

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

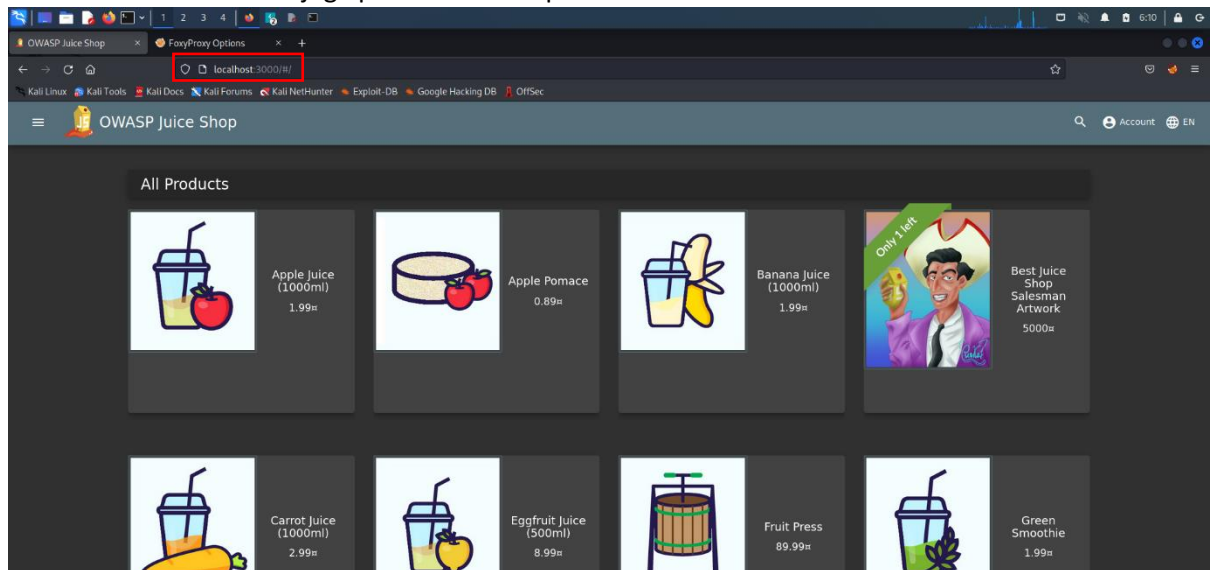
2022/2023

1. Start juiceshop dengan menggunakan npm

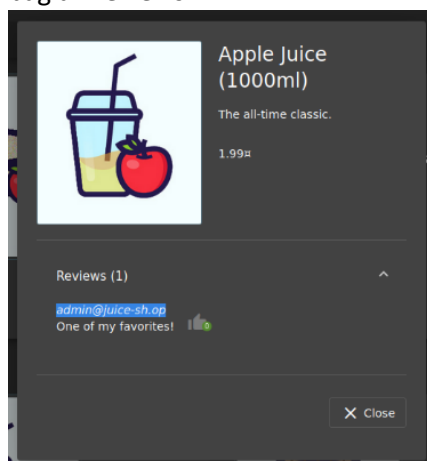
```
kali@kali: ~/juice-shop_14.0.1
File Actions Edit View Help
(kali@kali)~[/juice-shop_14.0.1]
$ npm start
> juice-shop@14.0.1 start /home/kali/juice-shop_14.0.1
> node build/app

info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v14.1.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file main.js is present (OK)
info: Required file vendor.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file styles.css is present (OK)
info: Port 3000 is available (OK)
warn: Error listing JSON files in /data/static/i18n folder: EACCES: permission denied, copyfile '/home/kali/juice-shop_14.0.1/data/static/i18n/en.json' -> '/home/kali/juice-shop_14.0.1/i18n/en.json'
info: Server listening on port 3000
error: error:25060067:libcrypto support routines:d1cfn_load:could not load the shared library
```

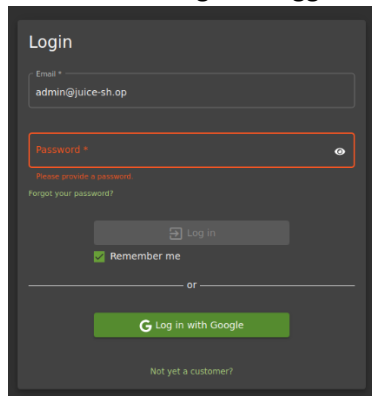
2. Masukkan localhost dan juga port dari hasil npm



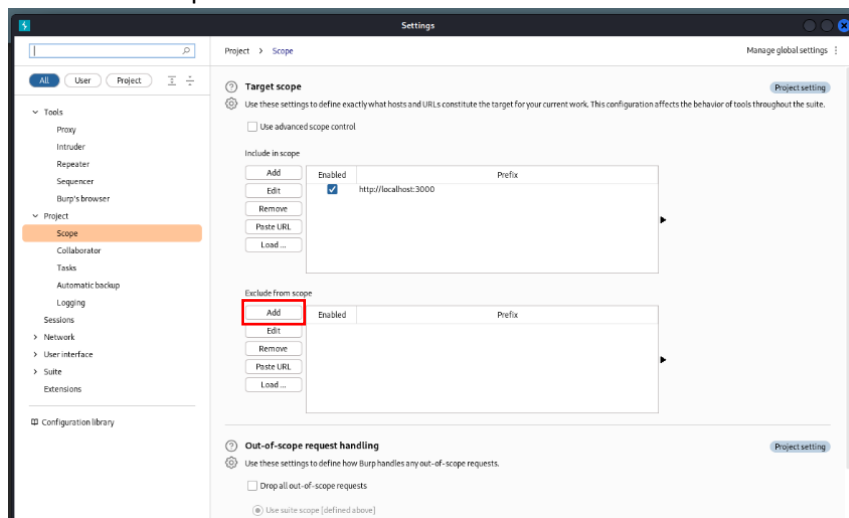
3. Pilih salah satu menu, disini saya memilih apple juice dan copy kan email yang ada pada bagian reviews



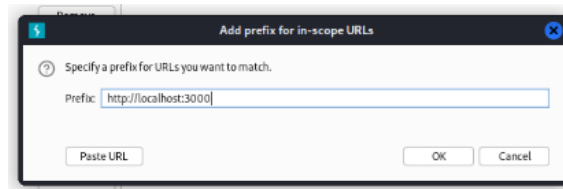
4. Coba lakukan login menggunakan email yang sudah dicopy kan sebelumnya



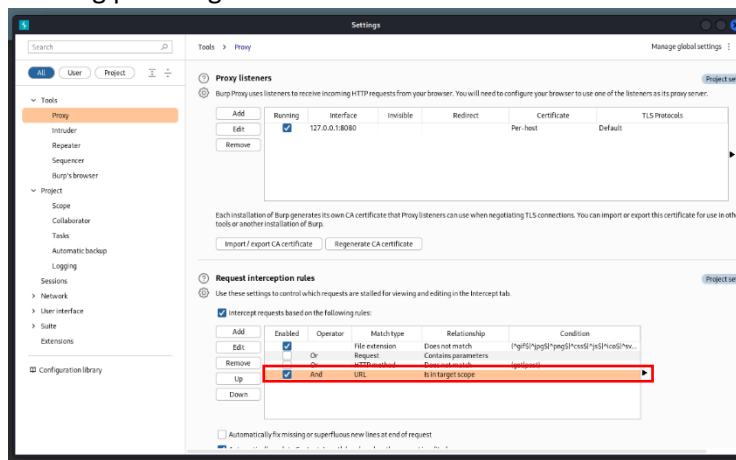
5. Buka dan jalankan burpsuite, lalu masuk kedalam setting. Tambahkan scope baru



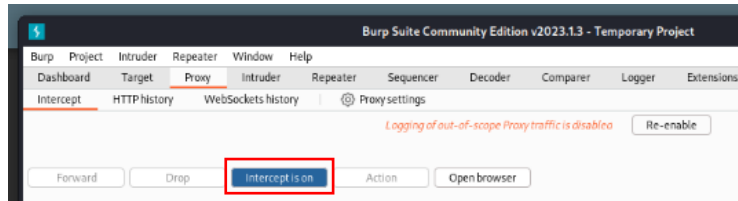
6. Masukkan url dari juiceshop



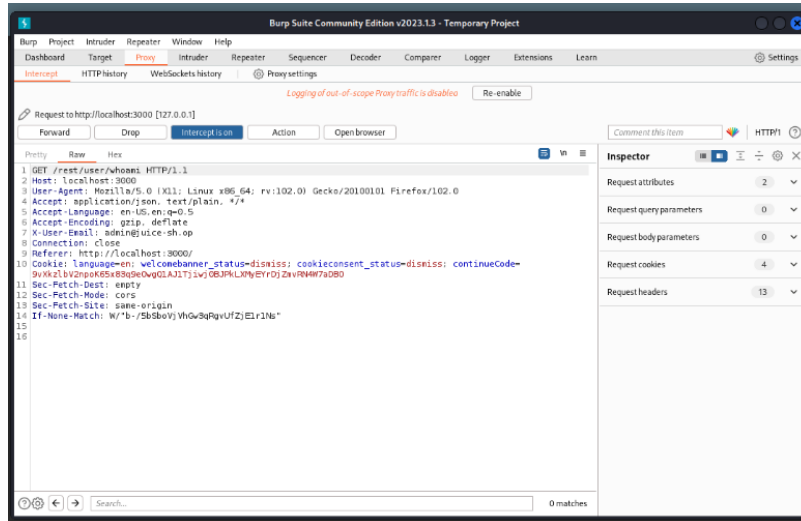
7. Centang pada bagian And



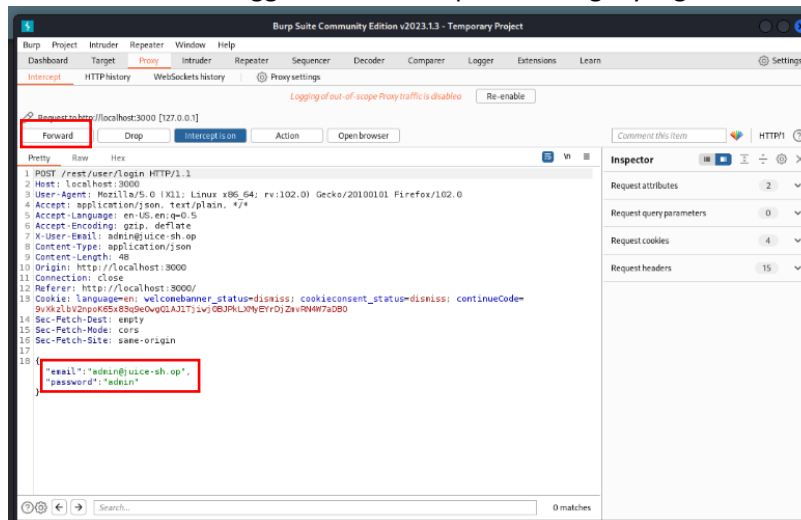
8. Masuk ke bagian proxy dan nyalakan intercept



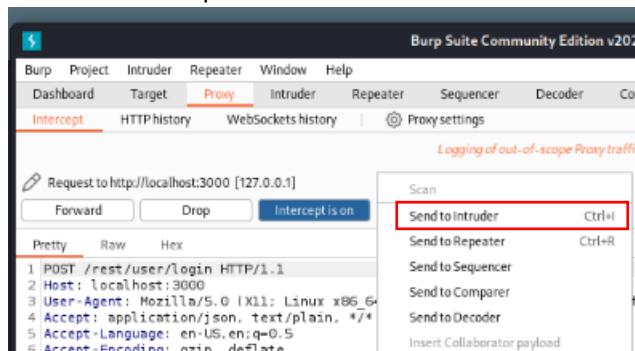
9. Lakukan login ulang menggunakan password random dengan email yang sudah dicopy kan sebelumnya pada juiceshop maka akan tampil seperti berikut pada intercept



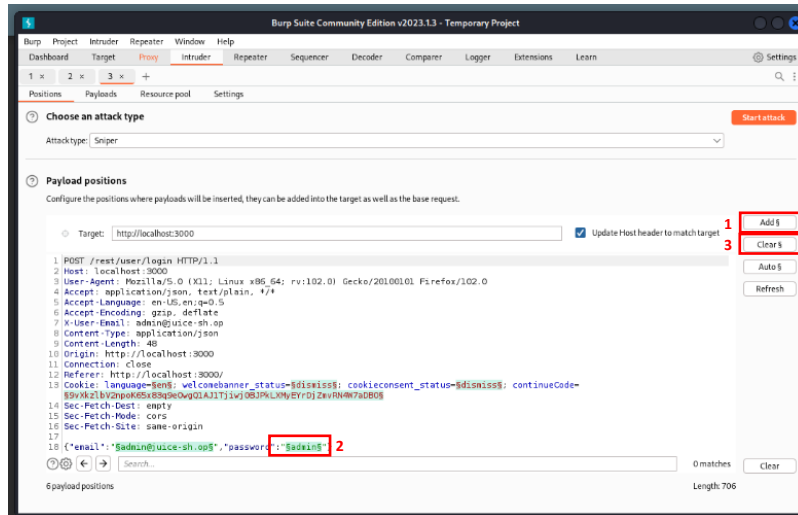
10. Lakukan forward hingga muncul hasil post dari login yang telah dilakukan



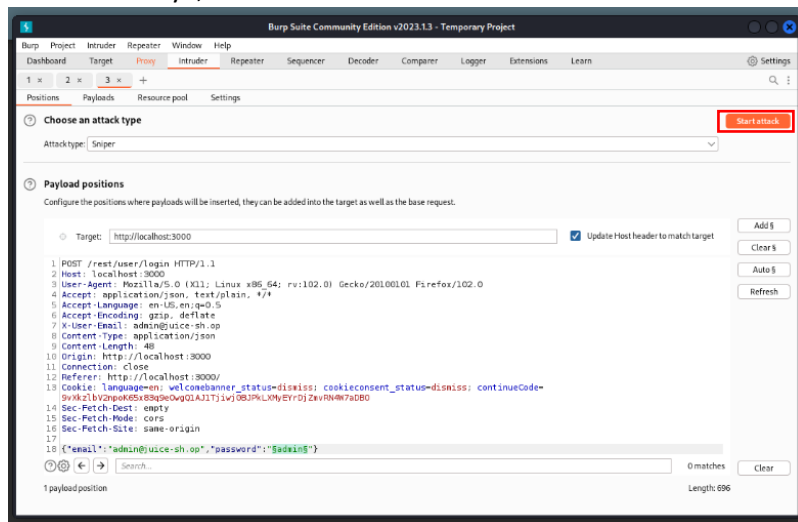
11. Kirimkan intercept ke intruder



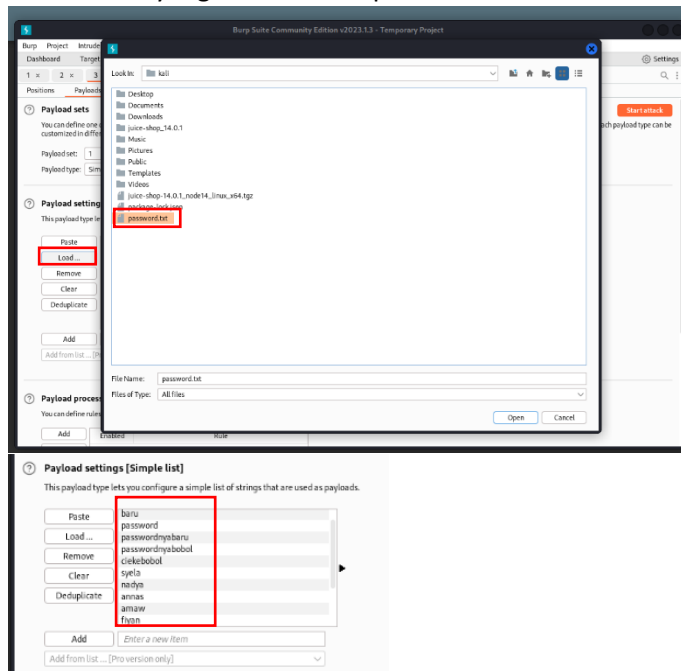
12. Lakukan clear, dan add pada bagian password



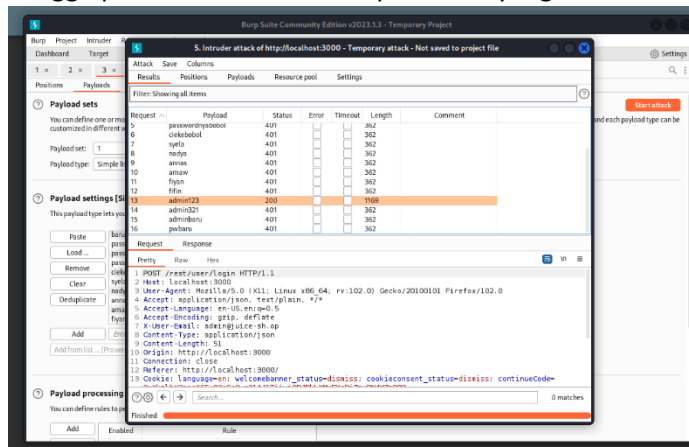
Berikut hasilnya, lalu lakukan start attack



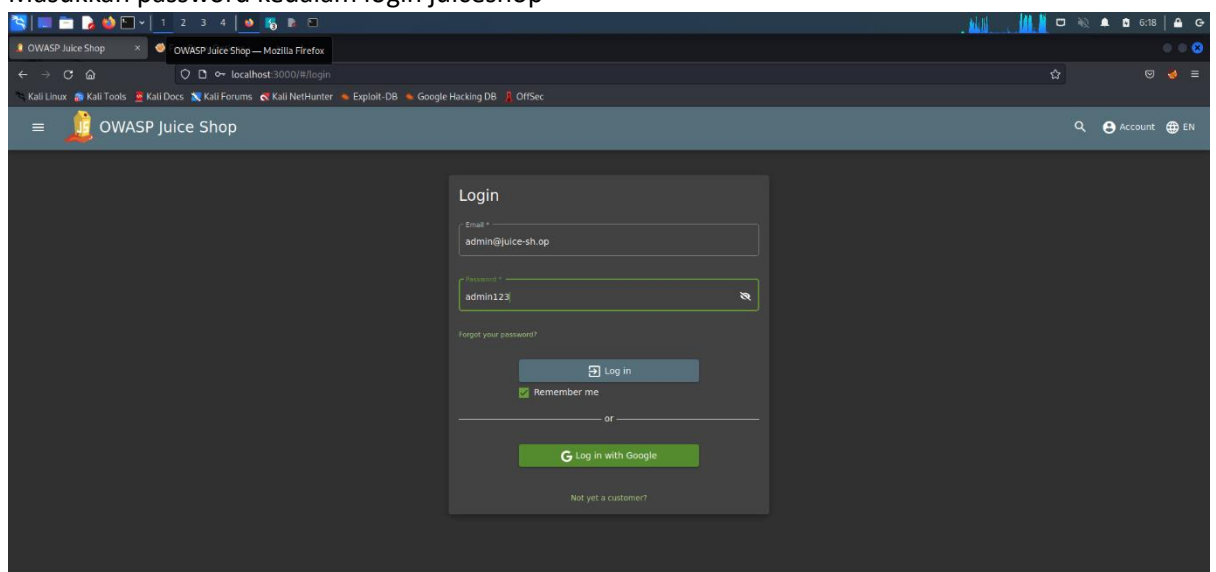
13. Load file txt yang berisikan list password untuk melakukan bruteforce



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



15. Masukkan password kedalam login juiceshop



Berikut hasilnya :

