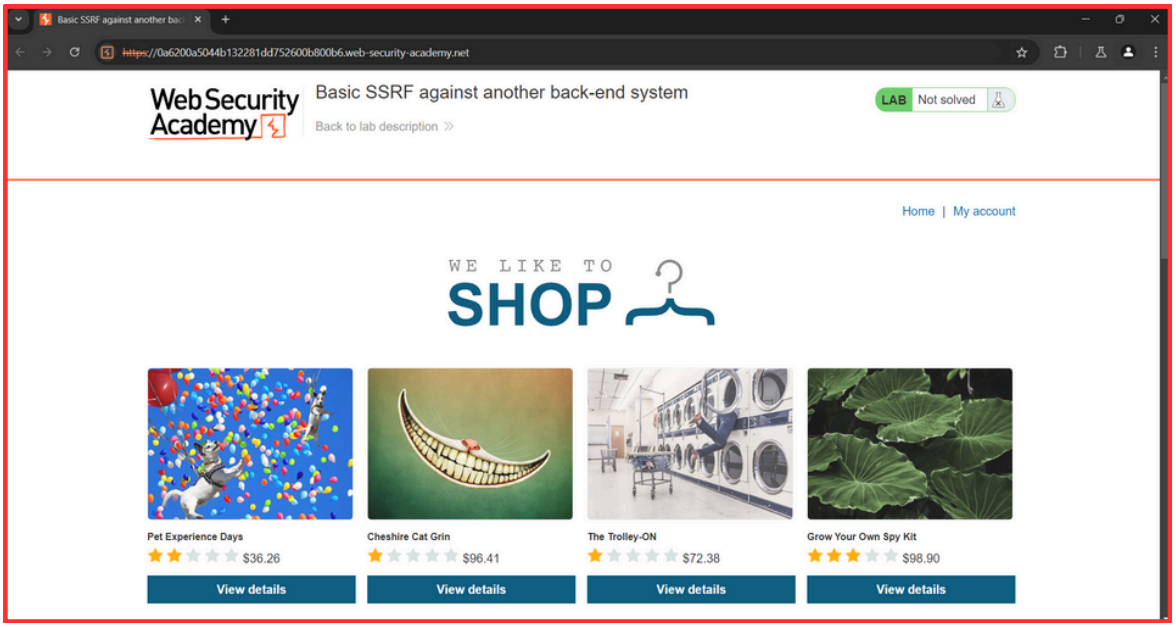
SSRF

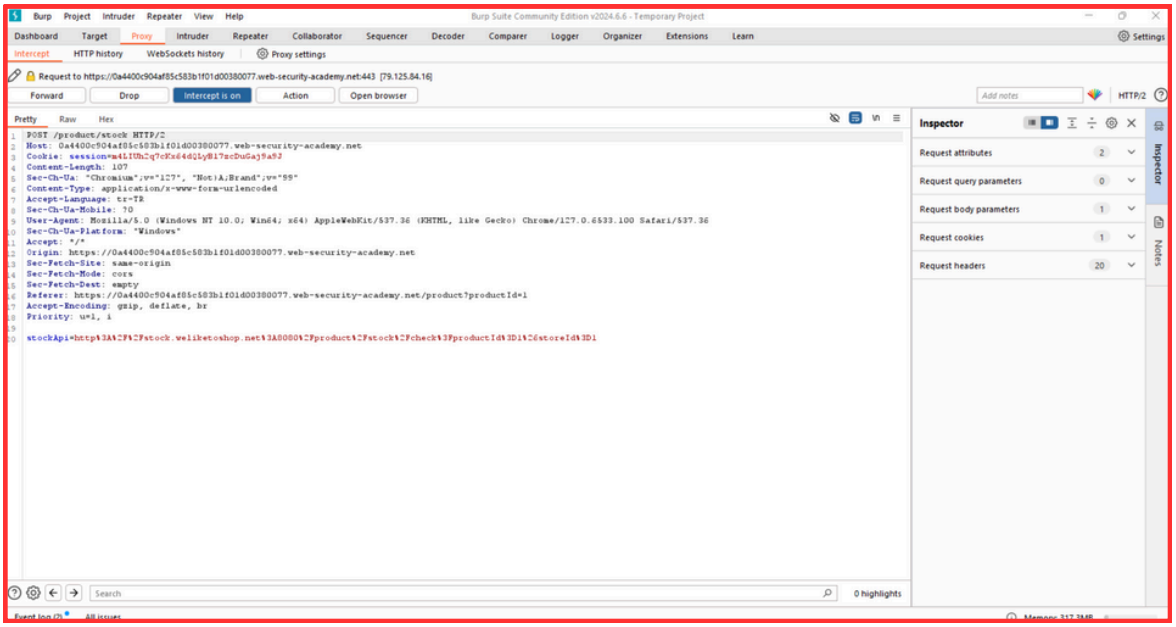
LAB 3

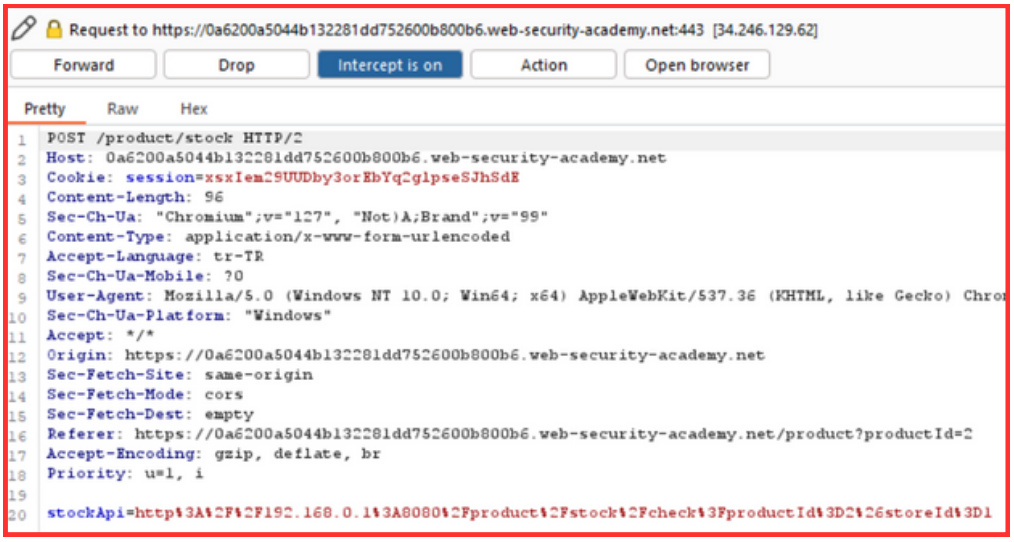
TARİH: 30.08.2024



Bu lab için bizden, zayıf anti-SSRF savunmalarını aşarak stok kontrol URL'sini http://localhost/admin adresine yönlendirip carlos kullanıcısını silmemiz istenmektedir.

Burada ihtiyaç duyabileceğimiz için önce BurpSuite programını açtım. Ardından bir ürünün sayfasına giderek stok kontrol butonuna tıklayıp bu paketi BurpSuite üzerinde yakaladım.

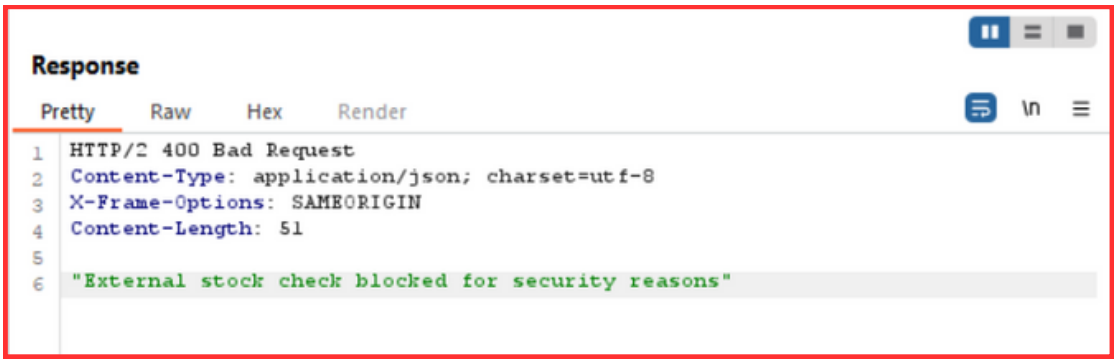




Yakaladığımız HTTP paketi içerisinde stockApi adında bir parametre bulunuyor. Bu parametre içinde bir URL verilmiş, muhtemelen aradığımız kısım burası. Paketi Repetear'a gönderip parametredeki URL kısmını http://127.0.0.1/ şeklinde değiştirdim.

```
stockApi=http://127.0.0.1/
```

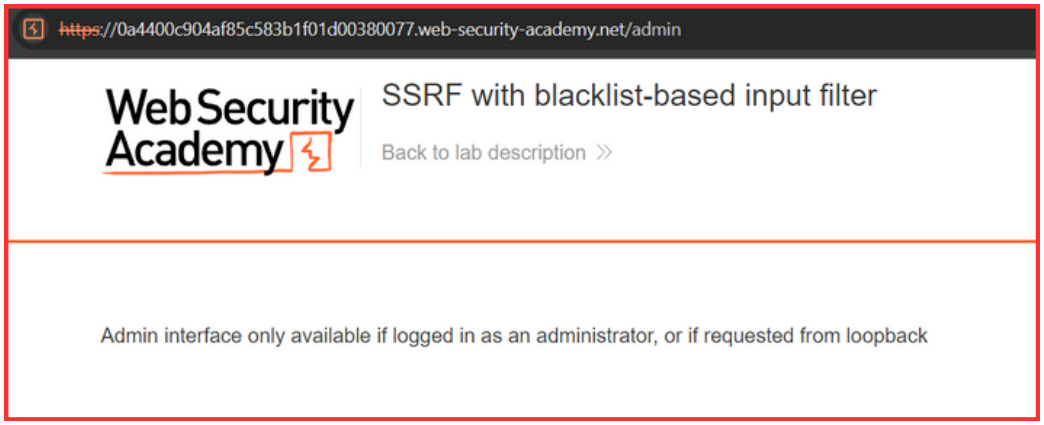
Düzenledikten sonra paketi gönderdim ve sunucudan gelen yanıtı inceledim. Bize dönen cevapta bazı güvenlik sebeplerinden dolayı engellendiğimizi söylüyor. Bunu by-pass edebilmek için farklı şekillerde URL parametresini denememiz gerek.



```
stockApi=http://127.1/
```

Farklı payloadlar denedikten sonra son olarak 0'ları kaldırıp URL'i http://127.1/ şeklinde yazdım ve paketi tekrar yolladım.

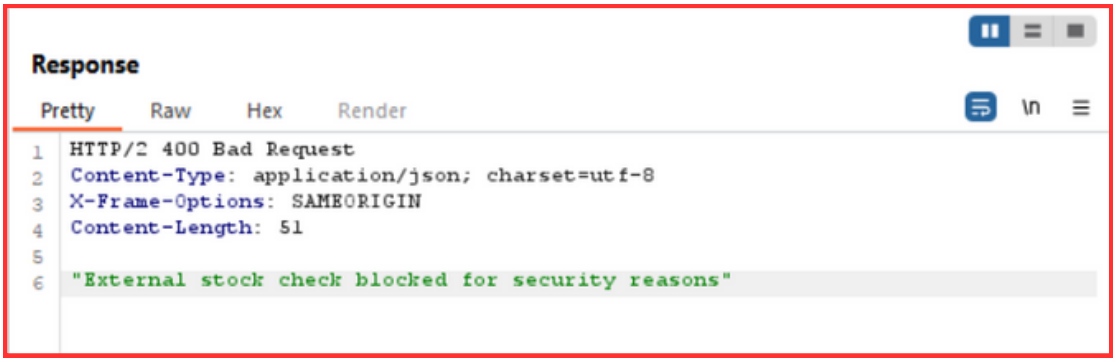
Bu sefer yanıt olarak bize sayfayı döndürdü böylecek buradaki güvenlik önlemini by-pass etmiş olduk. Yanıt olarak dönen sayfanın menüsünde Admin Panel sayfasının da eklendiğini görüyoruz.



Yanıt olarak gelen sayfaya sağ tıklayıp tarayıcıda açtım ve Admin Panel sayfasına erişmeye çalıştım. Panele erişemedik ancak URL'den /admin dizinini görmüş olduk. Kullandığımız URL'e bu dizini de ekliyorum.

```
stockApi=http://127.1/admin
```

Bulduğumuz /admin dizinini de URL'e ekledim ve paketi tekrar yolladım.



Gelen yanıta baktığımızda tekrar güvenlik engeline takıldığımızı görüyoruz. Dizin ekleyince engellendik, /admin dizinini farklı şekillerde yazarak paketi tekrar gönderelim.

```
stockApi=http://127.1/%2561dmin
```

Double URL encode yöntemiyle /admin dizini farklı şekillerde yazdığımda illegal karakter kullanımından dolayı engellendim. Daha sonra tek tek harfler için bunu uyguladım ve a harfini değiştirdiğimde siteye ulaştım. Ardından carlos kullanıcısını silerek labı tamamladım.