LAB: SSRF WITH BLACKLIST-BASED INPUT FILTER

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

GÖREV:

Blacklist tabanlı SSRF

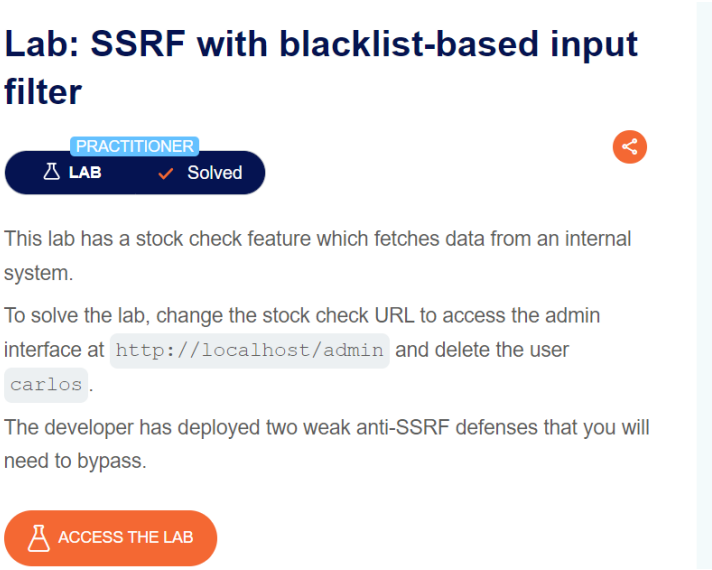
AÇIKLAMA:

Bu lab, dahili bir sistemden veri alan bir stok kontrol özelliğine sahiptir.

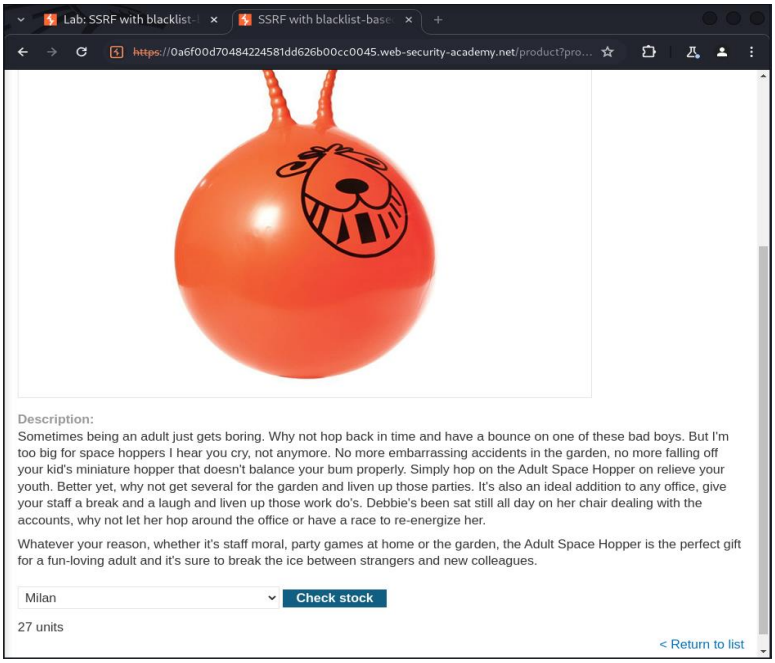
Lab'ı çözmek için, http://localhost/admin adresindeki yönetici arayüzüne erişmek için stok kontrol URL'sini değiştirin ve carlos kullanıcısını silin.

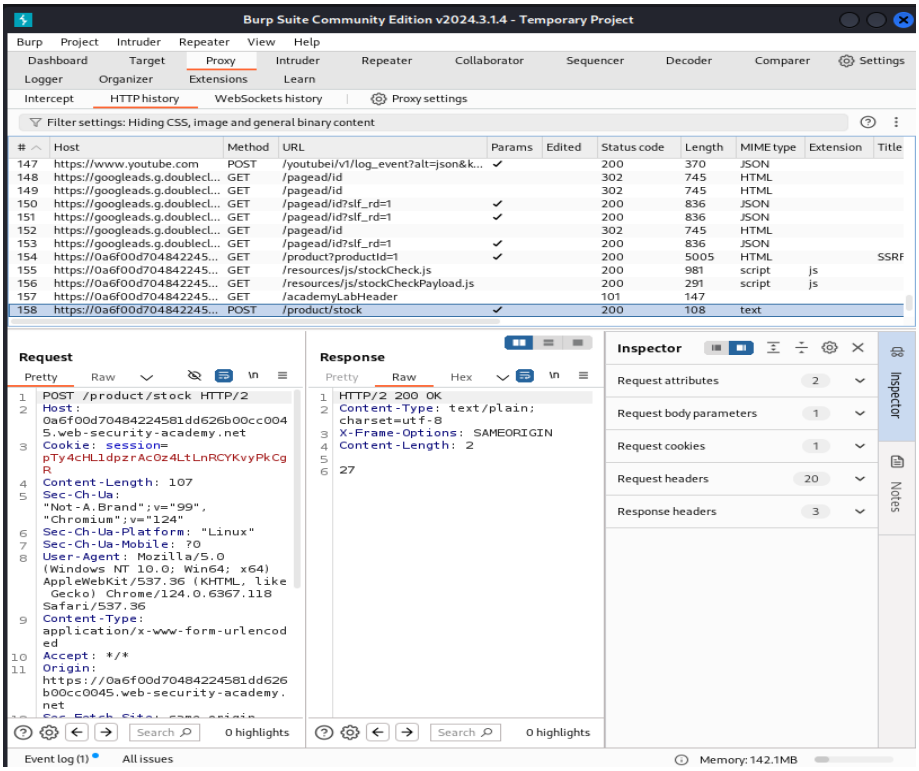
ÇÖZÜM:

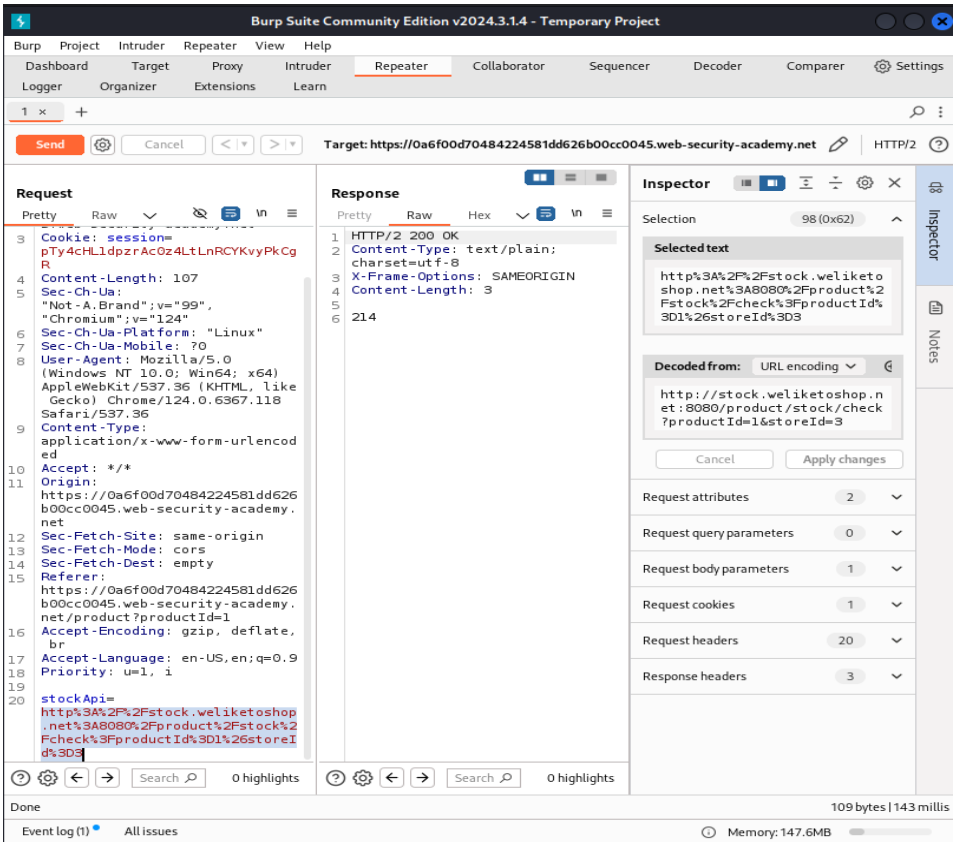
Laboratuvara erişimi başlatıyoruz.



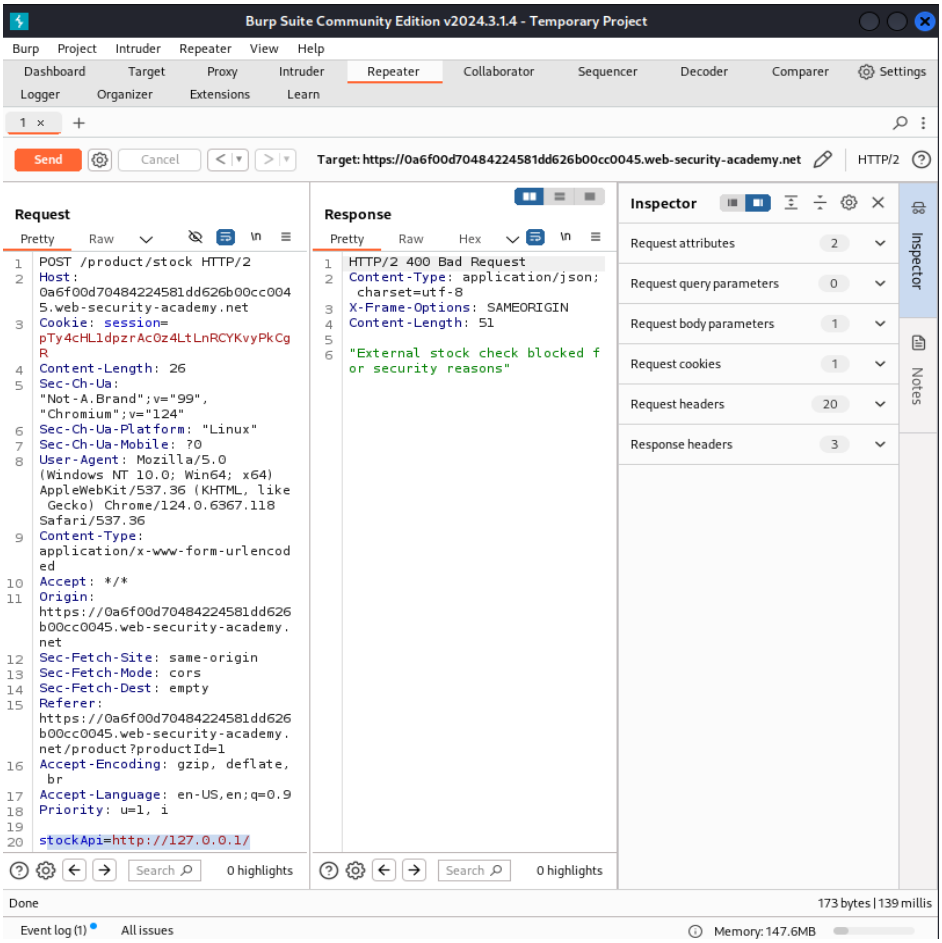
İlk adım olarak "Stok kontrolü"ne tıklayın, Burp Suite'te isteği yakalayıp Burp Intruder'a gönderilmelidir.


Lab: SSRF with blacklist-
SSRF with blacklist-base
https://0a6f00d70484224581dd626b00cc0045.web-security-academy.net/product?pro...
Description:
Sometimes being an adult just gets boring. Why not hop back in time and have a bounce on one of these bad boys. But I'm too big for space hoppers I hear you cry, not anymore. No more embarrassing accidents in the garden, no more falling off your kid's miniature hopper that doesn't balance your bum properly. Simply hop on the Adult Space Hopper on relieve your youth. Better yet, why not get several for the garden and liven up those parties. It's also an ideal addition to any office, give your staff a break and a laugh and liven up those work do's. Debbie's been sat still all day on her chair dealing with the accounts, why not let her hop around the office or have a race to re-energize her.
Whatever your reason, whether it's staff moral, party games at home or the garden, the Adult Space Hopper is the perfect gift for a fun-loving adult and it's sure to break the ice between strangers and new colleagues.
Milan
Check stock
27 units
< Return to list

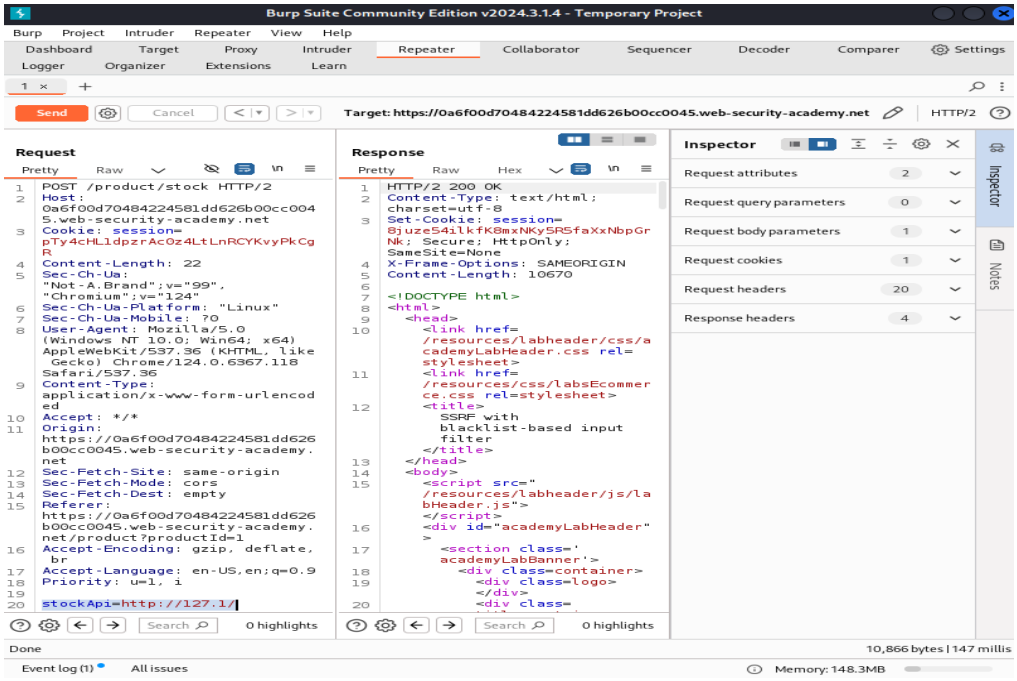

Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content
Host Method URL Params Edited Status code Length MIME type Extension Title
147 https://www.youtube.com POST /youtubei/v1/log_event?alt=json&k... 200 370 JSON
148 https://googleads.g.doublecl... GET /pagead/id 302 745 HTML
149 https://googleads.g.doublecl... GET /pagead/id 302 745 HTML
150 https://googleads.g.doublecl... GET /pagead/id?slf_rd=1 200 836 JSON
151 https://googleads.g.doublecl... GET /pagead/id?slf_rd=1 200 836 JSON
152 https://googleads.g.doublecl... GET /pagead/id 302 745 HTML
153 https://googleads.g.doublecl... GET /pagead/id?slf_rd=1 200 836 JSON
154 https://0a6f00d704842245... GET /product?productId=1 200 5005 HTML SSRF
155 https://0a6f00d704842245... GET /resources/js/stockCheck.js 200 981 script js
156 https://0a6f00d704842245... GET /resources/js/stockCheckPayload.js 200 291 script js
157 https://0a6f00d704842245... GET /academyLabHeader 101 147
158 https://0a6f00d704842245... POST /product/stock 200 108 text
Request
Pretty Raw
POST /product/stock HTTP/2
Host: 0a6f00d70484224581dd626b00cc0045.web-security-academy.net
Cookie: session=pTy4cHL1dpzrAc0z4LtLnRCYKvyPkCgR
Content-Length: 107
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Platform: "Linux"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0a6f00d70484224581dd626b00cc0045.web-security-academy.net
Search 0 highlights
Response
Pretty Raw Hex
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2
27
Search 0 highlights
Inspector
Request attributes 2
Request body parameters 1
Request cookies 1
Request headers 20
Response headers 3
Inspector
Notes
Event log (1) All issues
Memory: 142.1MB



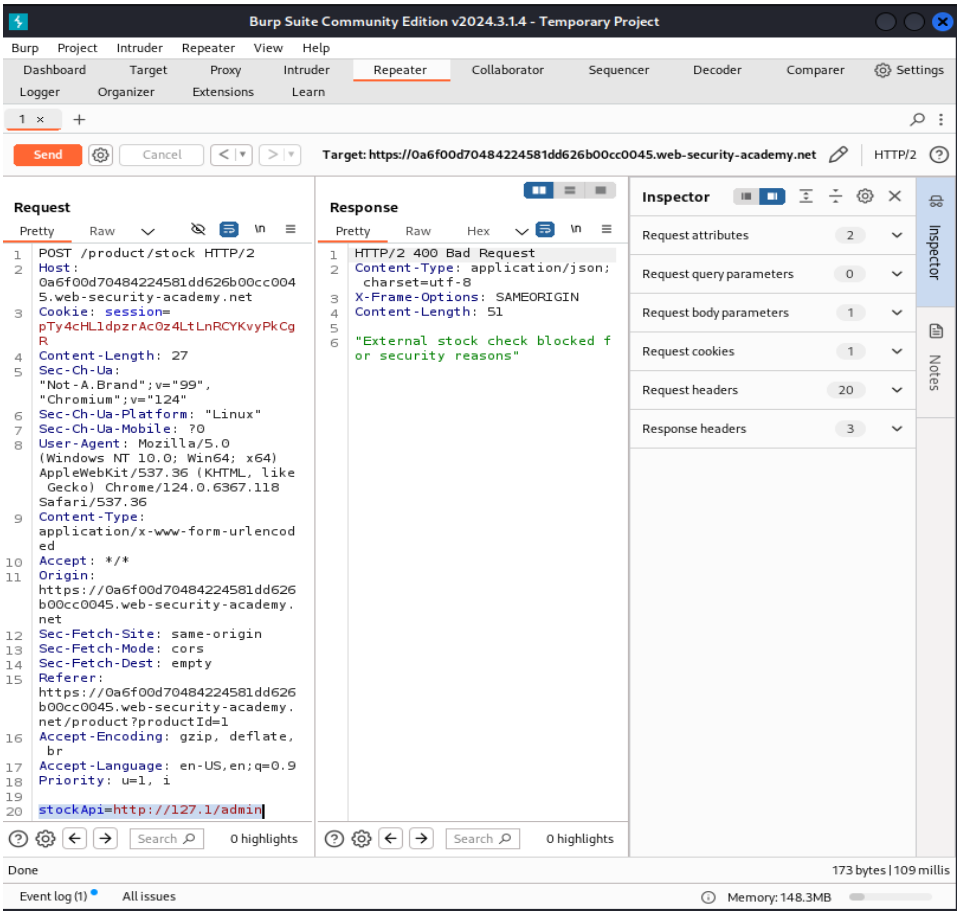
stockApi'de başarılı giriş yaptığımızı görmekteyiz. stockApi değerimizi http://127.0.0.1/ olarak değiştirip blocklanma durumuna bakacağız.



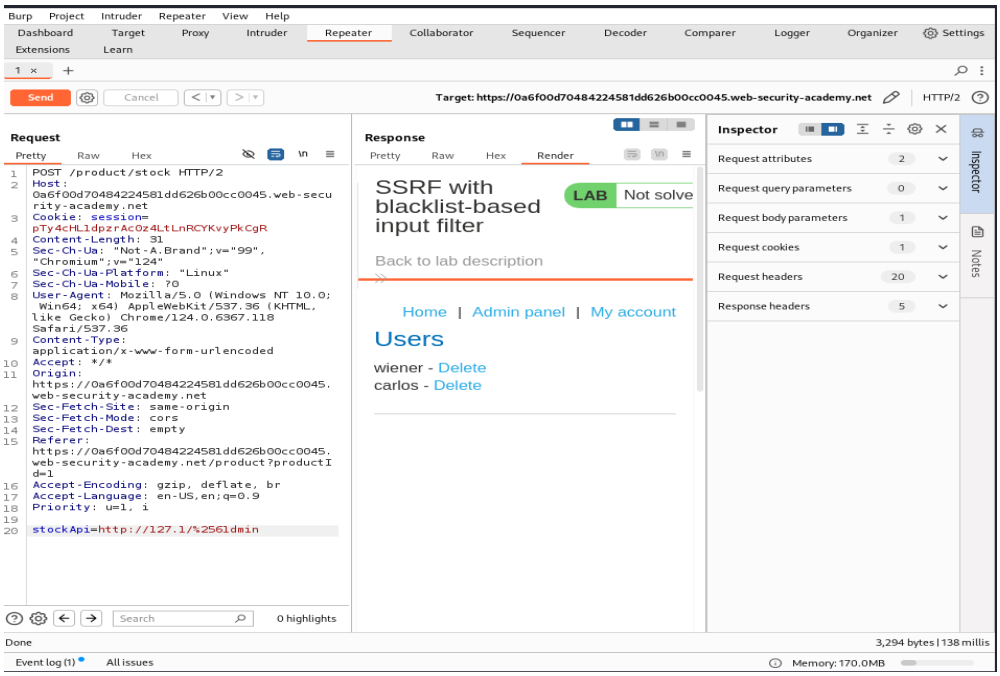
Bu adresin blocklandığını görüyoruz. URL'yi şu şekilde değiştirerek bloğu atlayacağız: http://127.1/



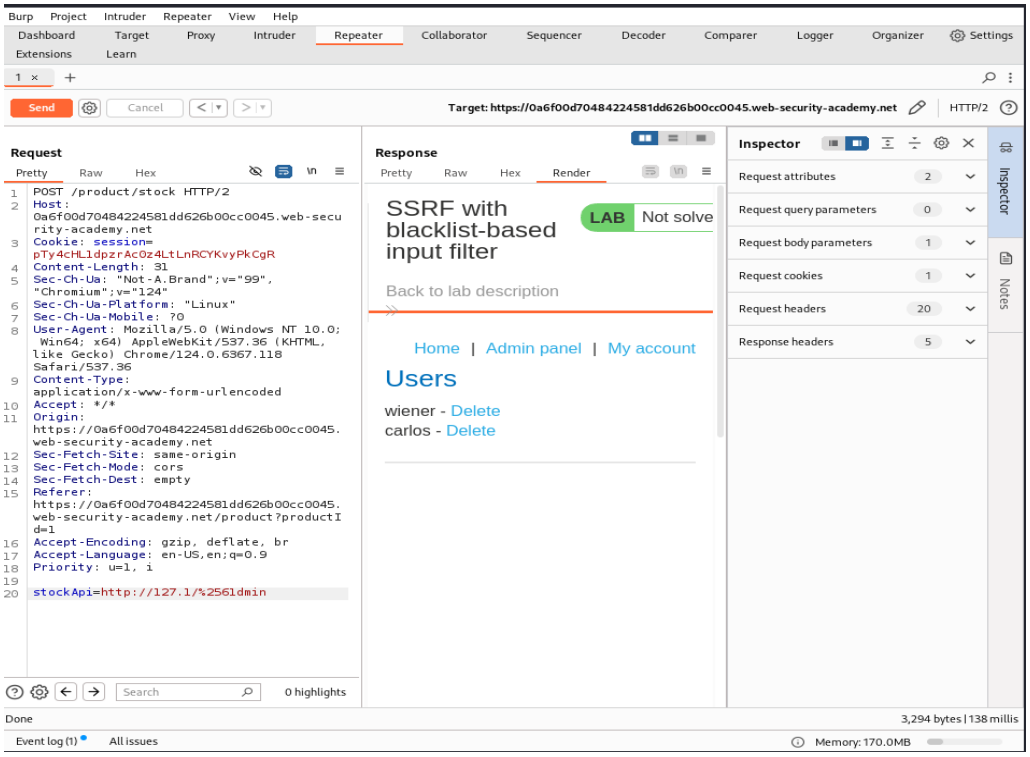
URL üzerinde işimize yarayacak değişiklikler yaparak diğer denemeleri yapıyoruz. Bu sefer de URL'yi http://127.1/admin olarak değiştirin ve URL'nin tekrar engellendiğini gözlemleyin.



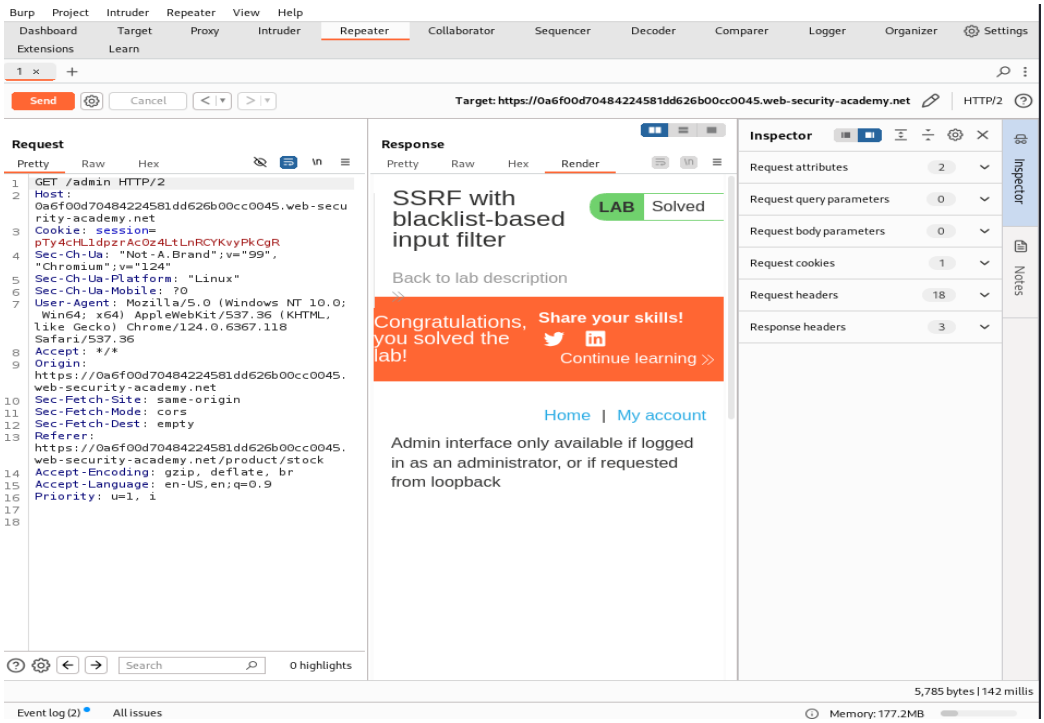
http://127.1/admin yerine http://127.1/%2561dmin yazarak admin paneline erişimi sağlıyoruz



Bizden istenen carlos kullanıcısını silmemizdi ona uygun işlemleri yapmaya devam ediyoruz. Carlos kullanıcısını sileceğimiz panel karşımıza gelmektedir.



stockApi'yi http://127.1/%2561dmin/delete?username=carlos yazarak kullanıcımızı siliyoruz.



Laboratuvarımızı tamamladık.

Şeyma Saylan