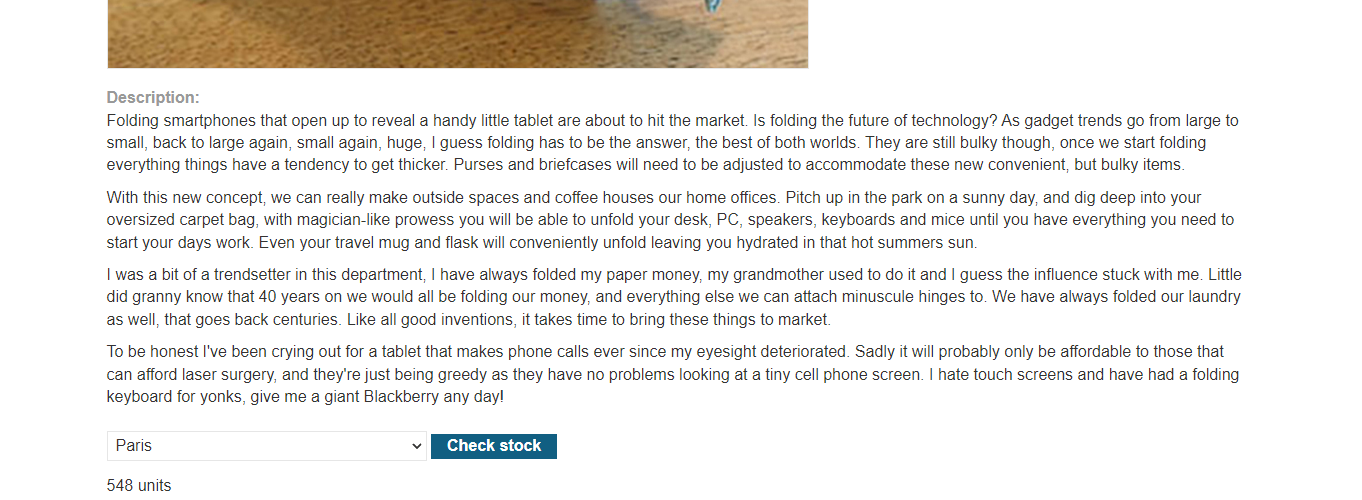
SSRF(Server Side Request Forgery)

SSRF yani sunucu taraflı istek sahteciliği, en basit tabiriyle isteklerin parametrelerini değiştirip gidiş yolunun manipüle edilmesidir.

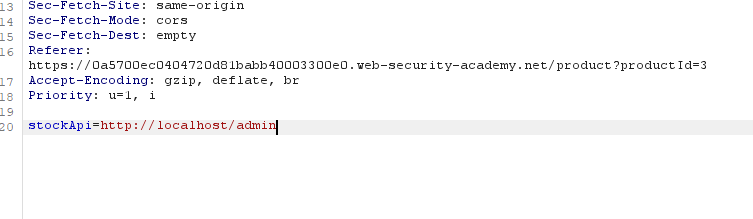
Portswigger Lab’ından bir shop uygulaması açtım. Görevim Carlos kullanıcısını silmekti. Biraz araştırdıktan sonra şöyle bir şey gördüm.

Herhangi bir ürüne gelip stok kontrolü yaptığımda burb aracımda bilgiyi API dan aldığını gördüm.



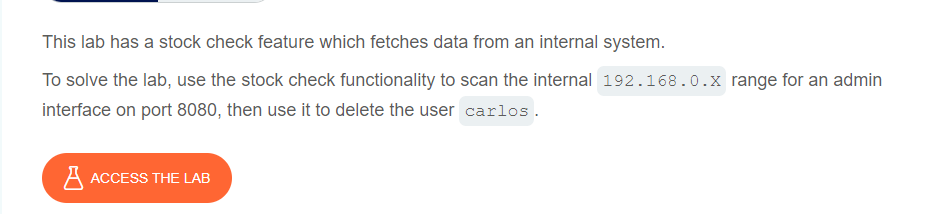


**API ı** [**http://localhost/admin**](http://localhost/admin) ile değitirdip admin paneline giriş sağlamaya çalıştım.

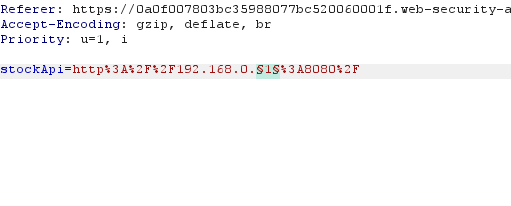


Admin paneline giriş yaptıktan sonra Carlos adlı kullanıcıyı sistemden sildim.

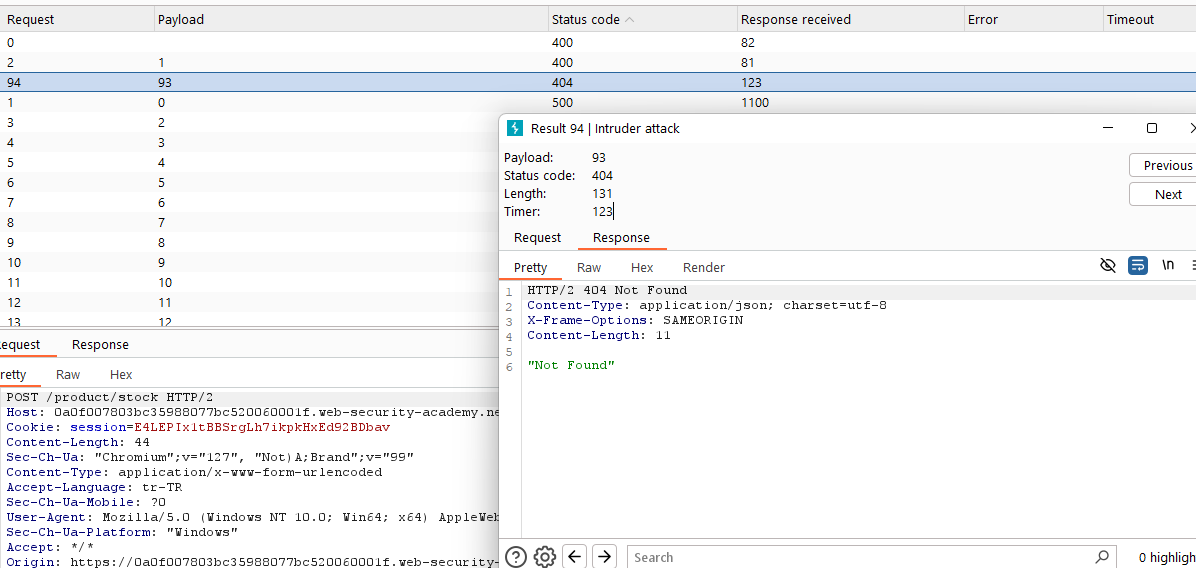
Bir diğer Lab’da ise benzer yöntemler kullanılıyordu. Yine görevim Carlos adlı kullanıcıyı sistemden silmekti. Bu sefer ise elimde bir IP adersi vardı.



192.168.0.X den anladığım intruder yapmam gerektiğiydi. Doğru aralığı bulduğunda işlem olacaktı.



İntruder 0 -255 olarak ayarlayıp atağı başlattım. IP 192.168.0.93 olduğunda length değerinde bir oynama oldu ve kontrol ettim. Muhtemelen cevaba ulaşmıştım ama response not found dönmüştü.



Buradan sonra dış kaynaklardan kopya çekmek durumunda kaldım. Normalde diğer cevaplar 500 dönerken bu sefer 404 dönmüştü. Aslında hala doğru adımdaydım. En azından bana yanıt geliyordu. Buradan sonra yapmam gereken **/admin** ekleyip sayfaya ulaşabilmekti.



Görevim olan Carlos kullanıcısını silip Lab’ı tamamlıyorum.