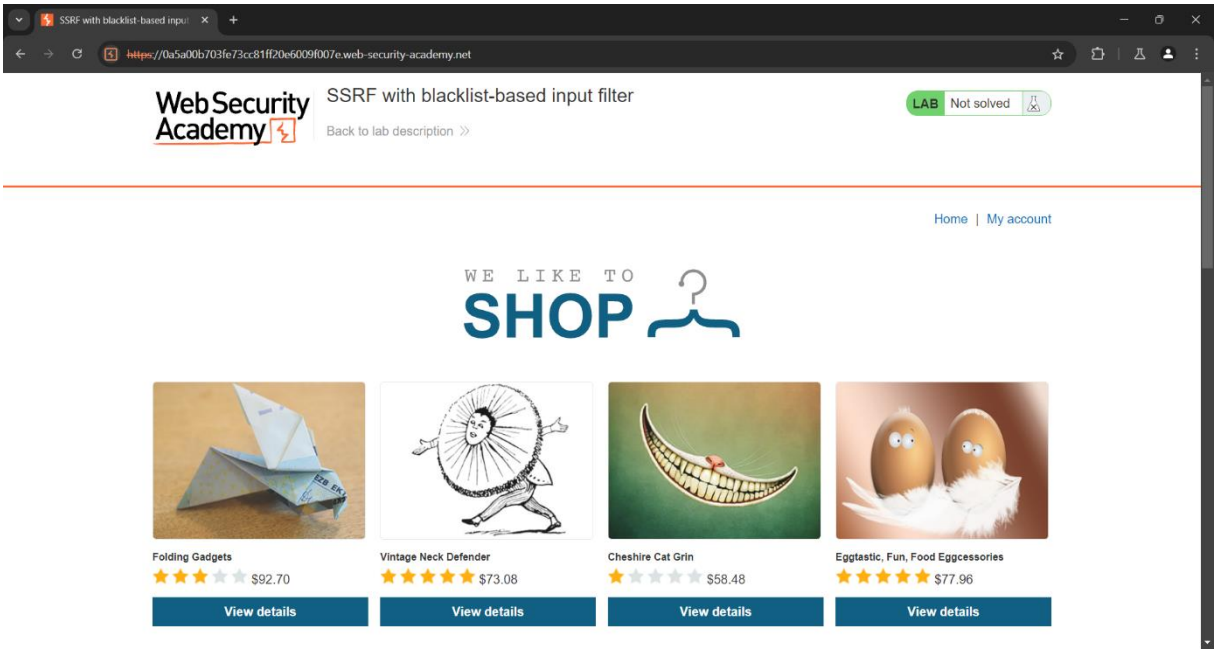
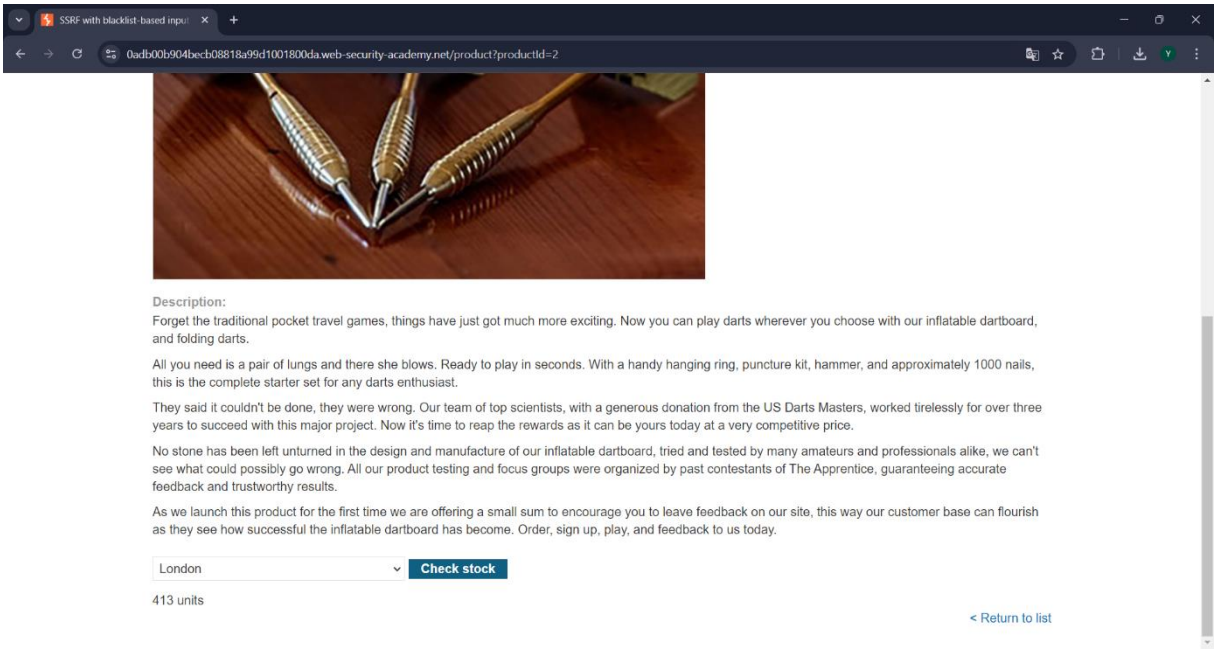
Portswigger Lab: SSRF Write-Up

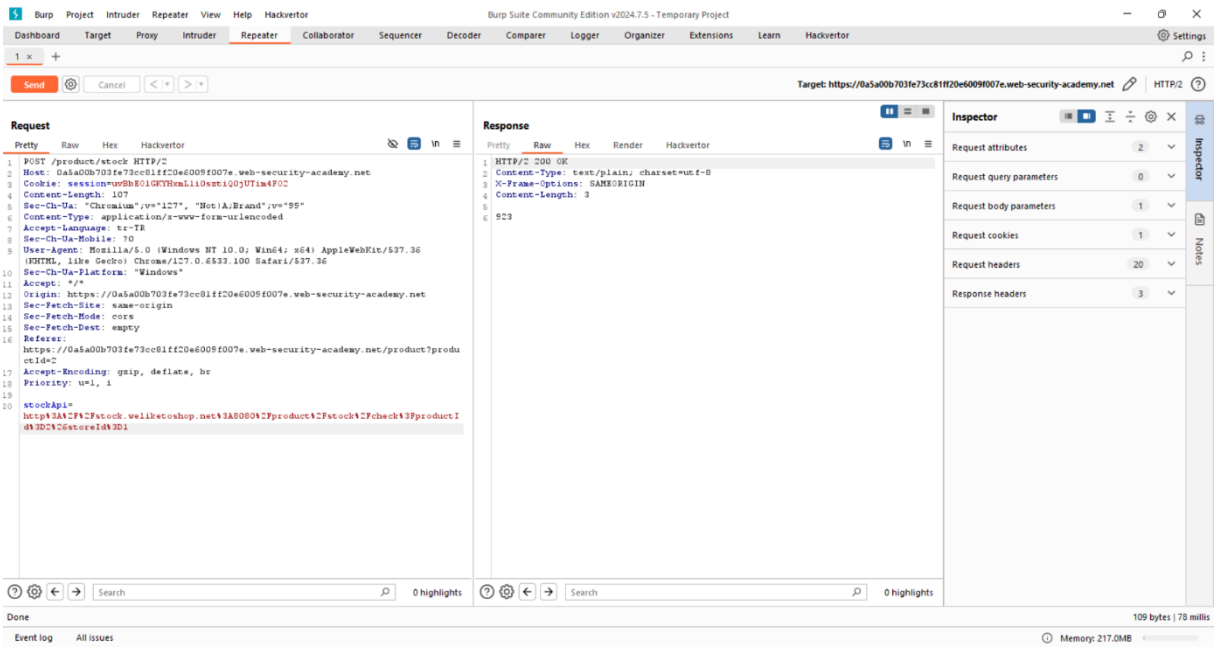
Bu sitemizin anasayfası burda ssrf ile Carlos adında ki kullancıyı silmemiz isteniliyor.



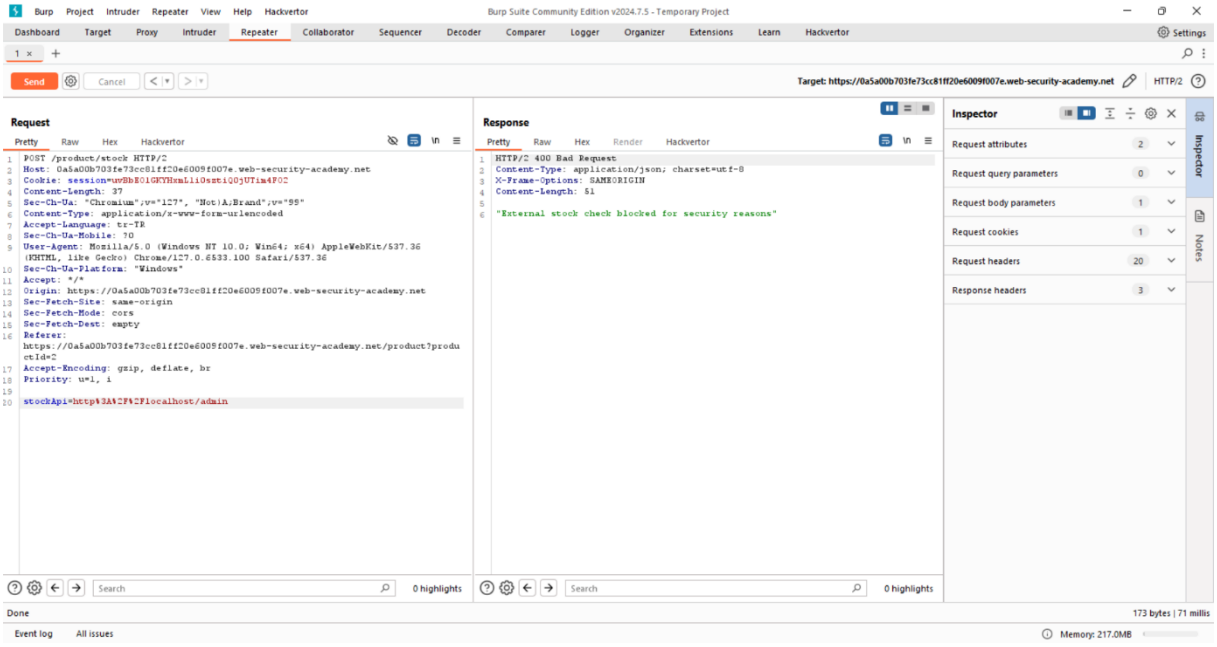
Bunun için ilk adım sunucu ile etkileşim kurulabilcek bir yer olmalı. Bunun için ürünlerin detaylarına bakalım.



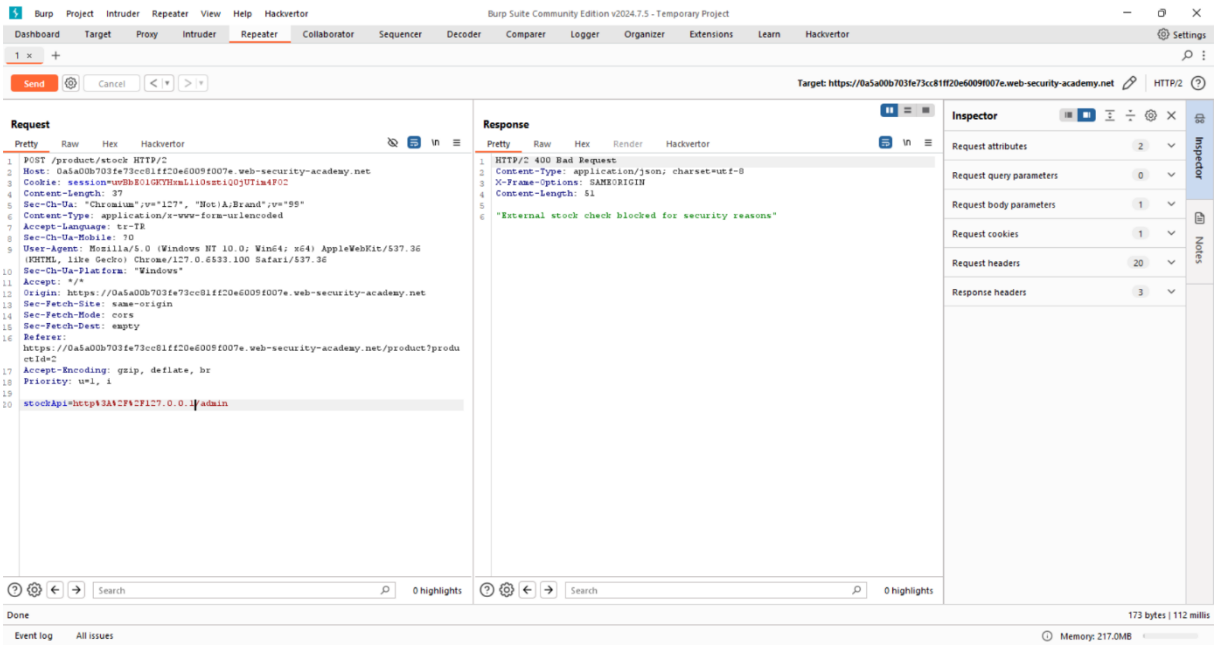
Rasgele bir ürün seçtim ve bu ürünün altında stok kontrol butonu vardı bunu burp suite ile takibe alalım.



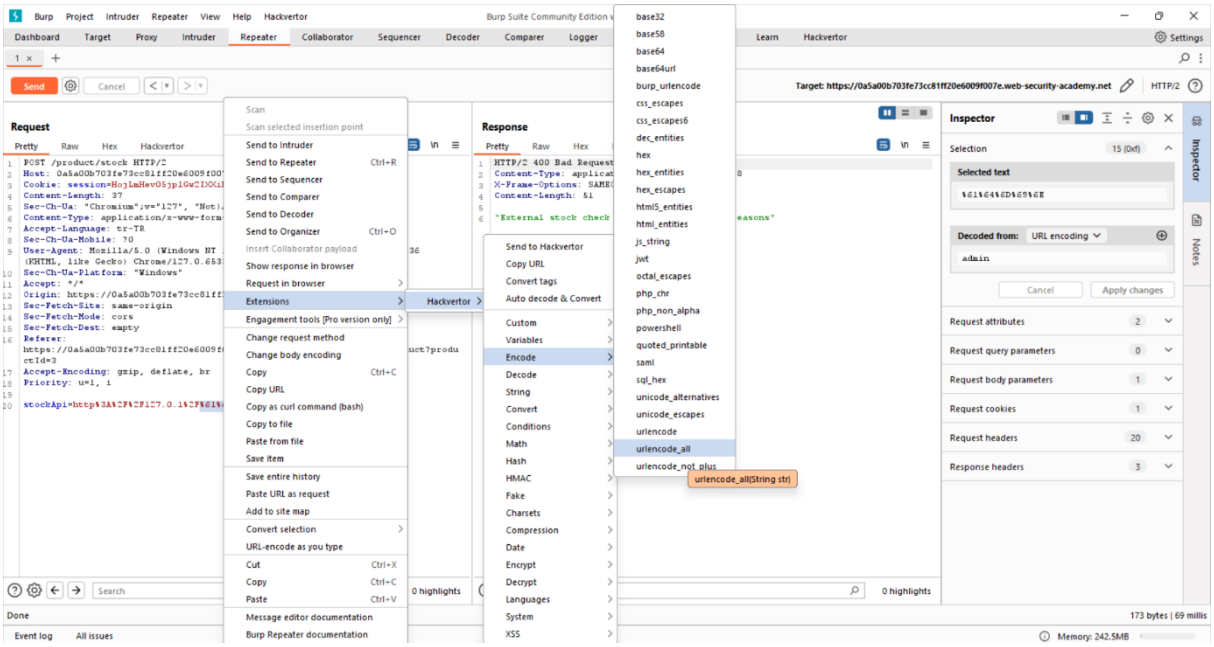
Karşımıza stockapi= diye bir parametre çıktı bununla oynamaya başlayalım.



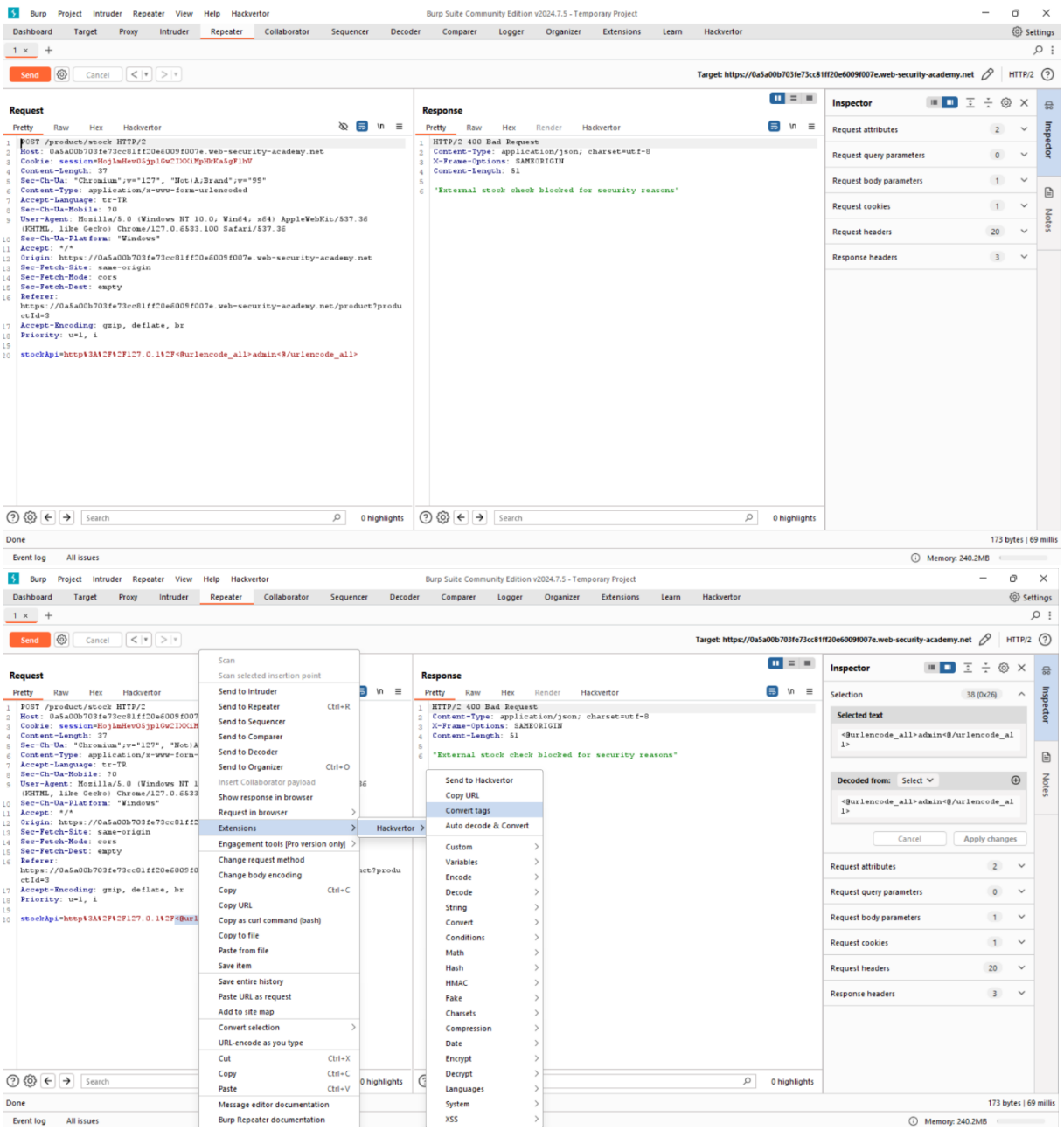
İlk önce portswiggerin verdiği şekilde http://localhost/admin girmeyi denedim ama bana bir mesaj döndü. Bu mesajdan sonra burayı bypass etmem gerektiğini anladım bunun için öncelikle localhost kısmını değiştirdim.



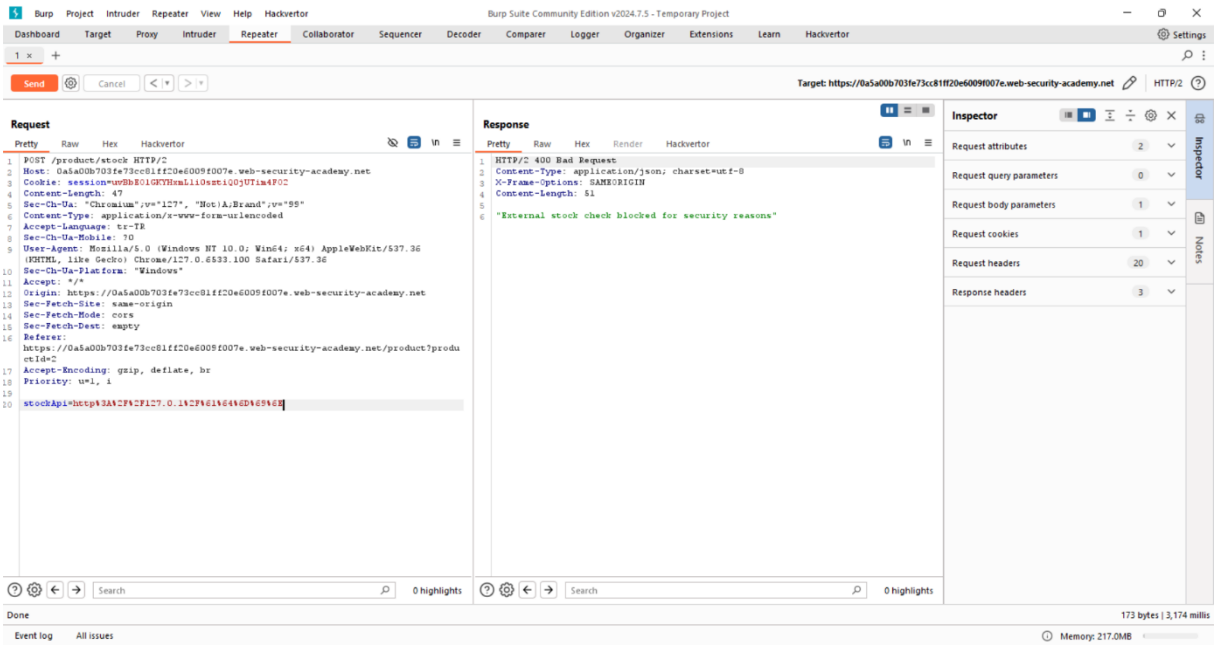
Burda 127.0.0.1 olarak değiştirdim sonuç değişmedi bu seferde admin yazısı ile oynamaya başladım.



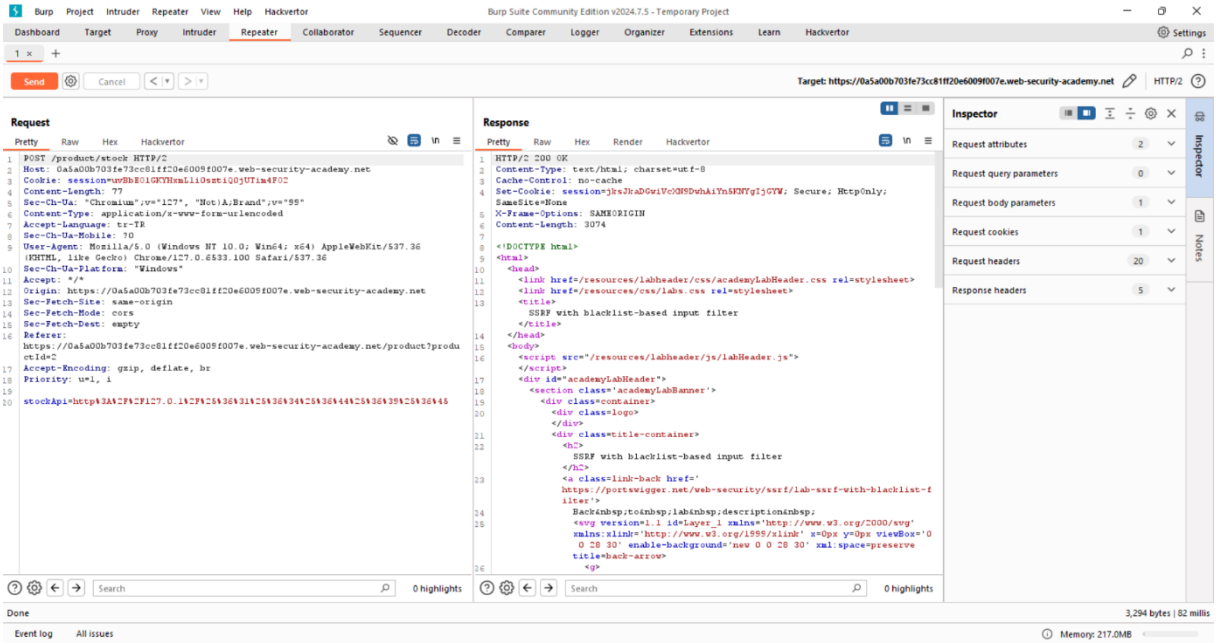
Burda hackvertor diye bir eklenti kullanıyorum bu eklenti ile admin kelimesini urlencode_all seçeneği ile dönüştürüyorum.Sonra aşağıdaki gibi bir görüntü çıkıyor.



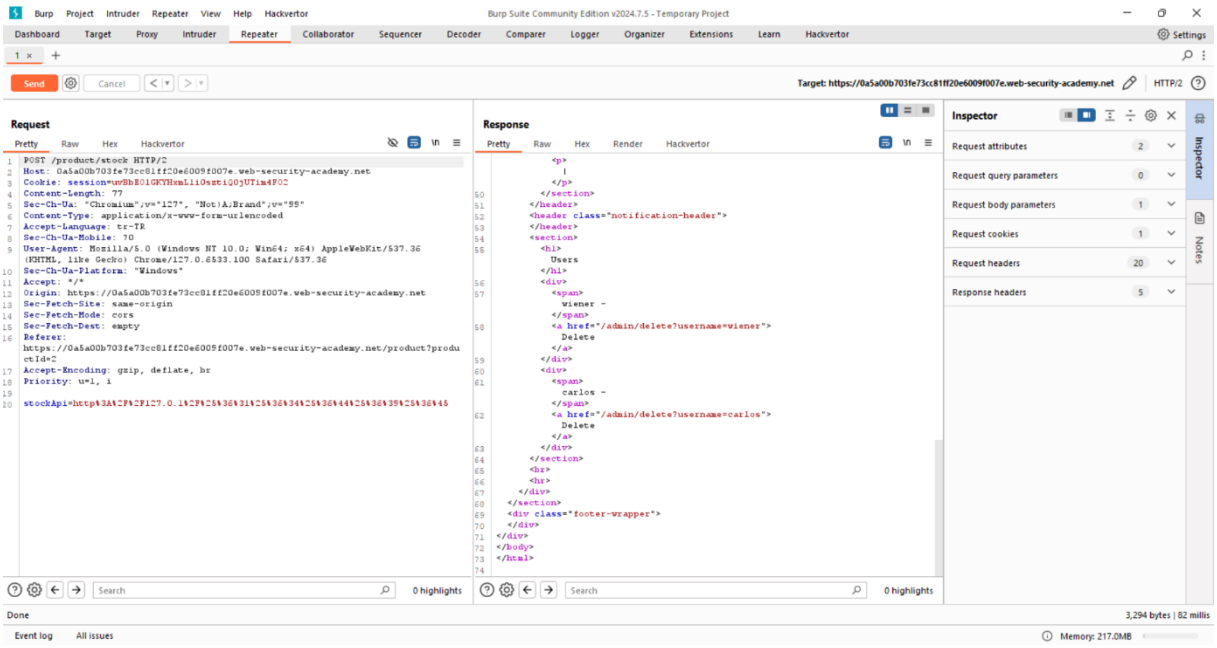
Burda yine aynı eklentiyi kullanarak convert tags seçeniğine basarak encode ediyoruz.



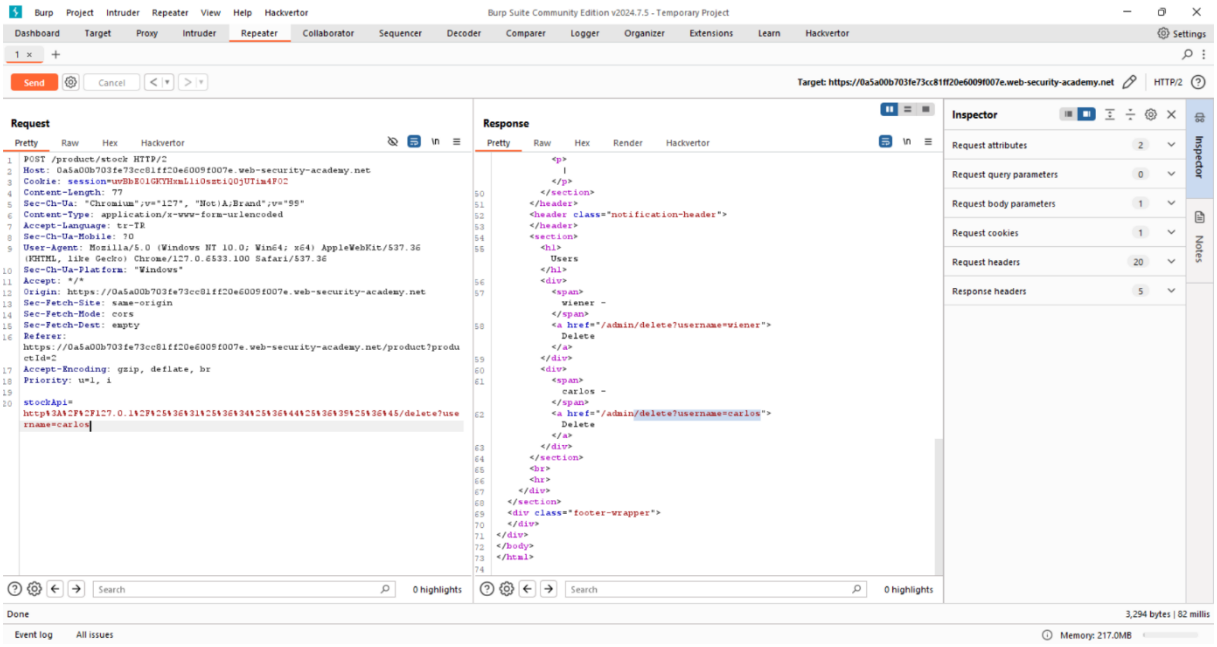
Encode edince denedik yine hata aldık bir tur daha encode ediyoruz.Aynı işlemleri buna uyguluyoruz ve aşağıdaki gibi bir görüntü çıkıyor.



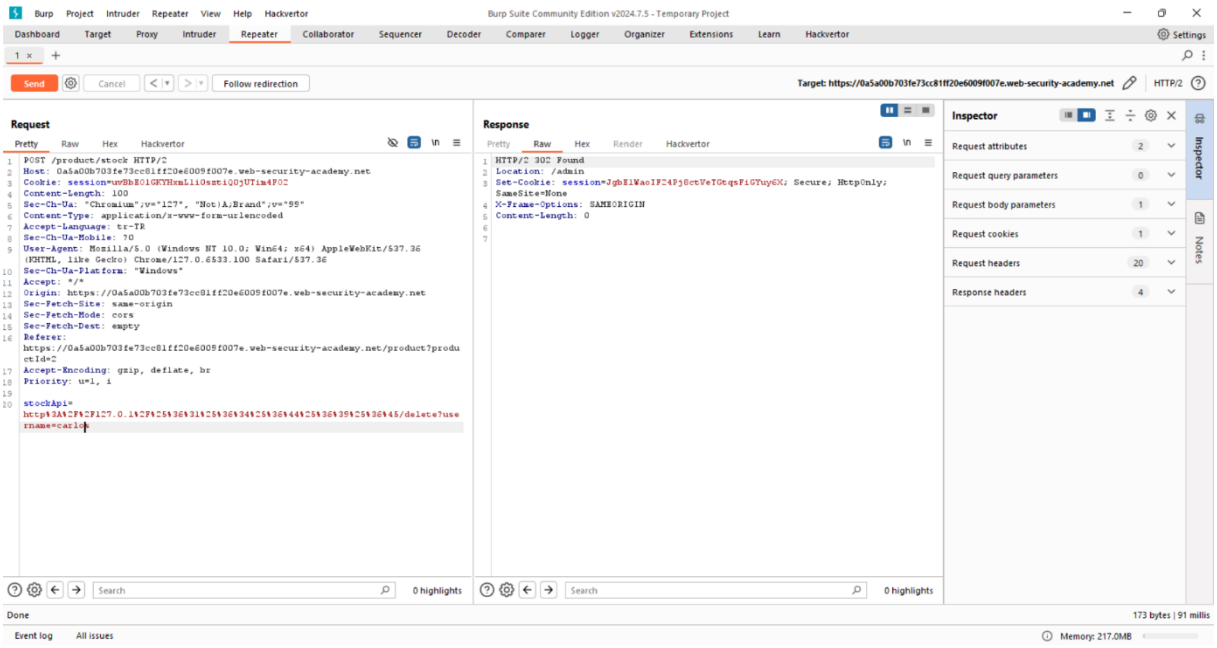
Burda admin panele girmeyi başardık sırada Carlos adlı kullanıcıyı silmek var.



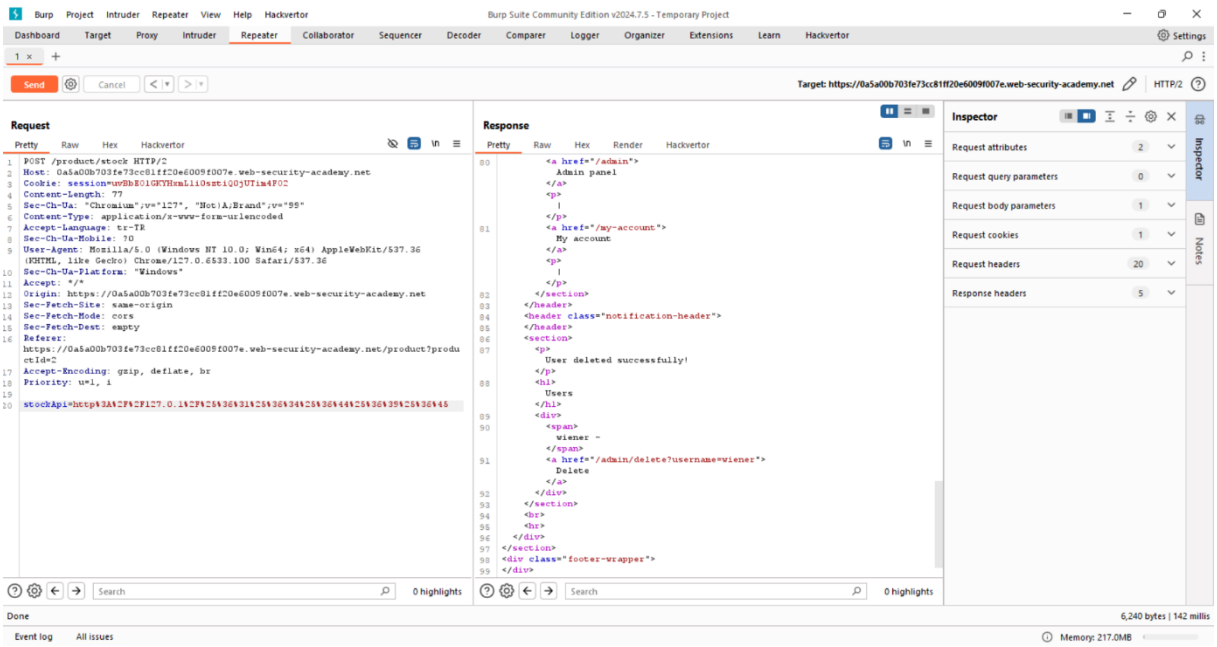
Bu kısımda Delete yolu gösterilmiş bunu kullanarak carlosu siliyoruz.



Bu şekilde yolu koyup çalıştırıyoruz.



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



Ve sonunda kullanıcı başarıyla silindi mesajı aldık.