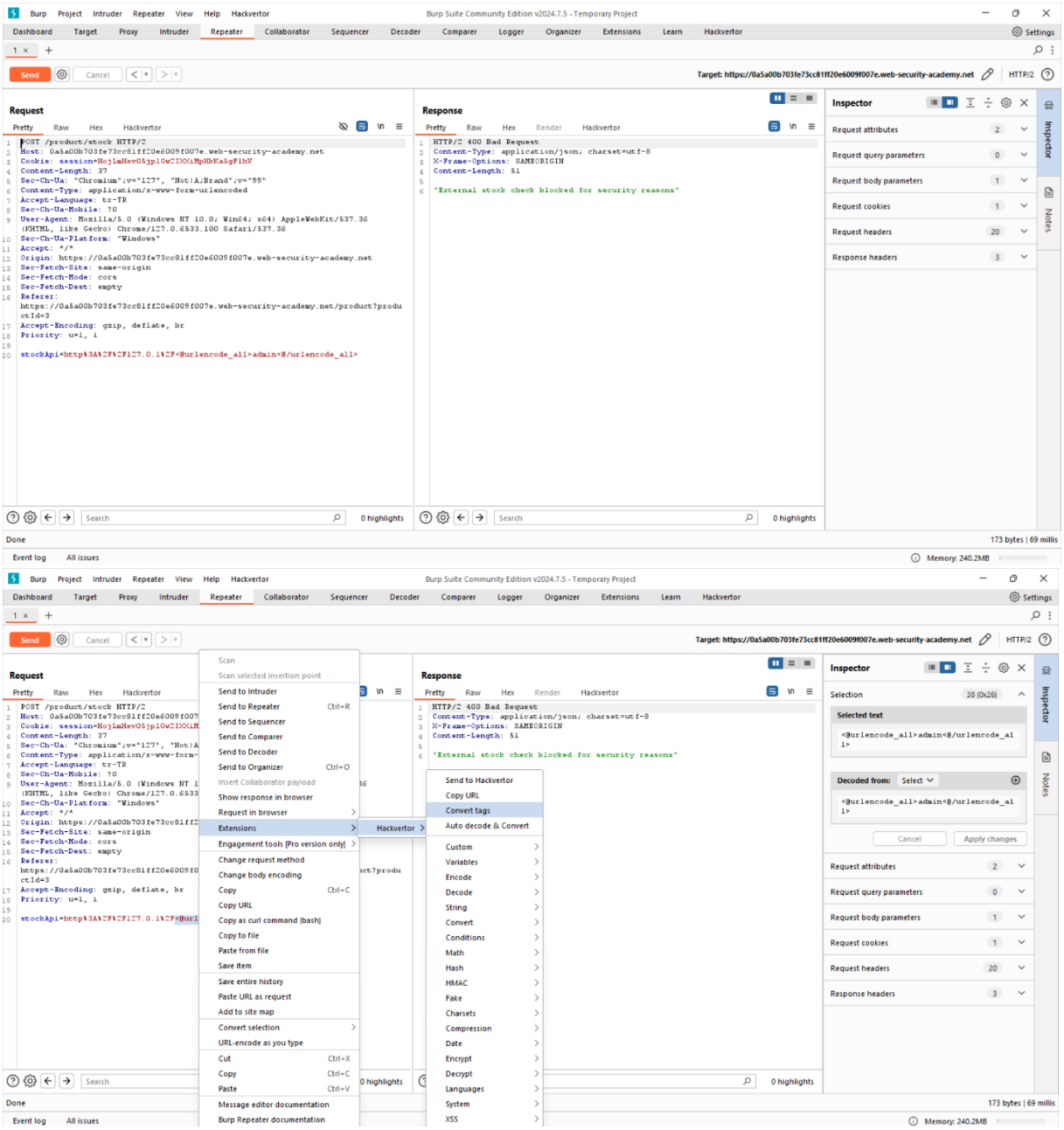
İlk önce portswiggerin verdiği şekilde http://localhost/admin ile girmeyi denedim ve bana bir mesaj döndü. Bu mesajdan sonra burayı bypass etmem gerektiğini anladım. Bunun için öncelikle localhost kısmını değiştirdim.



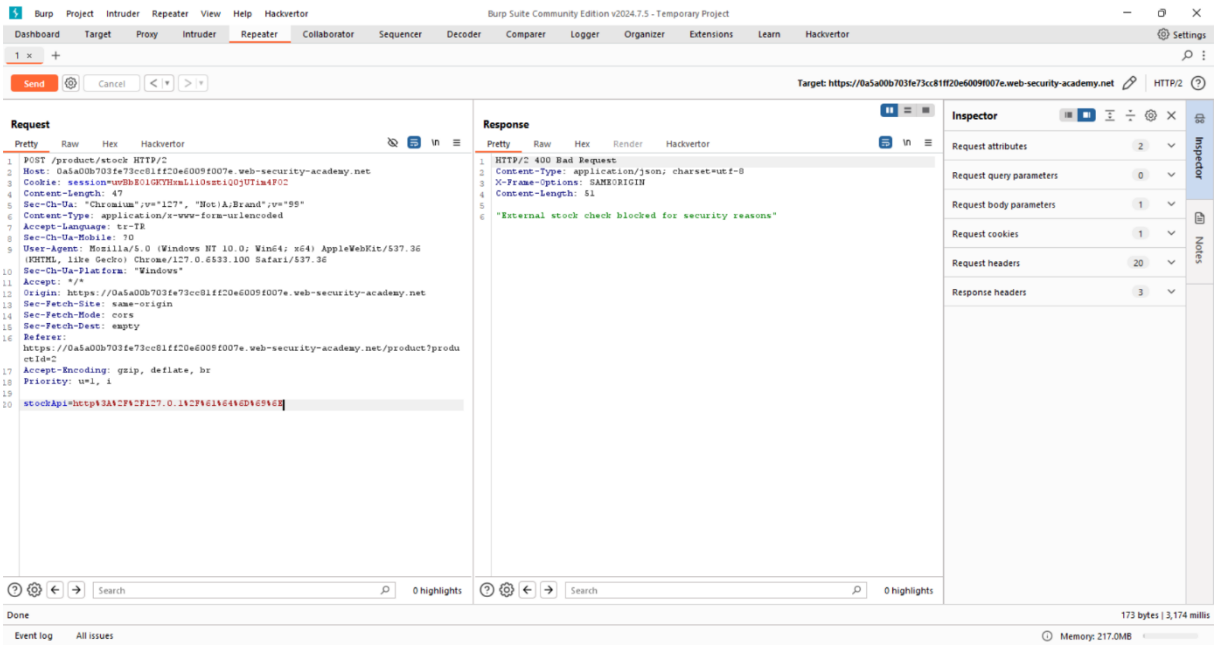
Burada 127.0.0.1 olarak değiştirdim ve sonuç değişmedi. Bu sefer de admin yazısı ile oynamaya başladım.



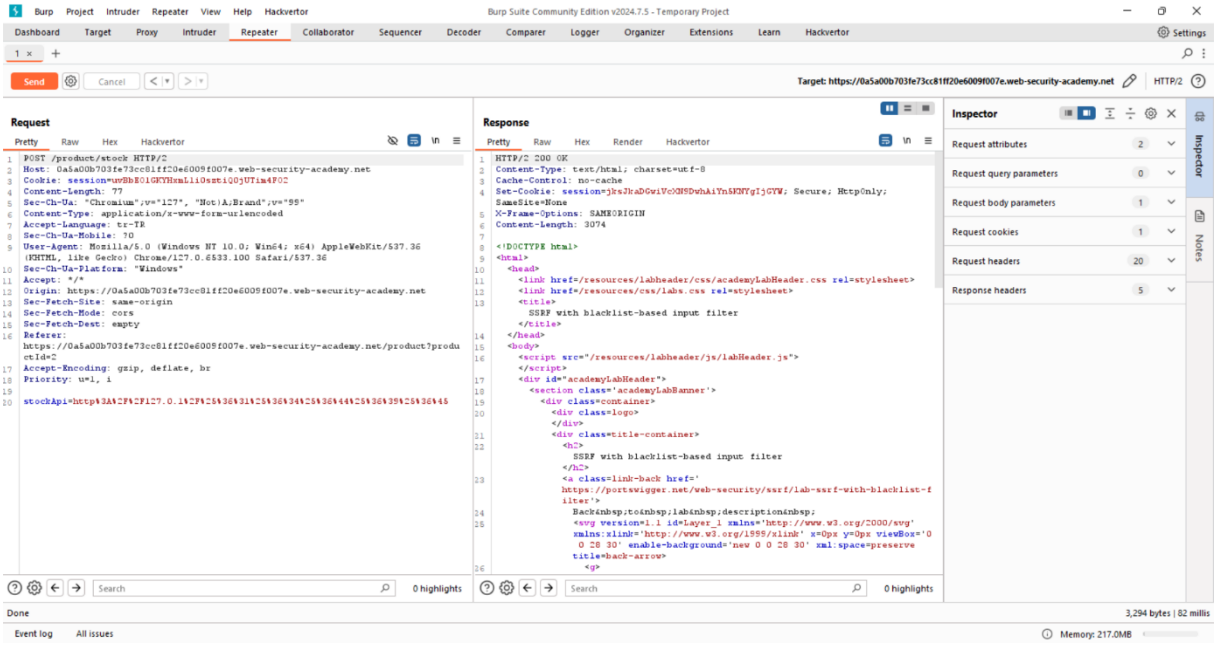
Local host ip ile biraz daha değişiklik yaptık “127.0.0.1” olarak kısalttık. Sonrasında hackvertor diye bir eklenti kullandım. Bu eklentiyle admin kelimesini urlencode_all seçeneği ile etiket arasına alıyoruz. Sonra aşağıdaki gibi bir görüntü çıkıyor.



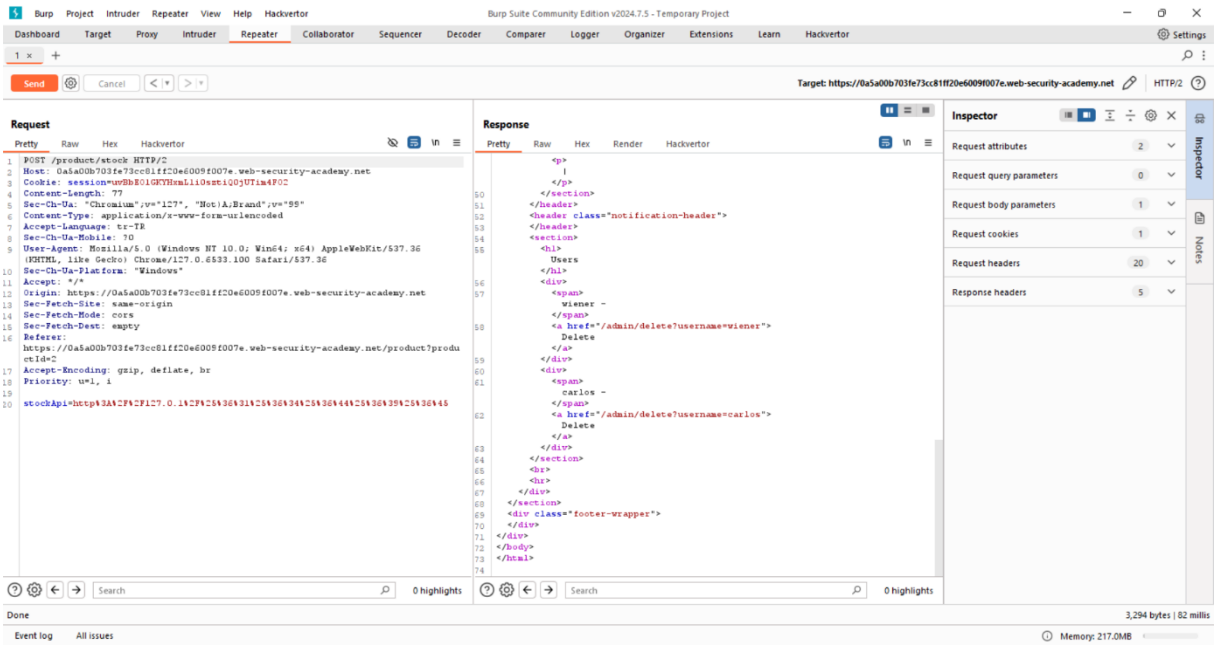
Burada yine aynı eklentiyi kullanarak convert tags seçeneğine basarak encode ediyoruz.



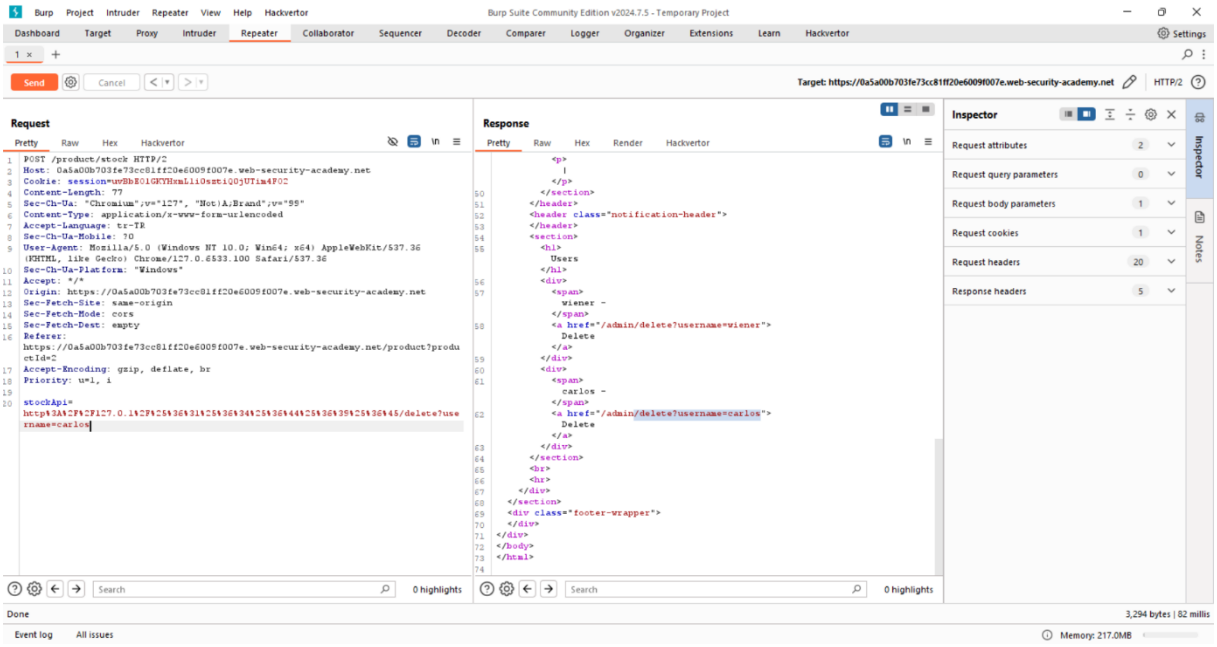
Encode edince tekrar denedik ve yine hata aldık. Bir tur daha encode ediyoruz. Aynı işlemleri buna uyguluyoruz ve aşağıdaki gibi bir görüntü çıkıyor.



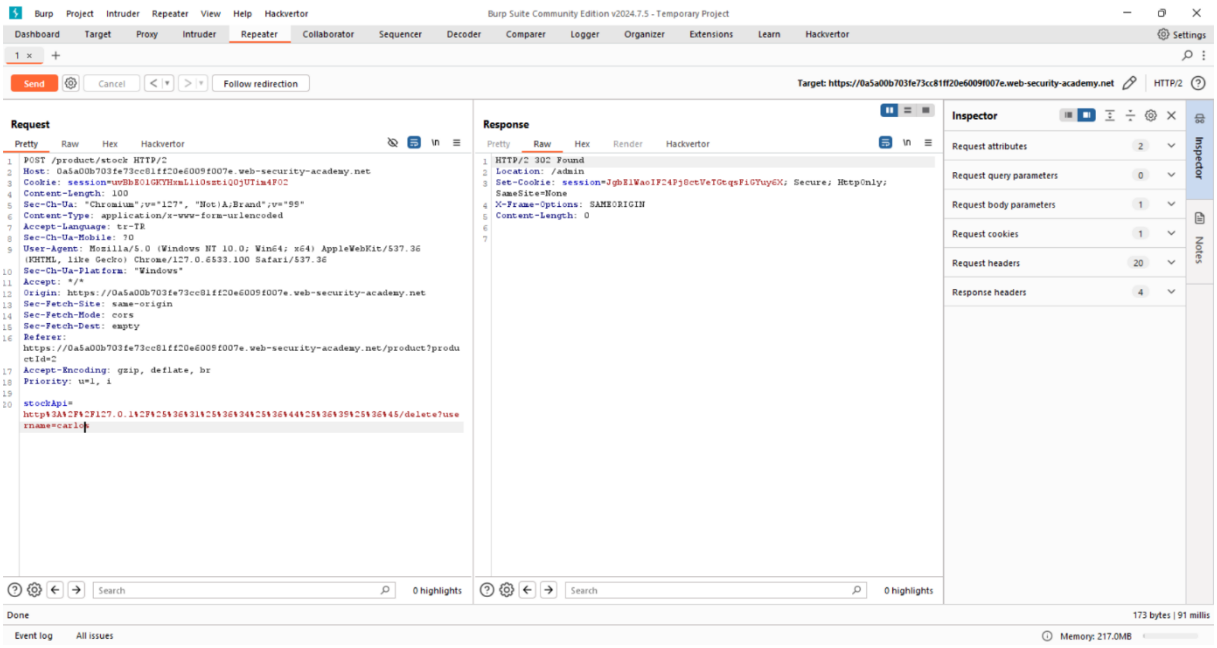
Burada admin panele girmeyi başardık sırada Carlos adlı kullanıcıyı silmek var.



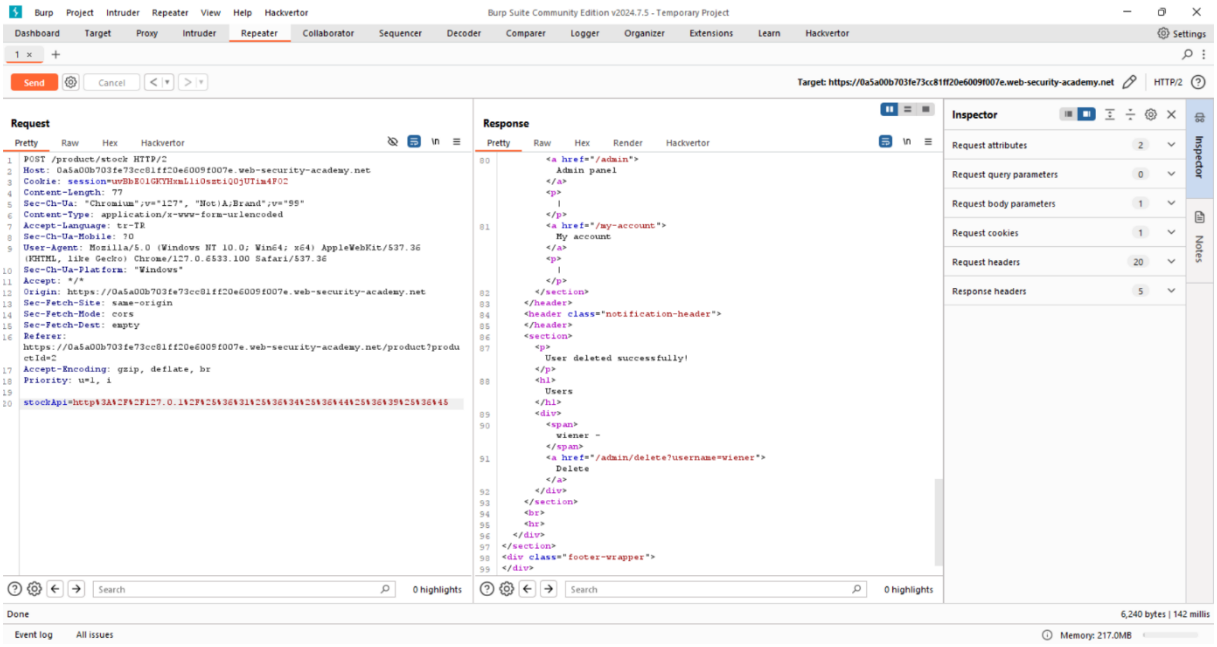
Bu kısımda Delete yolu gösterilmiş bunu kullanarak Carlos'u siliyoruz.



Bu şekilde yolu koyup çalıştırıyoruz.



Cevap olarak bize 302 döndü. Dönüp admin sayfasında tekrar kontrol ediyoruz.



Ve sonunda kullanıcı başarıyla silindi mesajını aldık.