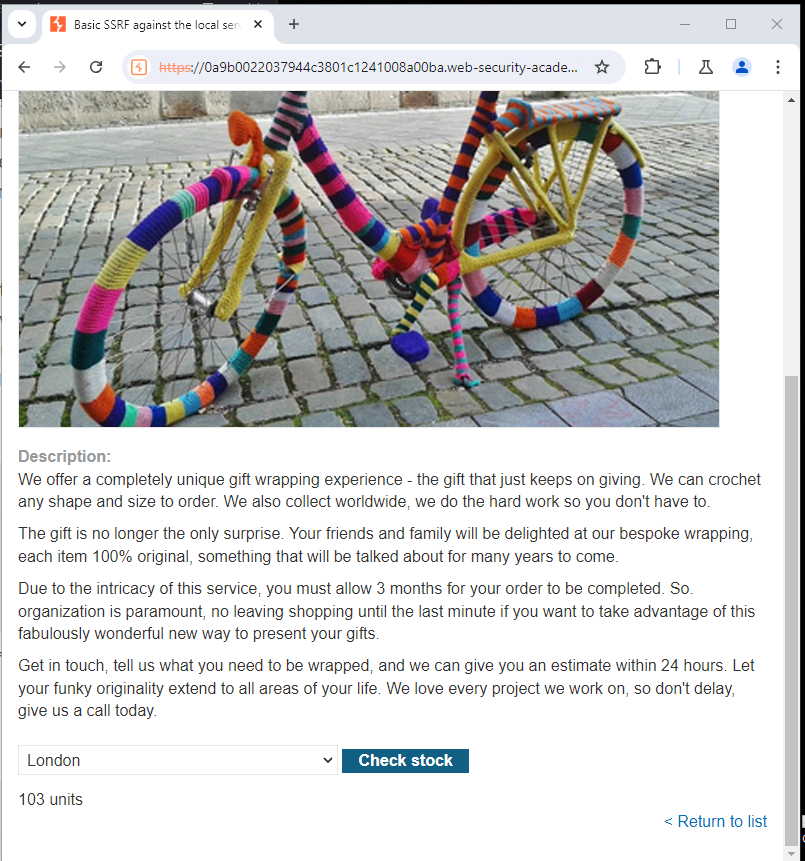
**Portswigger Writeup**

**Eren Ersoyluoğlu**

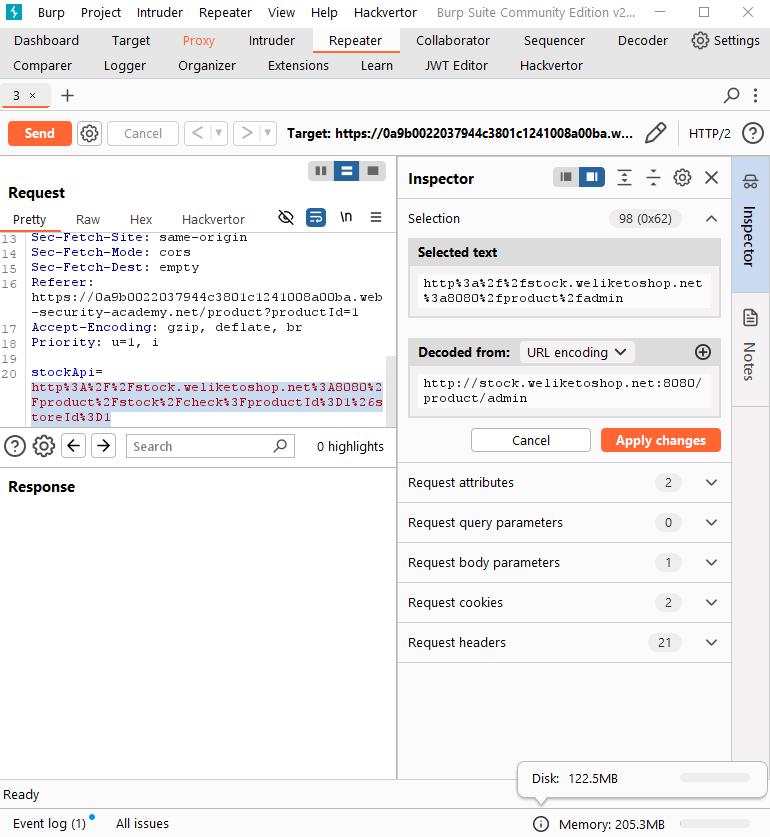
**Server-side request forgery (SSRF)**

**Localhost üzerinden SSRF saldırısı:**

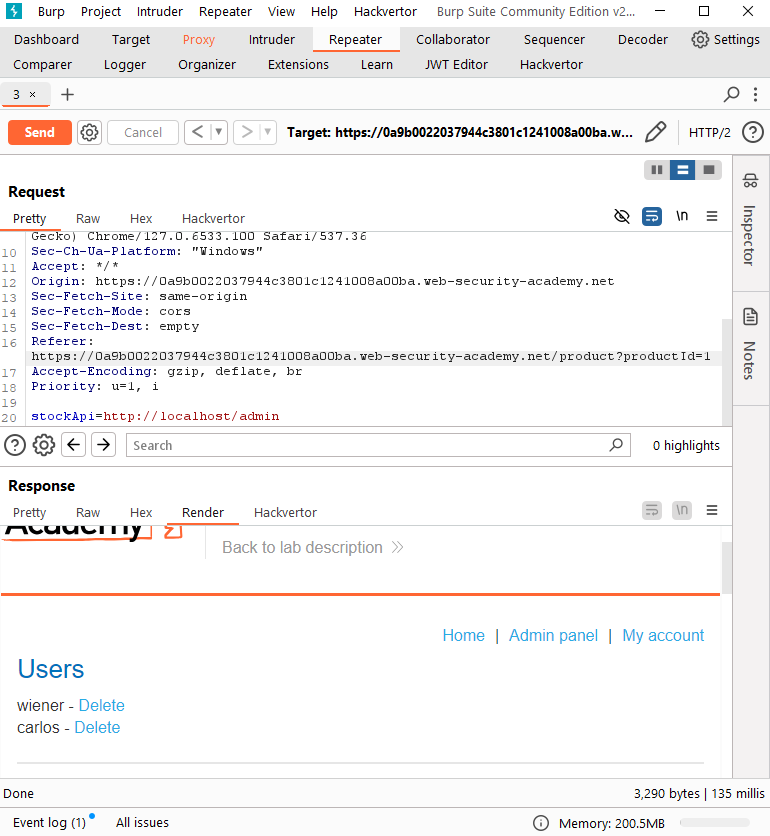
Zafiyetli siteye eriştiğimizde karşımıza bir alışveris sitesi çıkıyor, burda biraz inceleme yapınca ürünler hakkında stok bilgisi alabiliyoruz.



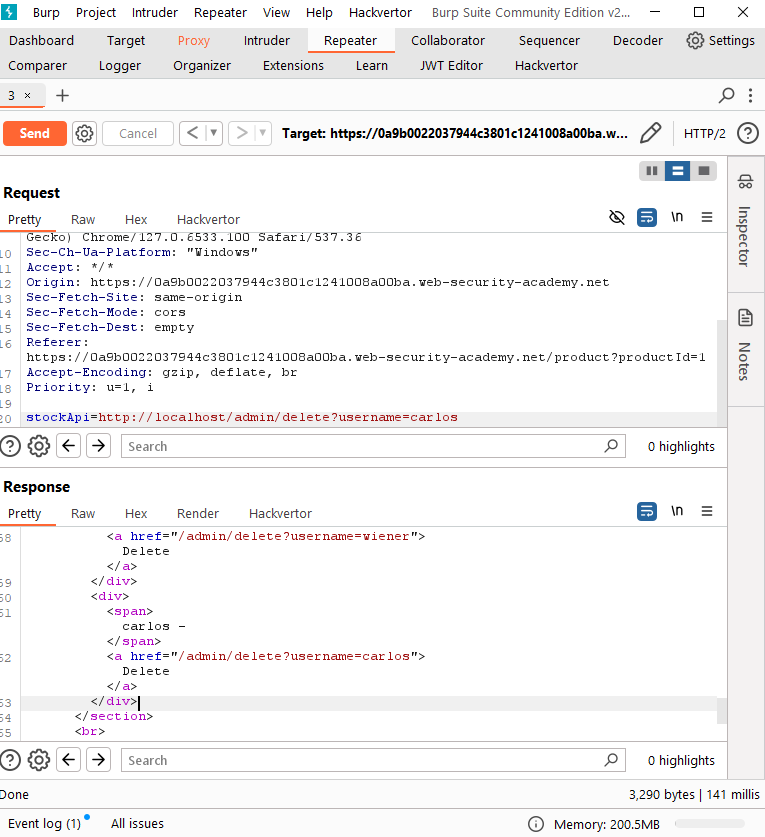
Bu isteği burp ile yakaladığımda stok kontrolü için bir Api çalıştığı ve bir sunucuya istek attıldığını gördüm



Bu istek üzerinde değişiklikler yaparak önce localhost’ a istek göndererek hata alıp almadığımı denedim sonrada localhost üzerinden amdin sayfasına erişmeye çalıştım.

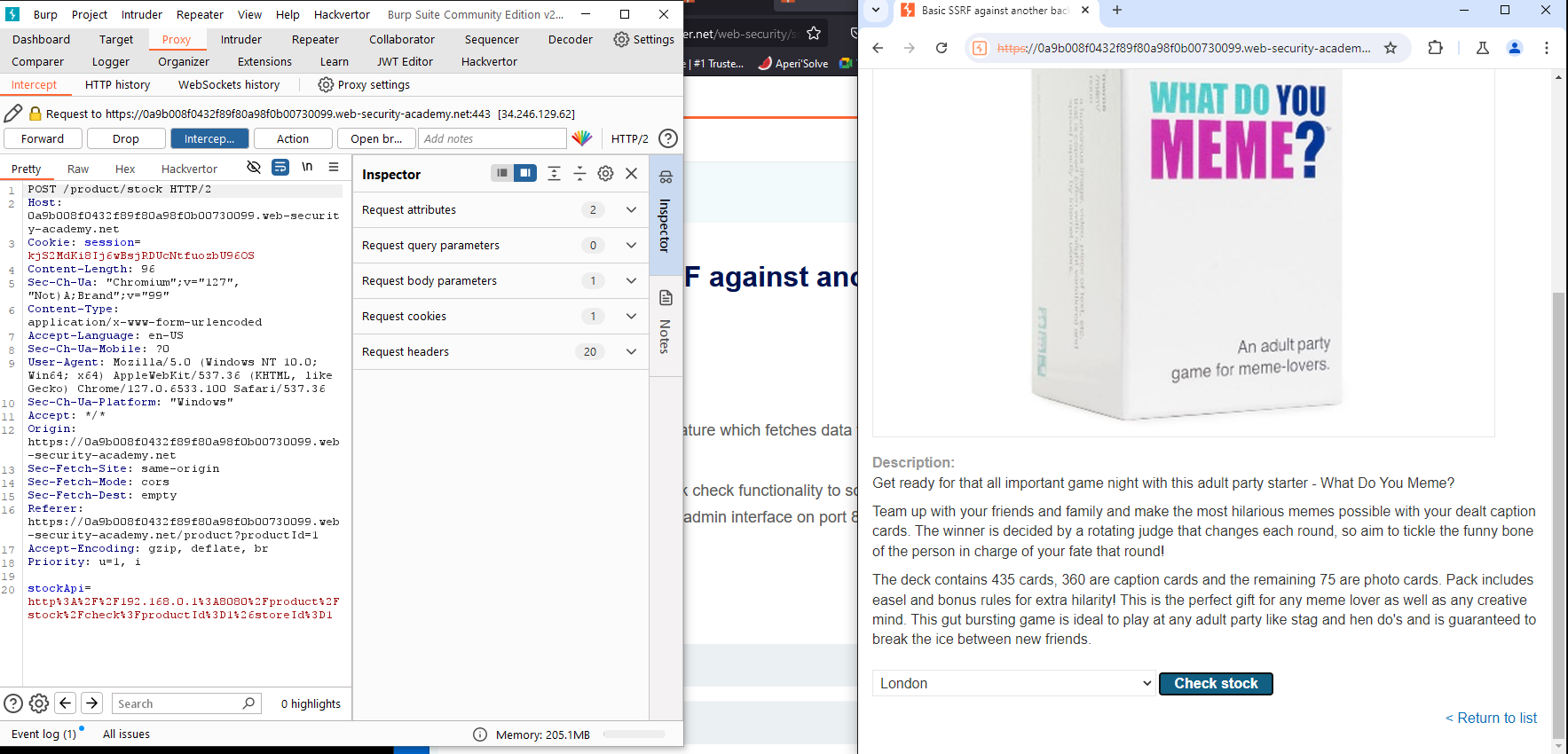


Admin sayfasından dönen respons’ a bakarak carlos kullanıcısını nasıl sileceğimi öğrendim ve bu isteği siteye gönderdim.

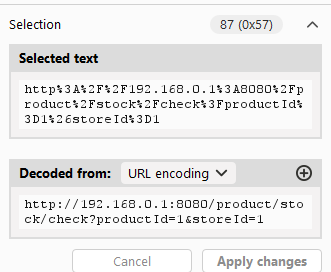


**Başka Back-end Serverlar üzerinden SSRF Saldırısı:**

Karşıma gelen alışveriş sitesini inceledim ve ürünler üzerinden stok kontrolü yapabildiğimiz öğrendim. Stok kontrolü yaparken back-end üzerinde başka bir IP de bulunan server’ a istek attığımızı fark ettim.



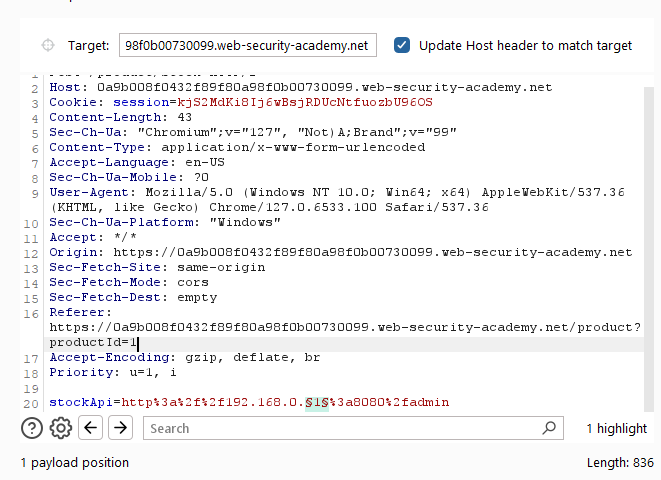
Gönderilen isteğin URL Decoded hali aşağıdaki gibidir:



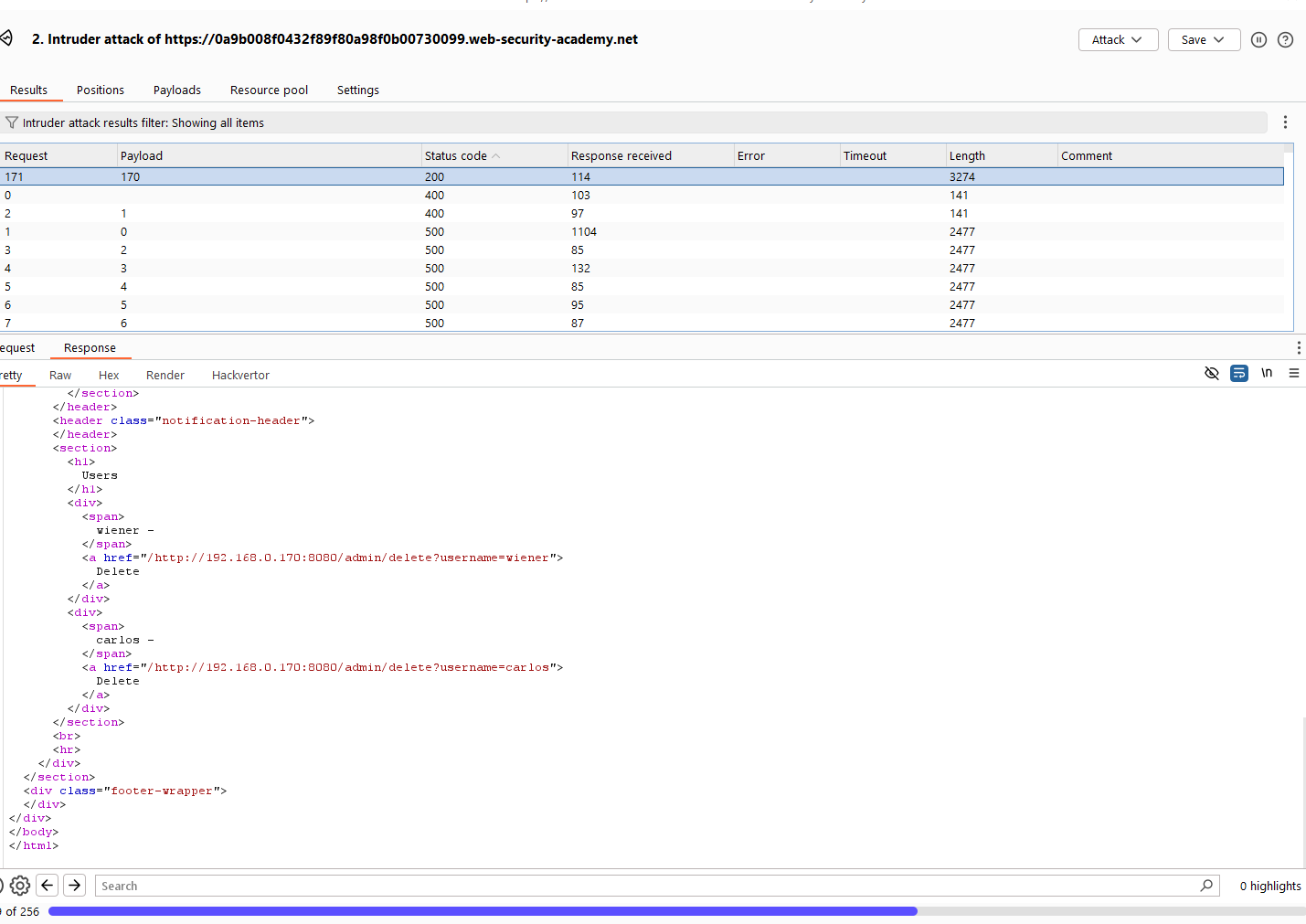
Bu ip üzerinde admin sayfasına erişmeye çalıştığımda hata aldığımı fark ettim.



Bunun üzerine back-end te çalışan başka IP varmı diye incelemek için burp intruder üzerinden 1 den 255 IP aralığına istek atıcak şekilde ayarladım.

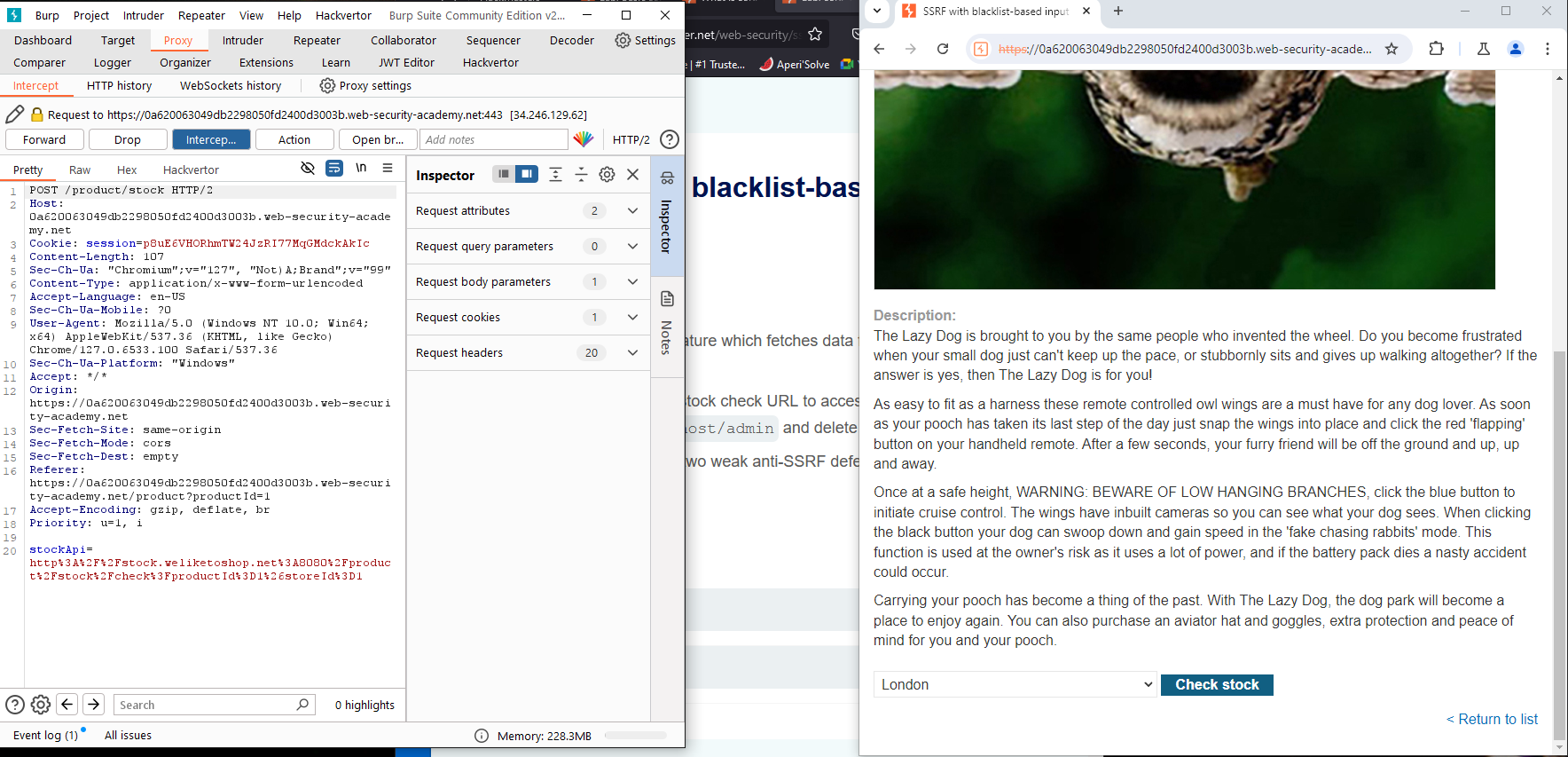


Gönderilen bir çok istekten sonra 170. IP’ de admin sayfasına erişim sağlayabildim ve bu isteği yönlendirerek Carlos kullanıcısını sitemden silebildim.

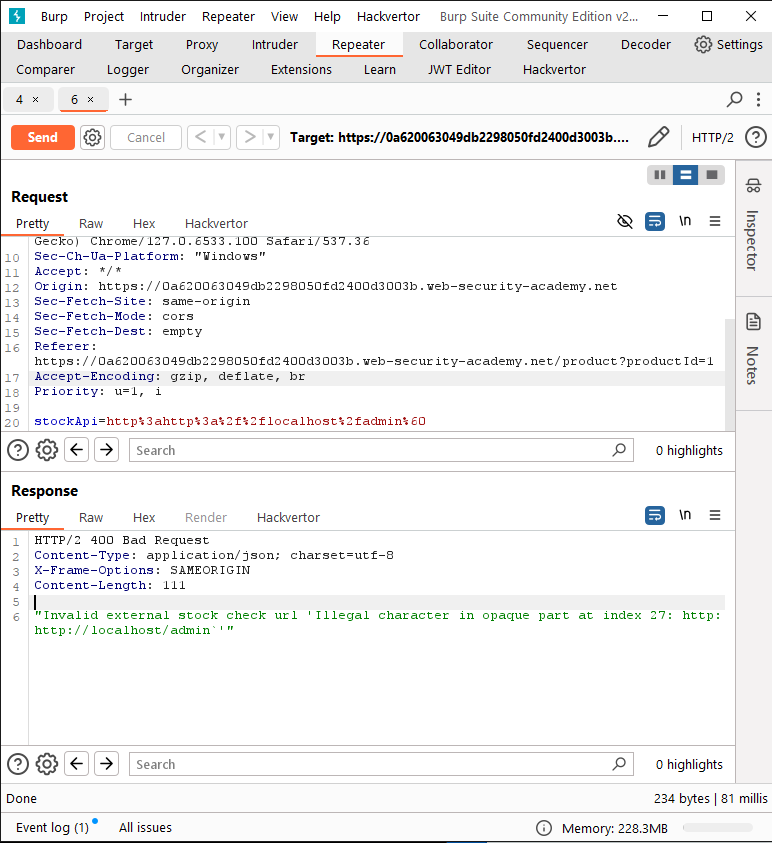


**Blacklist filtresini aşarak SSRF saldırısı:**

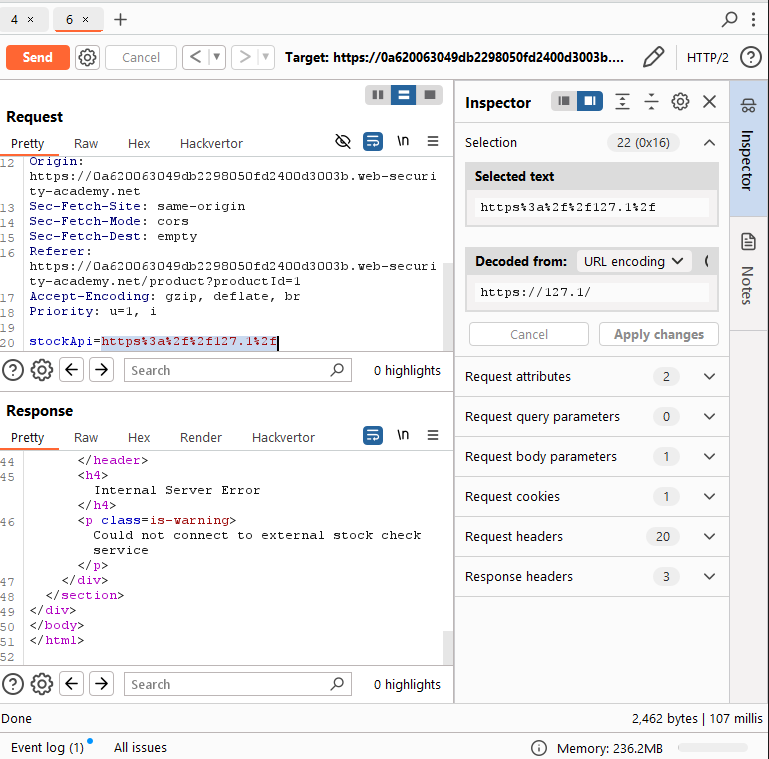
Siteye ulaştığımda ürünler üzerinden stok kontrolü yapabildiğimizi fark ettim, bu stok kontrolünü burp ile yakaladım.



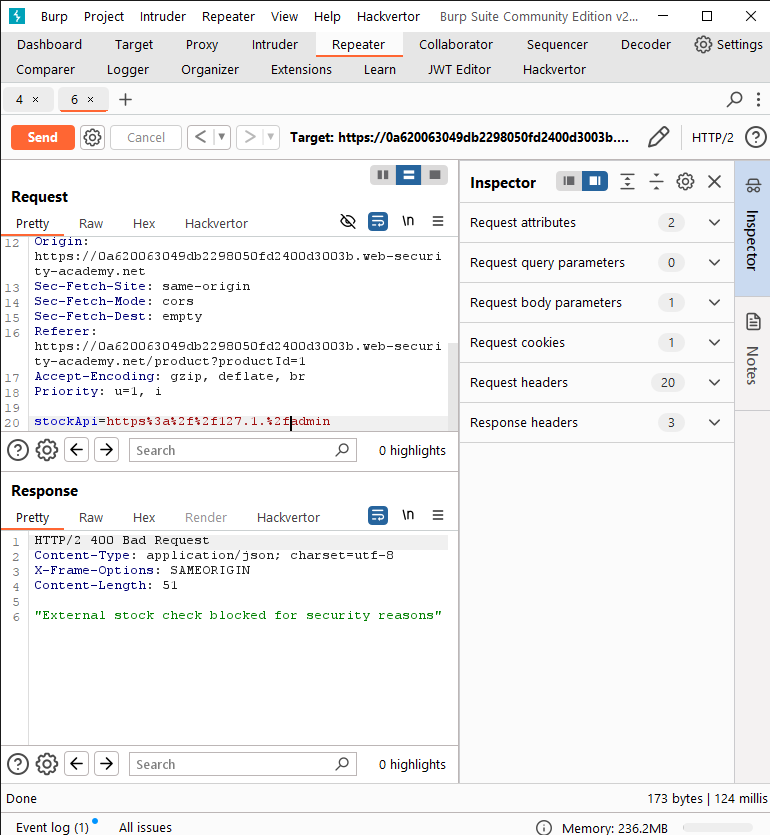
Repeater üzerinden istek gönderirken localhost ile admin sayfasına erişmeye çalıştım fakat localhost kelimesi Blacklist’ e alındığı için hata mesajı döndü.



Localhost yerine 127.0.0.1 yada sadece 127.1 kullanabilirdim ve 127.1 kullanmayı tercih ettim. 127.1 kullandığımda hata mesajının farklı olduğunu fark ettim ve buradan ilerledim.



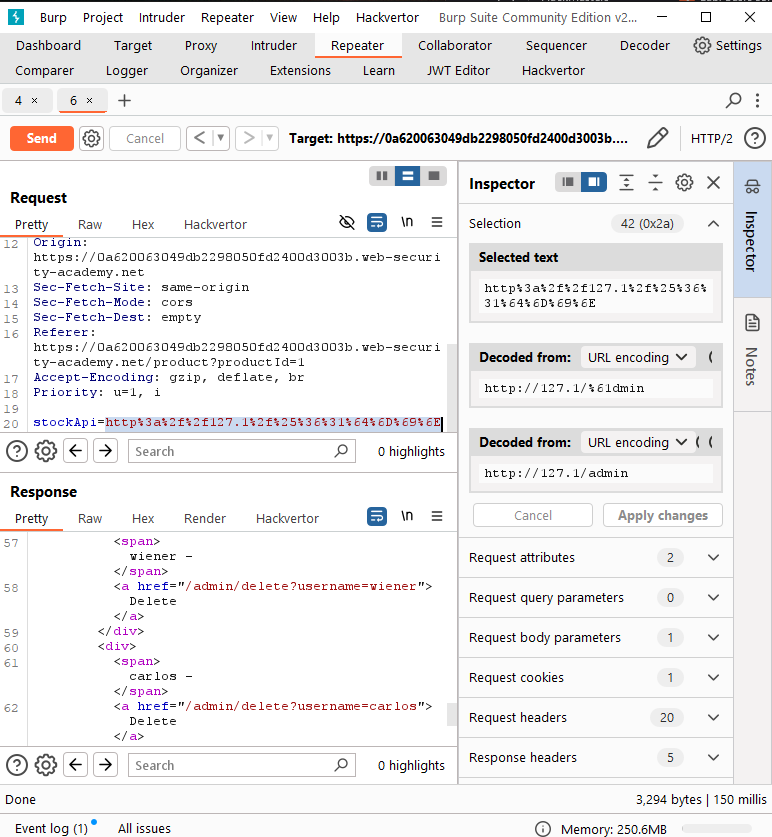
Admin sayfasına istek gönderdiğimde tekrar bir hata mesajı ile karşılaştım, admin kelimeside blacklist’ e alınmış.



Biraz araştırdığımda admin kelimesini URL Encode ederek gizleyebilceğimi düşündüm ve bütün harflerin URL karşılıklarına baktım.



Admin kelimesini bir kere Encode ettiğimde hata mesajı aldım fakat encode edilmiş halini tekrar encode ederek denediğimde admin sayfasına erişebildim ve bu isteği siteye göndererek Carlos kullanıcısını sildim.



**Identification and Authentication Failures**

**Response farklılığına göre Kullanıcı adı tahmini:**

Siteye erişim sağladığımda kullanıcı girişi tarafı ilgimi çekiyor.

A screenshot of a computer screen

Description automatically generated

Yaptığım giriş denemsini burp üzerinden yakalayıp bunu intruder a gönderiyorum

A screenshot of a computer screen

Description automatically generated

Aynı zamanda yaptığım denemede yanlış bir kullanıcı adı girdiğimde sistem bana bunu söylediğini görüyorum

A white rectangle with white lines

Description automatically generated

Kullanıcı adını işaretleyerek verilen wordlist üzerinden brute force saldırısı gerçekleştiriyorum.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

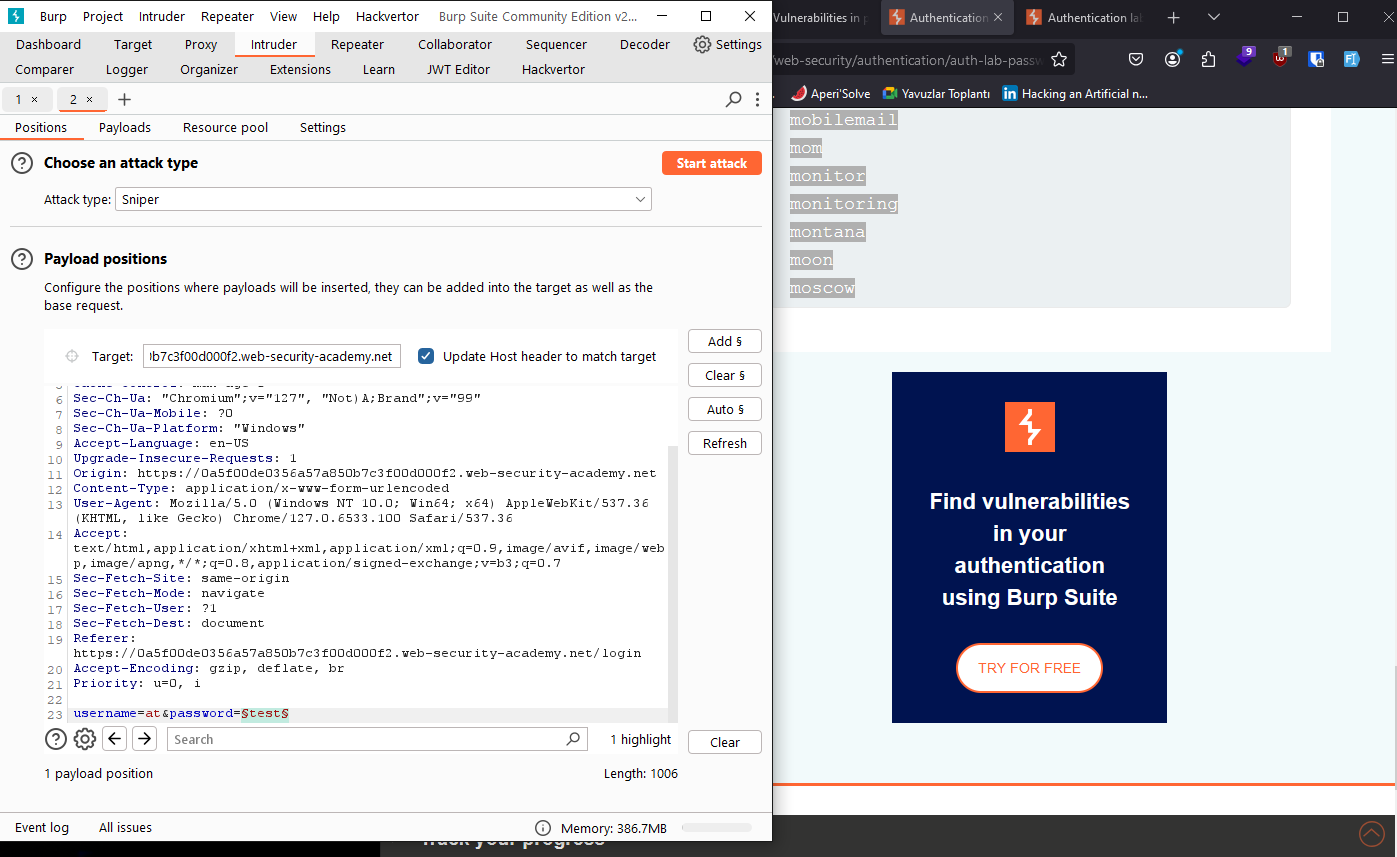
Description automatically generated

Saldırı saonucunda “at” kullanıcısnın daha farklı bir Response uzunluğuna sahip olduğunu görüyorum ve isteği incelediğimde bana yanlış parola diye uyarı döndüğünü görüyorum.

A screenshot of a computer

Description automatically generated

“at” kullanıcısını kullanarak bu seferde parola üzerinde bir brute force atağı gerçekleştiriyorum ve bu şekilde kullanıcı parolasınıda keşfediyorum.



A screenshot of a computer

Description automatically generated

**Response farklılığına göre Kullanıcı adı tahmini:**

Siteye erişim sağladığımda kullanıcı girişi yapmayı deniyorum ve bu sefer her yanlış denemede “Invalid username or password” hatası alıyorum.

A screenshot of a login form

Description automatically generated

Bu isteği burp ile yakalayıp Intruder’ a gönderiyorum.

A screenshot of a computer screen

Description automatically generated

Tekrardan kullanıcı adını işaretleyerek verilen wordlist’ i payload olarak ekliyorum ve Intruder’ ın ayarlarından grep-match özelliğini kullanarak “Invalid username or password” dönen bütün Respons’ ları işaretlemesini istiyorum. Burdaki amacım tüm hatalı girişlerde “Invalid username or password” olarak dönüşmü alıyorum yokda doğru bir kullanıcı girişi denendiğinde başka bir hata mesajı dönüyormu onu görmek.

A screenshot of a computer

Description automatically generated

Saldırı sonucu acceso kullanıcısnın işaretlenmediğini görüyorum demekki bu kullanıcı sistemde gerçekten bulunuyor.

A screenshot of a computer

Description automatically generated

Bu kullanıcı adı üzerinden parola denemeside yaptıktan sonra başarılı bir şekilde sisteme giriş yapabiliyorum

A screenshot of a computer

Description automatically generated

**Response süresine göre kullanıcı adı tahmini:**

Siteye erişim sağlıyorum ve kullanıcı girişi ekranında burp ile inceleme yapmaya başlıyorum. Bana verilen kullanıcı bilgisi ile giriş yapıyorum ve bu request’ i burp ile yakalıyorum.

A screenshot of a computer

Description automatically generated

Yakaladığım istek üzerinde deneme yaptıkça bir süre sonra giriş yapmaktan engellendiğimi görüyorum.

A screenshot of a computer

Description automatically generated

Biraz araştırdıktan sonra burp üzerinden “X-Forwarded-For” header’ ını isteğime ekleyerek bu engelden kaçabilceğimi görüyorum.

A white text on a white background

Description automatically generated

Denemelere devam ederken parolanın uzunluğu response time üzerindeki etksiini fark ediyorum, parola yanlış olsa bile parola ne kadar uzunsa o kadar uzun sürede sistem geri dönüş yapabiliyor.

A screenshot of a computer

Description automatically generated

Bunun üzerine isteği Intruder’ a gönderiyorum ve bana verilen wordlist ile username denemesi yapıyorum, aynı zamanda X-Forwarded-For içinde bir sayı payload’ ı hazrıladım böylelike sistem tarafından Engellenmeden saldırıma devam edebilirim.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Yaptığım brute force sonucunda “ak” kullanıcısında normalden uzun bir response sresi görüyorum, demekki bu sistemde olan bir kullanıcı ismi.

A screenshot of a computer

Description automatically generated

Bana verilen wordlist ile parola denemesi yaptığımda da parolayı bulabiliyorum.

A screenshot of a computer

Description automatically generated

**XML external entity (XXE)**

**XXE ile sistemden dosya okuma:**

Siteye erişim ağladığımda ürünlerde stok kontrolü yaparken XML kullanıldığını görüyorum.

A screenshot of a computer

Description automatically generated

XML kullanarak sistem dosyasını okumak için xxe adında bir obje oluşturuyorum ve bu objeye etc/passwd dosyasını atıyorum, xxe objesini productid içinde çağırdığımda dosya başarılı bir şekilde response’ ta gözüküyor.

A screenshot of a computer

Description automatically generated

**XXE kullanarak siteden dosya okuma:**

Siteye erişim sağladığımda ürünlerde stok kontrolü yaparken XML isteği gönderildiğini görüyorum.

A screenshot of a computer

Description automatically generated

Bu XML tag i içinde xxe olarak bir değişken tanııyp buna soruda bize verilen URL yi tanımlayınca response tarafında “latest” diye dönüş alıyorum.

A screenshot of a computer

Description automatically generated

Dizinleri tke tek gezdikten sonra admin kullanıcısının bilgilerine ulaşıyorum.

A screenshot of a computer

Description automatically generated

**Dosya çekmek için Xinclude kullanmak:**

Siteye eriştiğimde bu sefer Stok kontrolü için doğrudan bir XML kullanımı göremiyorum.

A screenshot of a computer

Description automatically generated

XML sorgusunun server-side çalıştığını görmek için xxe adında bir entity gönderiyorum ve entity kullanımın engellendiği hakkında uyarı alıyorum.

A screenshot of a computer

Description automatically generated

XML sorgusuna direk erişimim olmadığı için önce Xinclude’ u sisteme tanıtıyorum ve Xinclude kullanarak istediğim dosyayı çekebiliyorum.

A screenshot of a computer

Description automatically generated