DATA WAREHOUSE

A01 – Broken Access Control

OLEH :

Nadya Indah Trisnawati (3122640034)

Mochammad Jauhar Ulul Albab (3122640044)

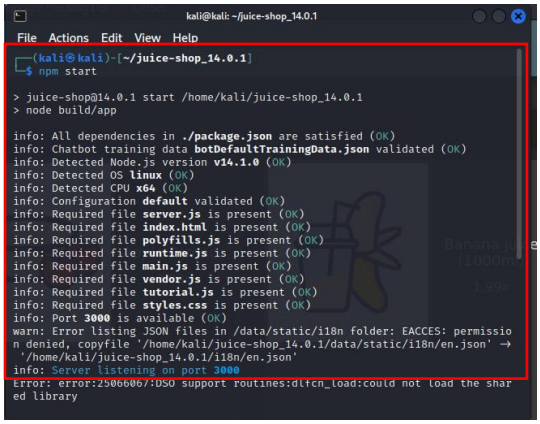
PROGRAM STUDI TEKNIK INFORMATIKA

DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER

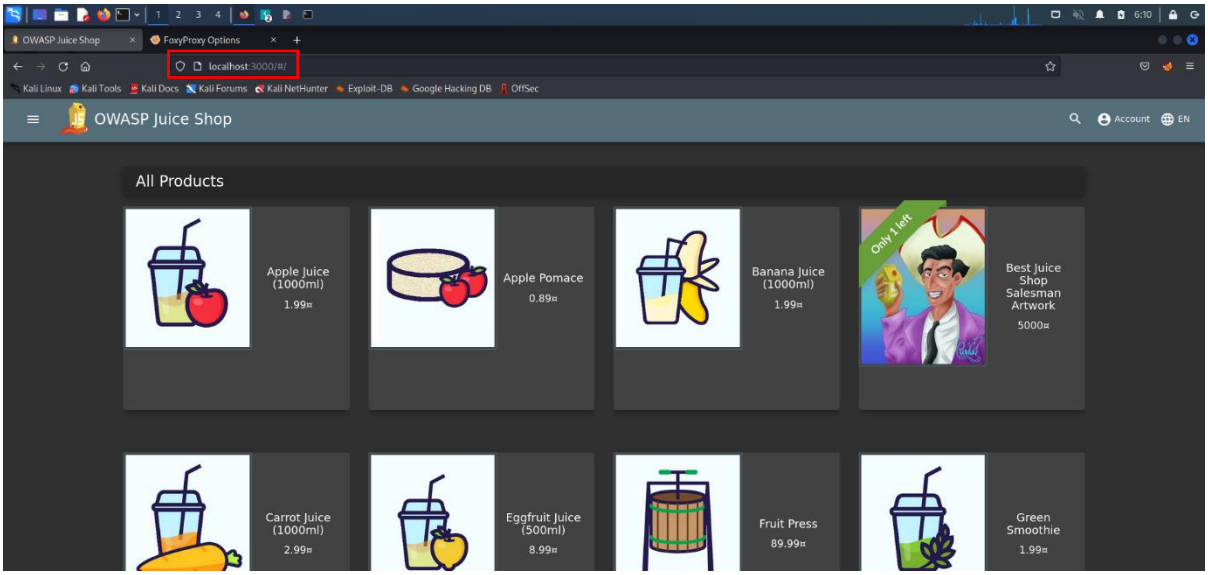
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

2022/2023

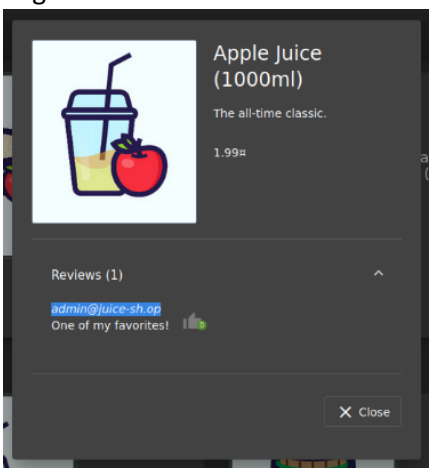
1. Start juiceshop dengan menggunakan npm



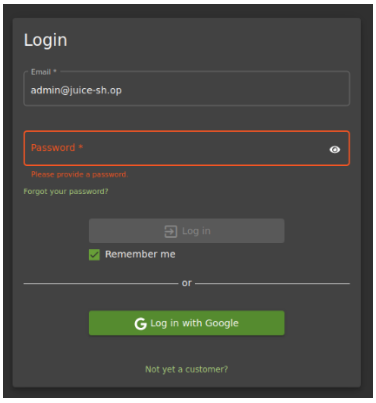
2. Masukkan localhost dan juga port dari hasil npm



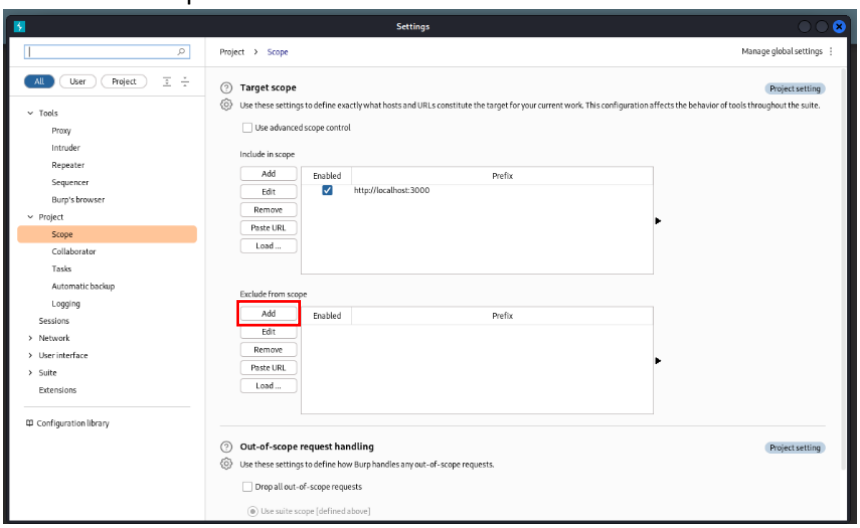
3. Pilih salah satu menu, disini saya mimilih apple juice dan copy kan email yang ada pada bagian reviews



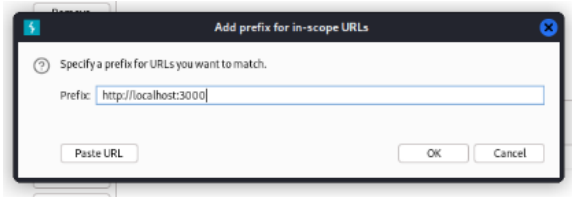
4. Coba lakukan login menggunakan email yang sudah dicopy kan sebelumnya



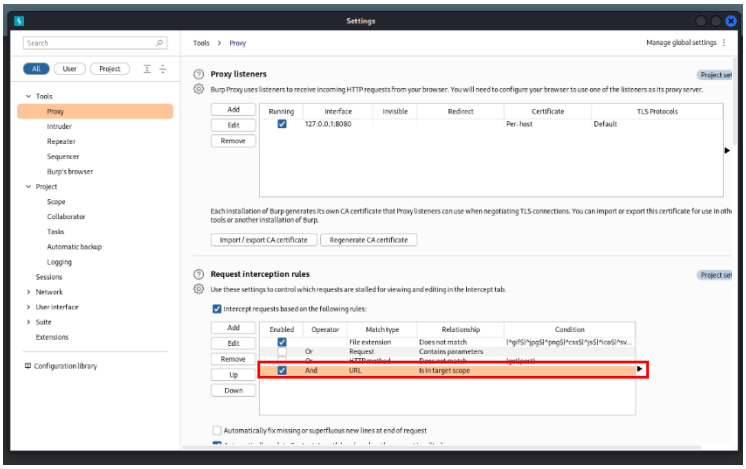
5. Buka dan jalankan burpsuite, lalu masuk kedalam setting.
   Tambahkan scope baru



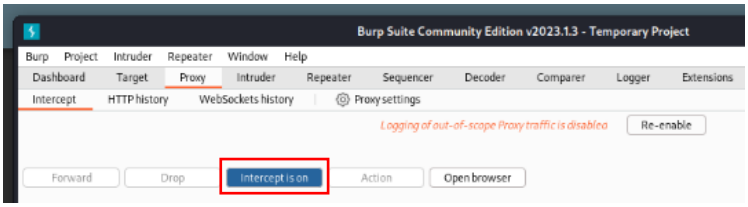
6. Masukkan url dari juiceshop



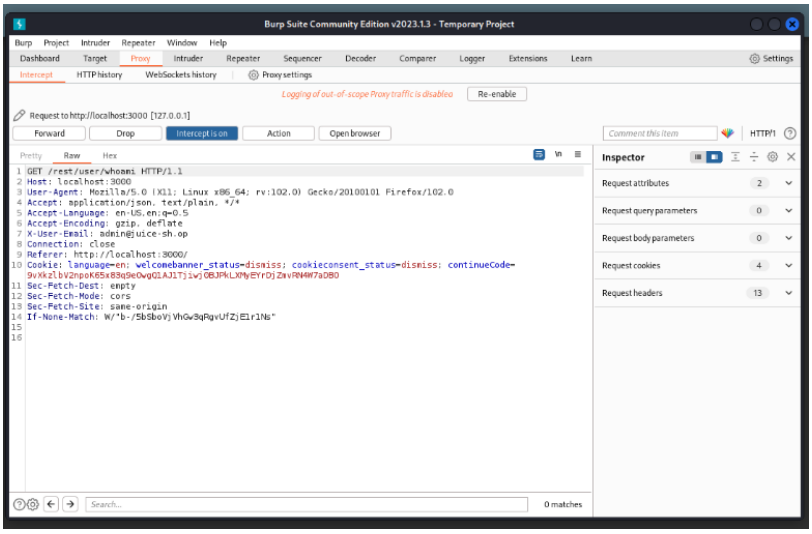
7. Centang pada bagian And



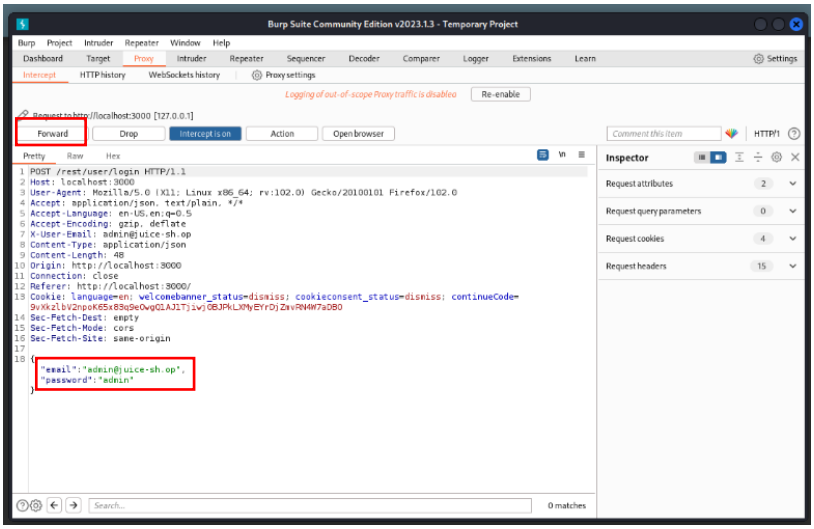
8. Masuk ke bagian proxy dan nyalakan intercept



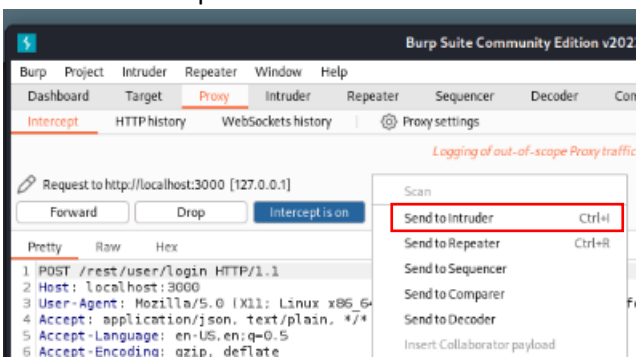
9. Lakukan login ulang menggunakan password random dengan email yang sudah dicopy kan sebelumnya pada juiceshop maka akan tampil seperti berikut pada interceot



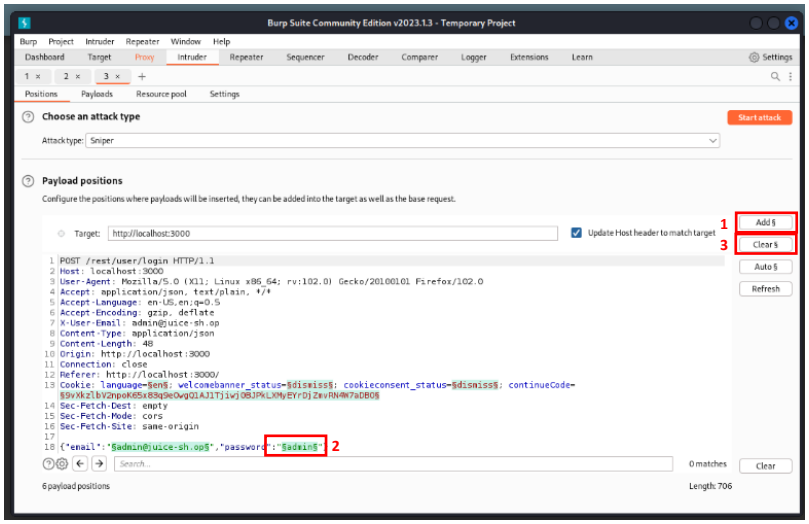
10. Lakukan forward hingga muncul hasil post dari login yang terah dilakukan



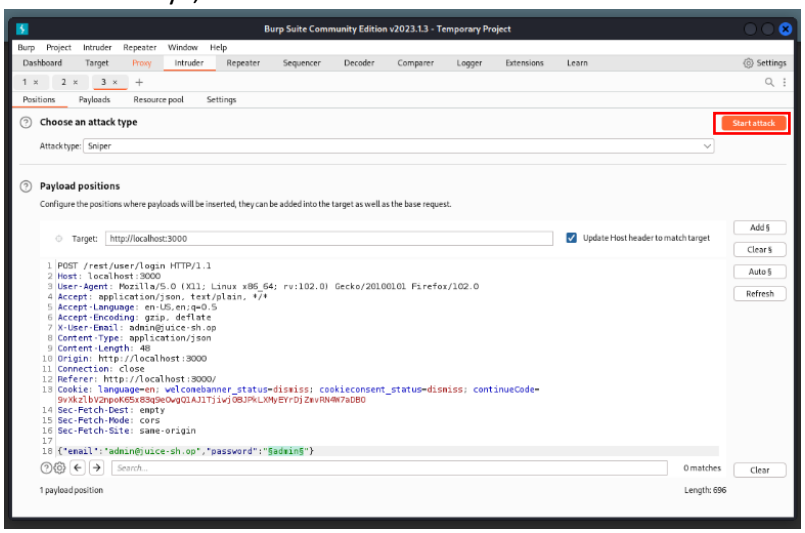
11. Kirimkan intercept ke intruder



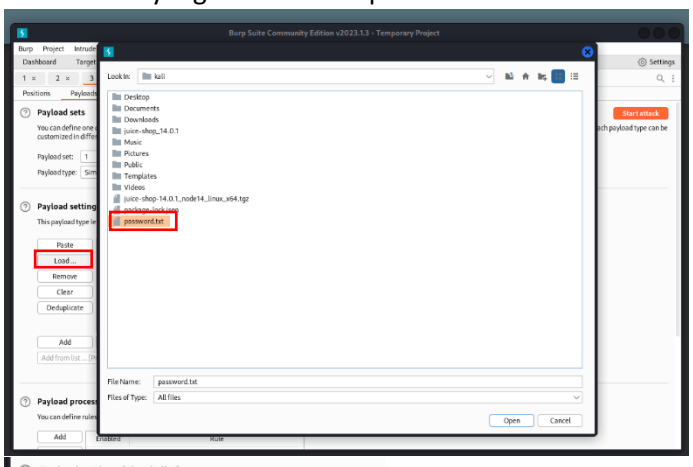
12. Lakukan clear, dan add pada bagian password

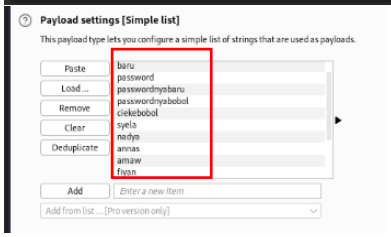


Berikut hasilnya, lalu lakukan start attack

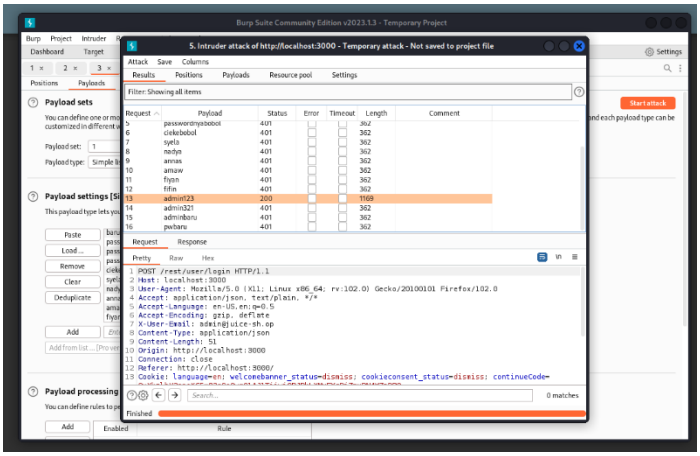


13. Load file txt yang berisikan list password untuk melakukan bruteforce

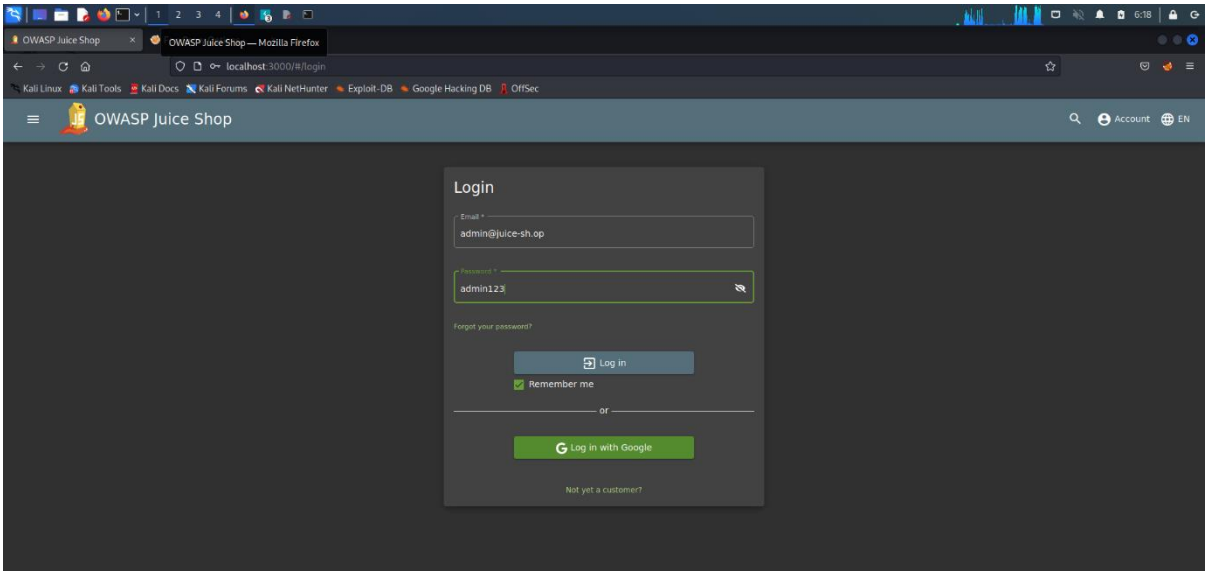




14. Tunggu process attack lalu cari password yang memiliki status 200



15. Masukkan password kedalam login juiceshop



Berikut hasilnya :