LAPORAN RESMI
PRAKTIKUM KEAMANAN JARINGAN
A01 – BROKEN ACCESS CONTROL

Oleh :

Tarisa Dinda Deliyanti 3122640037

Fisabili Maghfirona Firdaus 3122640051

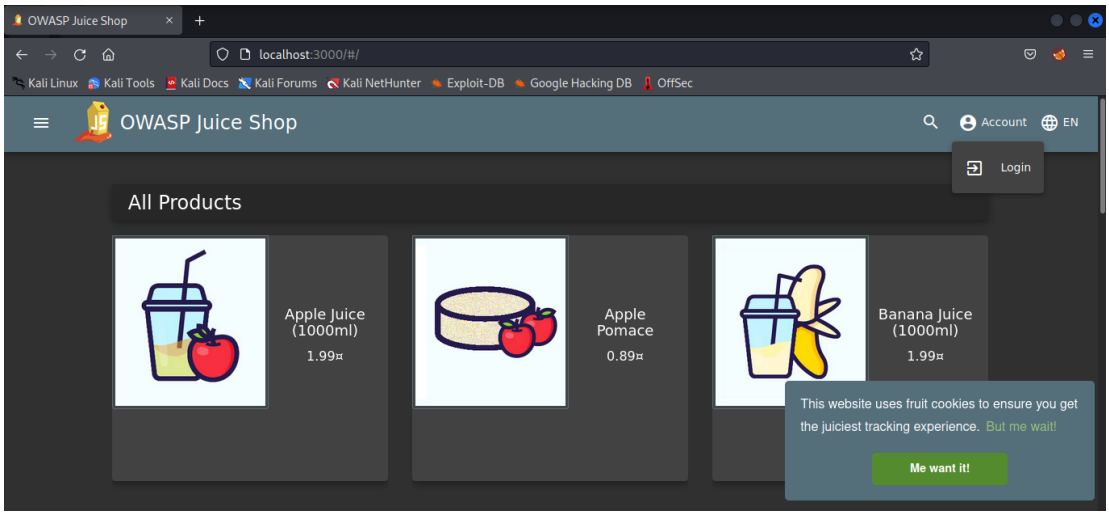
D4 LJ Teknik Informatika B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
TAHUN AJARAN 2022/2023

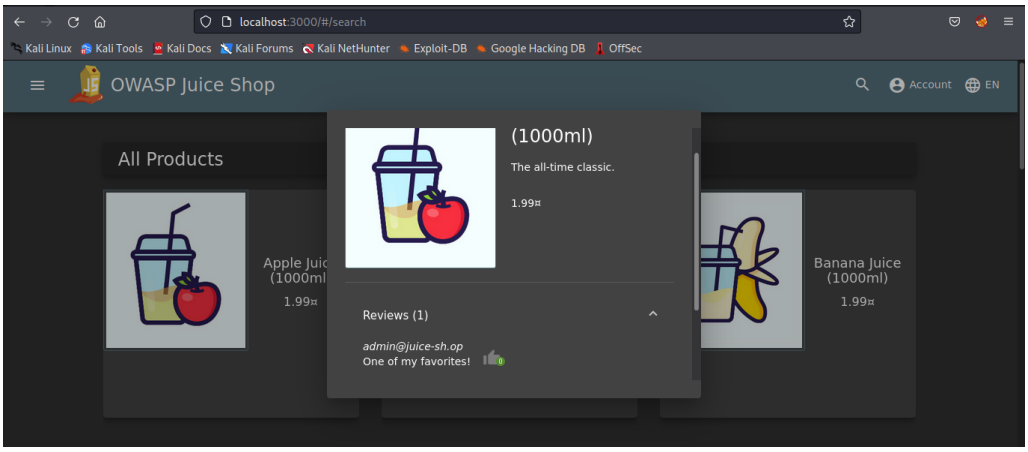
1. Menjalankan website Juice Shop menggunakan perintah “npm start” di dalam folder Juice Shop. Setelah port tersedia, kemudian membuka localhost:3000

```
┌──(kali㉿kali)-[~]
└─$ cd juice-shop_14.0.1

┌──(kali㉿kali)-[~/juice-shop_14.0.1]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/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 main.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Server listening on port 3000
```

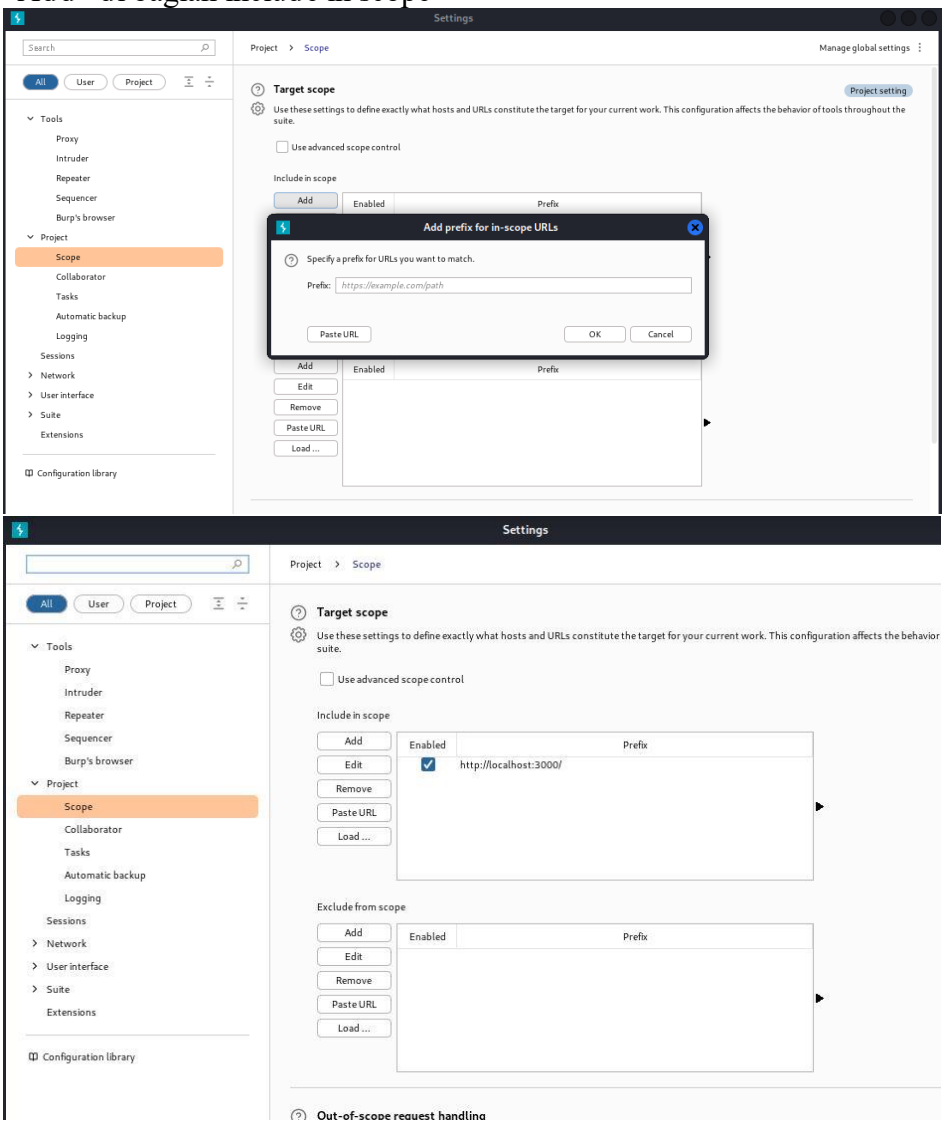
2. Berikut tampilan website yang ditampilkan di port 3000



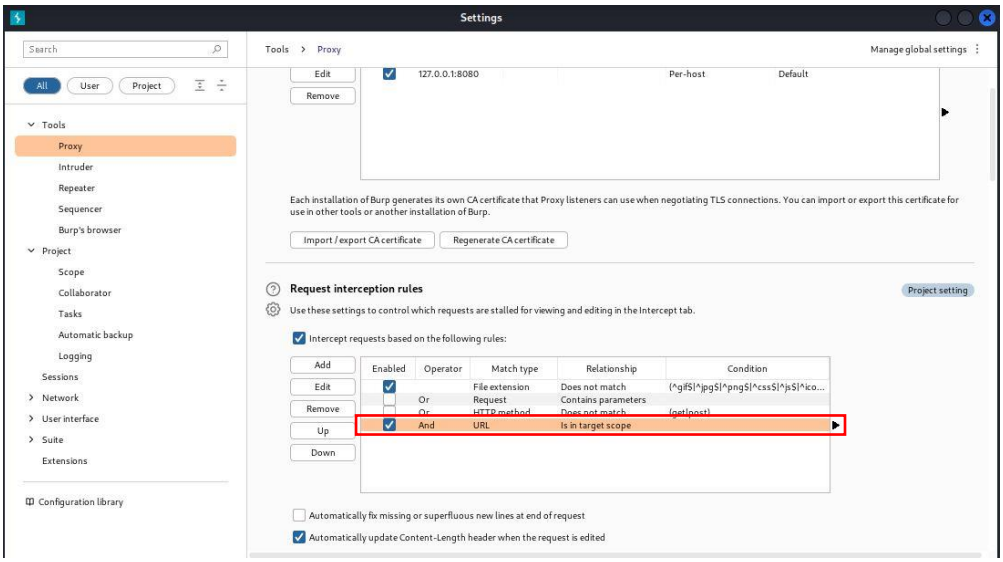
3. Mencari alamat email admin melalui review yang ada di produk Apple Juice. Alamat email admin digunakan untuk mengecek broken access control. Dari gambar di bawah ini, didapatkan informasi bahwa email admin yaitu admin@juice-sh.op



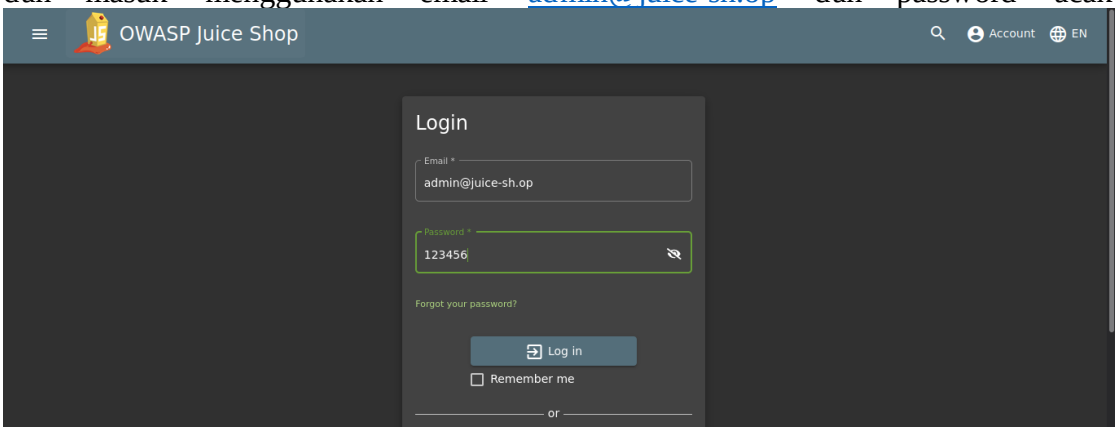
4. Menjalankan aplikasi burpsuite. Kemudian buka Proxy lalu pilih Proxy Setting lalu pilih Project dan pilih Scope. Setelah muncul tampilan seperti berikut, tambahkan prefix alamat website yang akan dibuka yaitu localhost:3000 dengan mengklik tombol "Add" di bagian include in scope



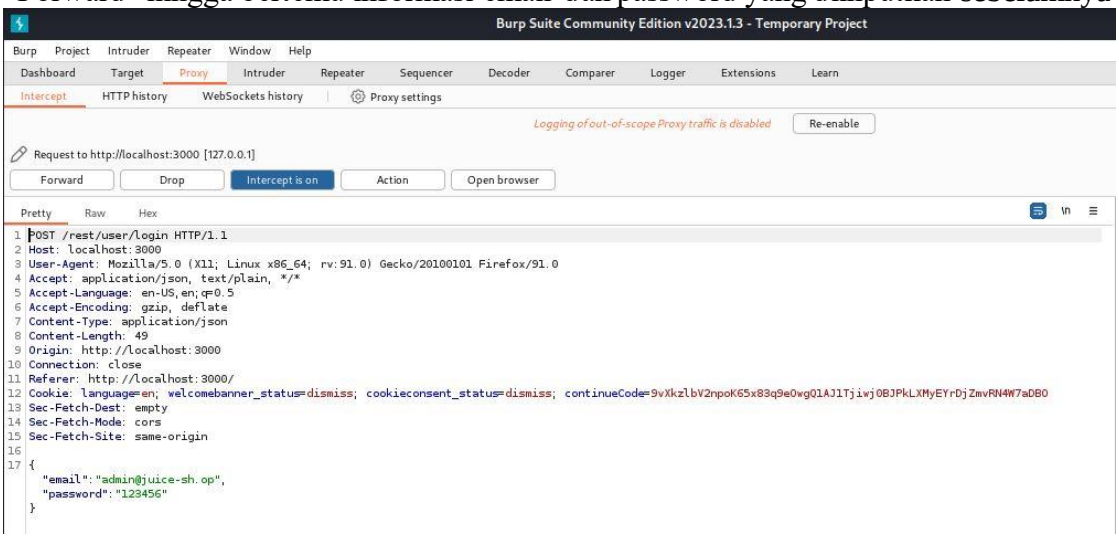
5. Klik Tools, pilih Proxy, dan centang bagian yang diberi kotak berwarna merah seperti pada gambar berikut



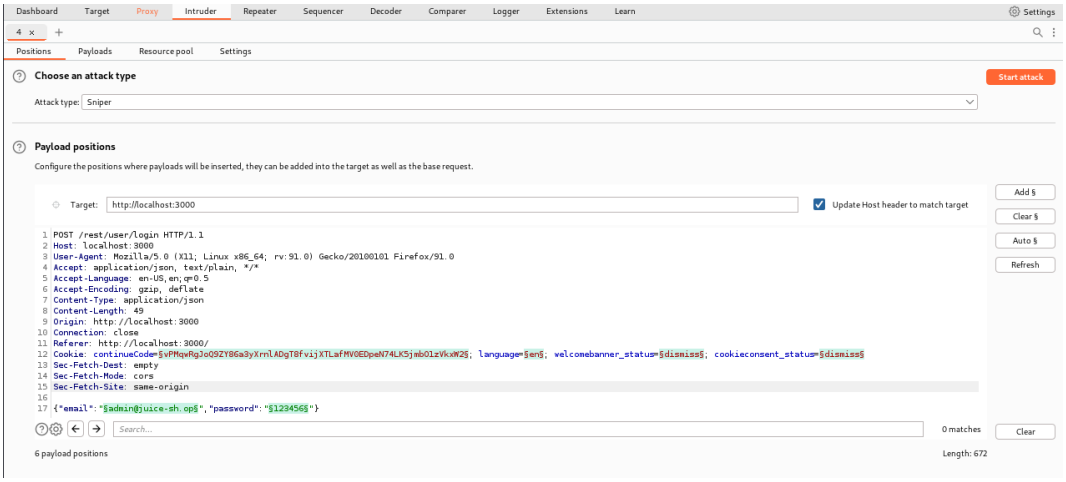
6. Mengubah intercept dari off ke on. Setelah itu, kembali ke halaman login Juice Shop dan masuk menggunakan email admin@juice-sh.op dan password acak



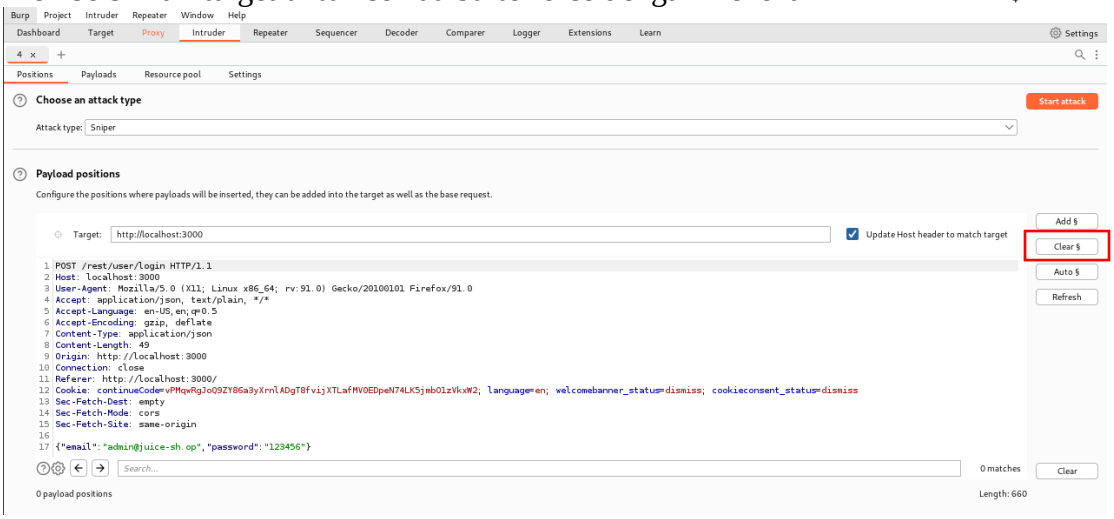
Setelah klik tombol Login, kembali ke burpsuite dan di halaman Intercept klik "Forward" hingga bertemu informasi email dan password yang diinputkan sebelumnya



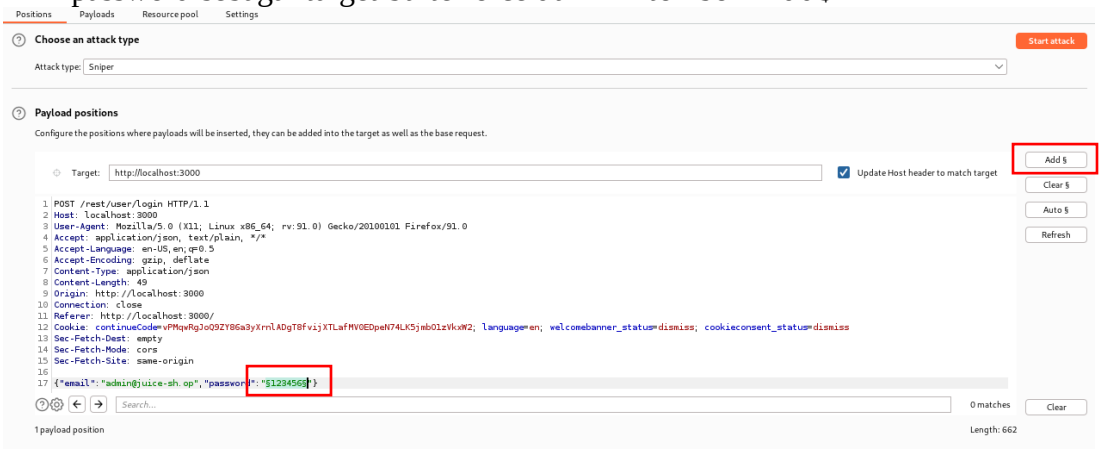
7. Klik kanan lalu pilih "Send to intruder" dan klik menu Intruder hingga muncul tampilan seperti gambar berikut



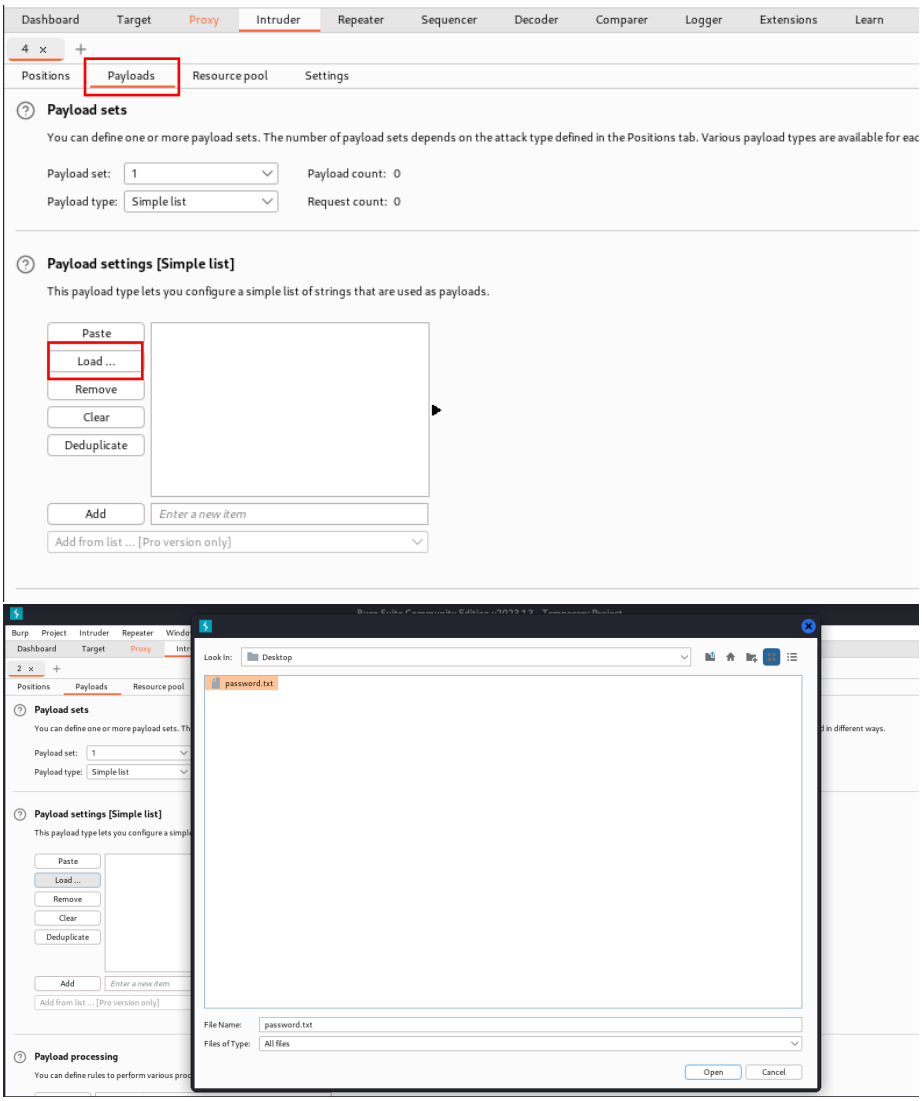
8. Membersihkan target untuk semua burte force dengan menekan tombol “Clear$”



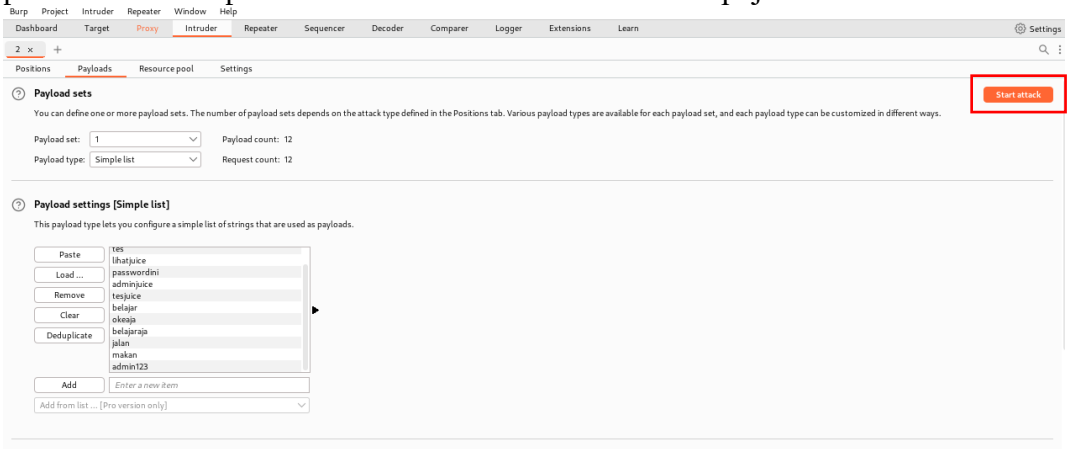
9. Pilih password sebagai target burte force dan klik tombol "Add$"



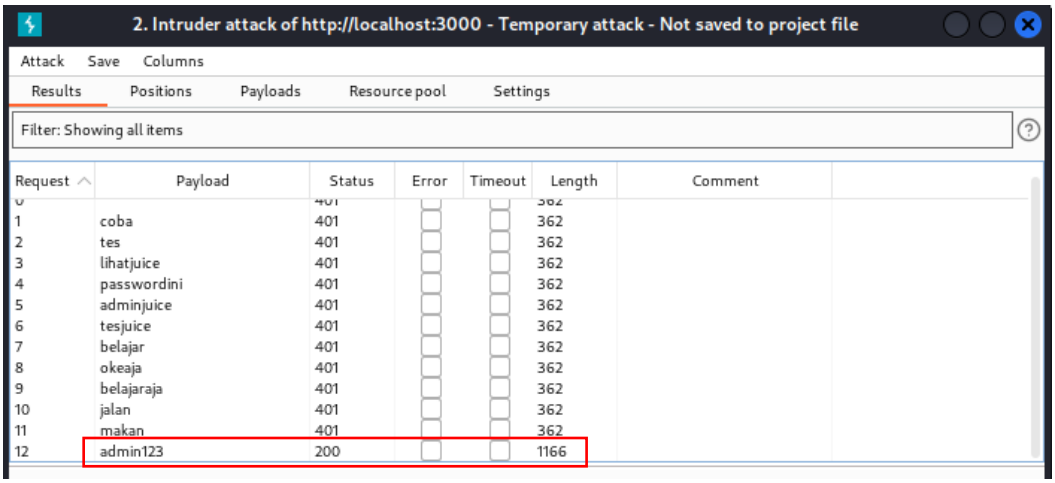
10. Klik menu Payload di Intruder dan pilih file berformat .txt setelah klik tombol “Load”



11. Setelah file password.txt berhasil diload akan muncul tampilan yang berisi daftar password acak seperti berikut dan klik “Start attack” di pojok kanan



12. Berikut hasil setelah menekan tombol “Start attack”



Terdapat dua macam HTTP status yaitu 401 yang berarti permintaan browser ke server tidak memiliki kredensial autentik yang valid dan 200 yang berarti server berhasil menerima request dari browser yang kita gunakan.

13. Login menggunakan password dengan status 200 untuk masuk ke akun admin