

# **Praktikum Keamanan Jaringan**

## **OWASP Juice Shop – Broken Access Control**



Oleh:

Aldo Faiz Winarno (3122640039)

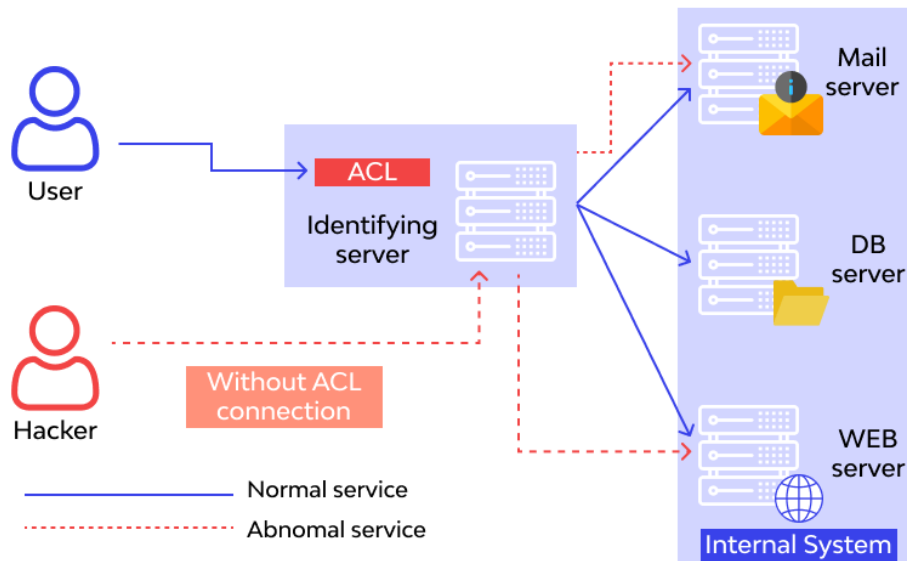
D4 LJ IT B

**POLITEKNIK ELEKTRONIKA NEGERI SURABAYA**

**TAHUN 2023**

# Broken Access Control

Sumber : [https://owasp.org/Top10/id/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/id/A01_2021-Broken_Access_Control/)



## Deskripsi

Akses Kontrol menetapkan sebuah peraturan yang dimana user tidak dapat melakukan sebuah aksi diluar permission yang diberikan. Kegagalan atas hal ini dapat mengakibatkan pengeluaran informasi yang tidak diizinkan, modifikasi, atau penghancuran dari semua data atau pemberlakuan sebuah fungsi bisnis di luar limit sebuah user. Kelemahan Akses Kontrol termasuk dari :

Melewati pengecekan akses kontrol dengan memodifikasi URL, internal application state, atau HTML page, atau menggunakan custom API attack tool.

Membolehkan primary key untuk dapat diganti ke record user lain, membolehkan penglihatan atau perubahan akun orang lain.

Penaikan sebuah privilege (Elevation Privilege). Yang dimana sebuah orang dapat dianggap sebagai user tanpa melakukan logged in dan yang dimana sebuah user dapat dianggap sebagai admin tanpa melakukan logged in.

Manipulasi metadata, seperti memanipulasi dengan JSON Web Token (JWT) akses kontrol token, atau memanipulasi cookie atau hidden field untuk menaikan privilege (elevation privilege) atau menyalahgunakan penggunaan dari JWT invalidation.

Konfigurasi yang salah pada CORS sehingga menyebabkan API akses yang tidak diizinkan.

Force browsing untuk mengakses authenticated pages sebagai unauthenticated user atau mengakses privileged pages sebagai user standard. Mengakses API yang tidak memiliki akses kontrol untuk POST, PUT, dan DELETE.

## Cara Mencegah

Akses Kontrol hanya efektif pada kode server-side yang dapat dipercaya dan server-less API, yang dimana penyerang tidak dapat memodifikasi pengecek akses kontrol atau meta datanya.

Menolak semua akses kecuali ke public resource.

Melakukan implementasi mekanisme akses kontrol sekali dan digunakan kembali pada seluruh aplikasi sehingga meminimalisir penggunaan CORS.

Agar user tidak dapat melakukan create, read, update, atau mendelete record secara bebas, model akses kontrol seharusnya membatasi hal tersebut dengan menggunakan ownership untuk tiap record.

Batas yang diperlukan oleh bisnis yang unik pada aplikasi seharusnya dilakukan oleh domain models.

Nonaktifkan direktori listing web server dan pastikan file metadata (contohnya .git) dan file backup tidak ada di dalam web roots.

Catat kegagalan akses kontrol dan alert admin jika diperlukan (seperti adanya kegagalan yang terjadi berulang - ulang).

Ukur batasan dari API dan akses ke kontroler untuk meminimalisir kerusakan dari automated attack tooling.

JWT tokens harus langsung di hilangkan validasinya pada server setelah logout.

Developers and QA staff should include functional access control unit and integration tests.

## **Burpsuite**

Burp Suite adalah alat pentesting yang sering digunakan untuk menguji keamanan aplikasi web. Alat ini memiliki berbagai fitur yang dapat membantu dalam mengidentifikasi dan mengeksploitasi kerentanan pada aplikasi web. Burp Suite dapat digunakan untuk memindai aplikasi web dan mengidentifikasi kerentanan, mencoba mengambil alih sesi pengguna, serta melakukan serangan lainnya. Berikut adalah beberapa fungsi utama dari Burp Suite:

1. Intercepting proxy: Burp Suite memiliki fitur intercepting proxy yang memungkinkan pengguna untuk memantau dan memodifikasi data yang dikirimkan antara aplikasi web dan server. Dengan fitur ini, pengguna dapat memodifikasi permintaan dan respon yang dikirimkan antara aplikasi web dan server untuk menguji keamanan aplikasi.
2. Scanner: Burp Suite memiliki fitur scanner yang dapat digunakan untuk melakukan pemindaian (scanning) kerentanan pada aplikasi web. Dengan fitur ini, Burp Suite dapat melakukan pemindaian otomatis pada aplikasi web untuk mengidentifikasi kerentanan seperti SQL injection, cross-site scripting (XSS), dan kerentanan lainnya.
3. Intruder: Burp Suite memiliki fitur Intruder yang dapat digunakan untuk melakukan serangan brute-force atau fuzzing pada aplikasi web. Dengan fitur ini, Burp Suite dapat mengirimkan serangkaian permintaan yang berbeda ke aplikasi web untuk menguji keamanannya.
4. Repeater: Burp Suite memiliki fitur repeater yang memungkinkan pengguna untuk mengirimkan permintaan yang sama berulang kali ke server untuk menguji respons dari server. Dengan fitur ini, pengguna dapat memodifikasi permintaan untuk menguji respons dari server.
5. Collaborator: Burp Suite memiliki fitur Collaborator yang dapat digunakan untuk menguji kerentanan pada aplikasi web yang terhubung dengan sumber eksternal (misalnya, server

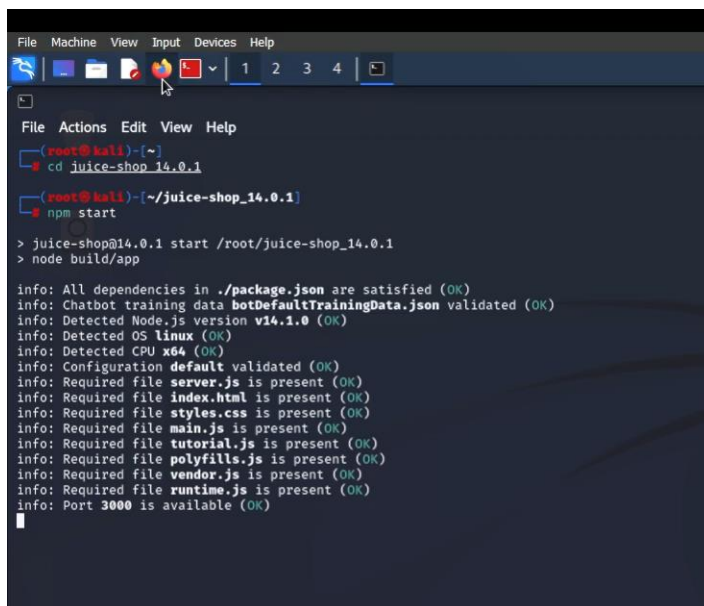
email, server DNS, dan sebagainya). Dengan fitur ini, pengguna dapat menguji apakah aplikasi web mengirimkan informasi rahasia ke sumber eksternal.

6. Decoder: Burp Suite memiliki fitur decoder yang dapat digunakan untuk memecahkan kode atau enkripsi yang digunakan pada aplikasi web. Dengan fitur ini, pengguna dapat mengidentifikasi jenis enkripsi yang digunakan pada aplikasi web dan melakukan uji coba untuk melihat seberapa mudahnya untuk memecahkan enkripsi tersebut.

## Percobaan

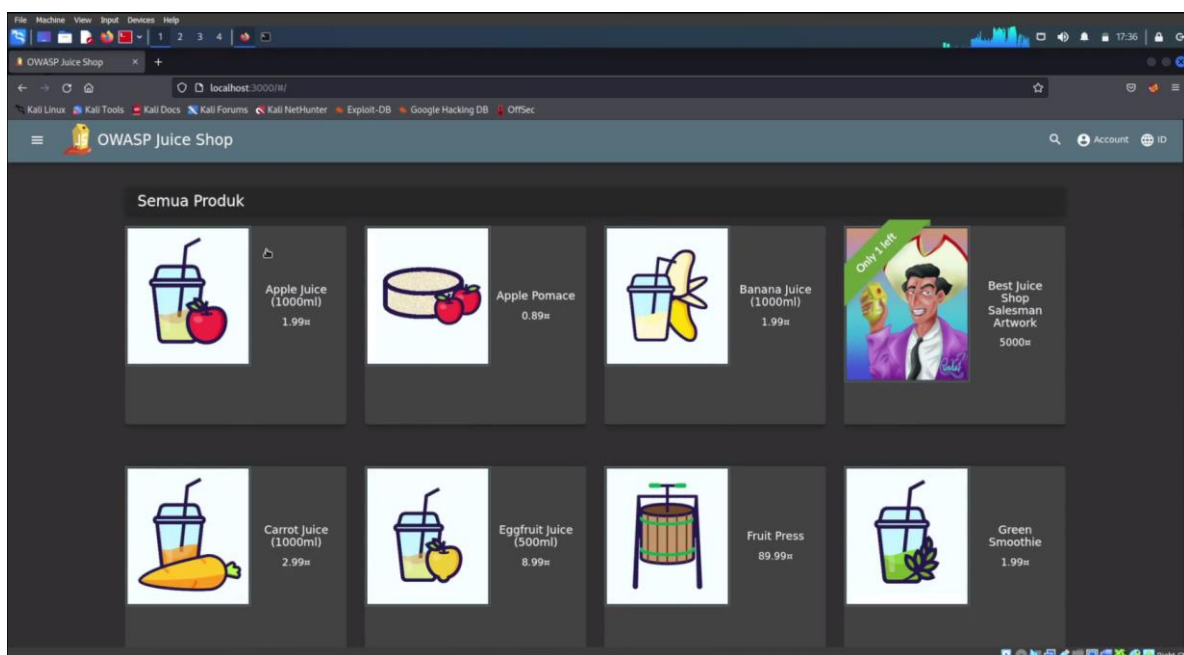
Pada percobaan ini akan masuk/login sebagai admin.

### 1. Menjalankan aplikasi juiceshop.

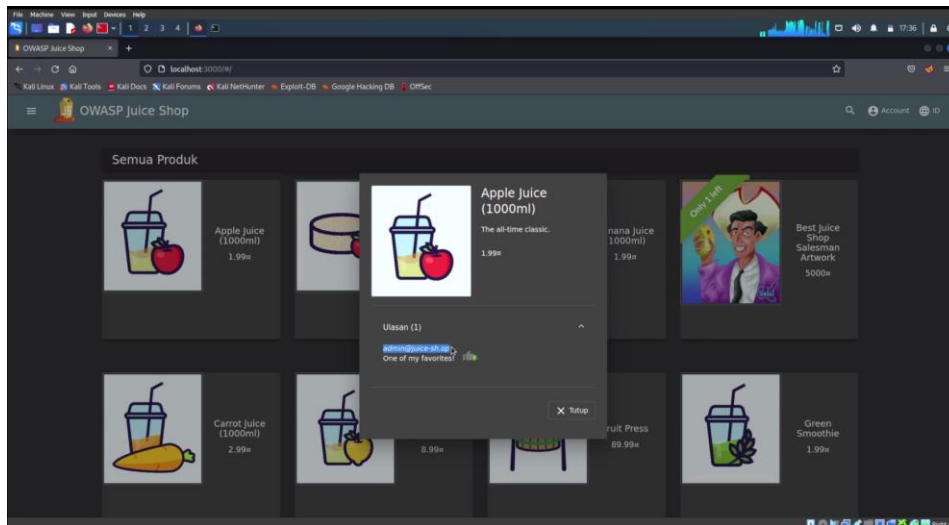


```
File Machine View Input Devices Help
File Actions Edit View Help
(root@kali)~
cd juice-shop_14.0.1
(root@kali)~[/juice-shop_14.0.1]
npm start
> juice-shop@14.0.1 start /root/juice-shop_14.0.1
> node build/app

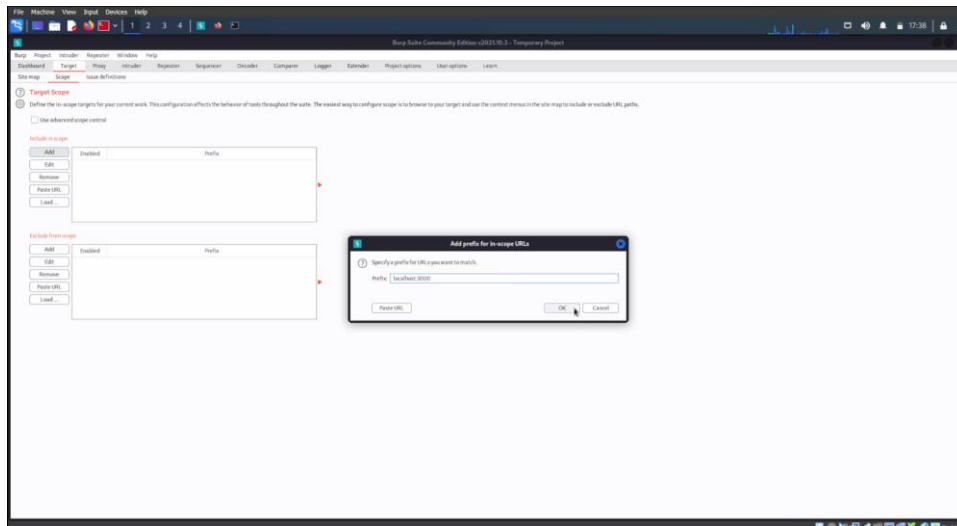
info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v14.1.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file styles.css is present (OK)
info: Required file main.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file vendor.js is present (OK)
info: Required file runtime.js is present (OK)
info: Port 3000 is available (OK)
```



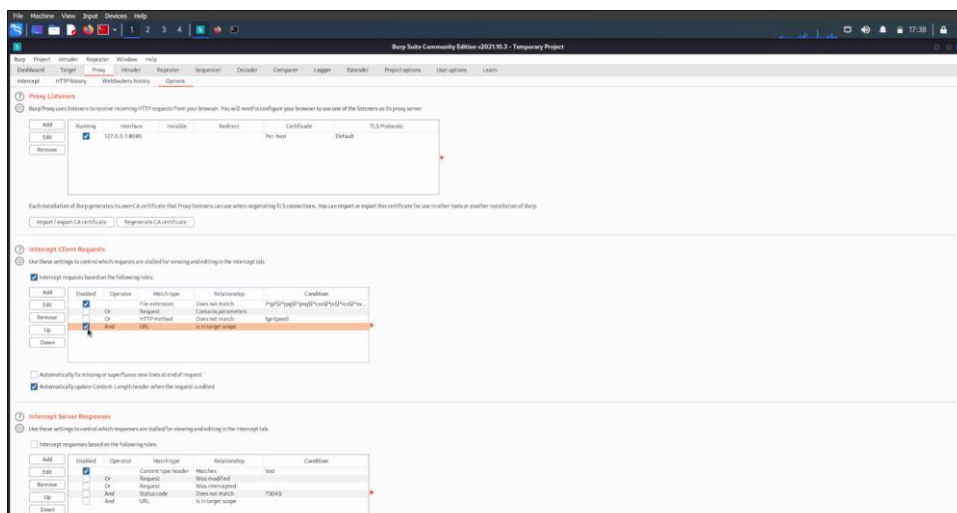
## 2. Membuka produk dan mencari ulasan produk, kemudian copy email admin.



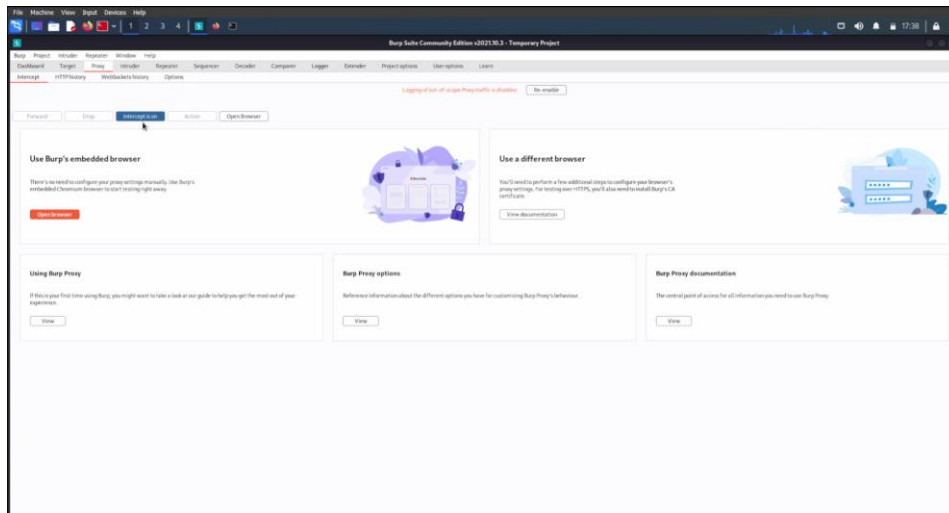
## 3. Membuka burpsuite, kemudian masuk ke menu target -> scope dan tambahkan link juice shop.



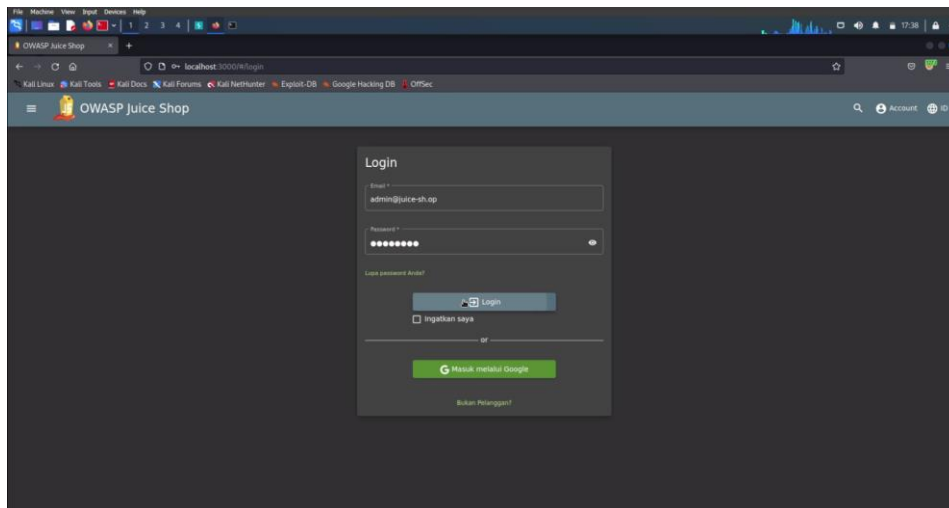
## 4. Masuk ke menu proxy -> options, kemudian checklist intercept client request operator 'AND'.



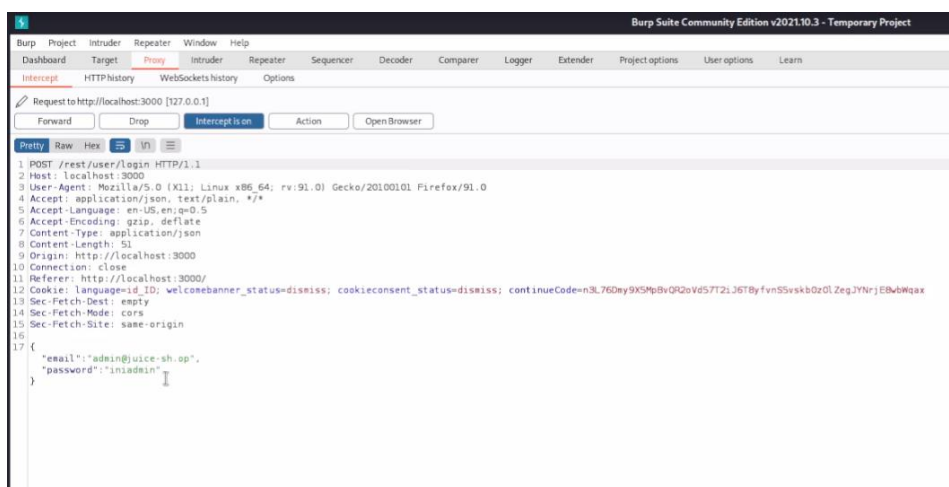
## 5. Masuk ke menu intercept dan pastikan intercept telah on.



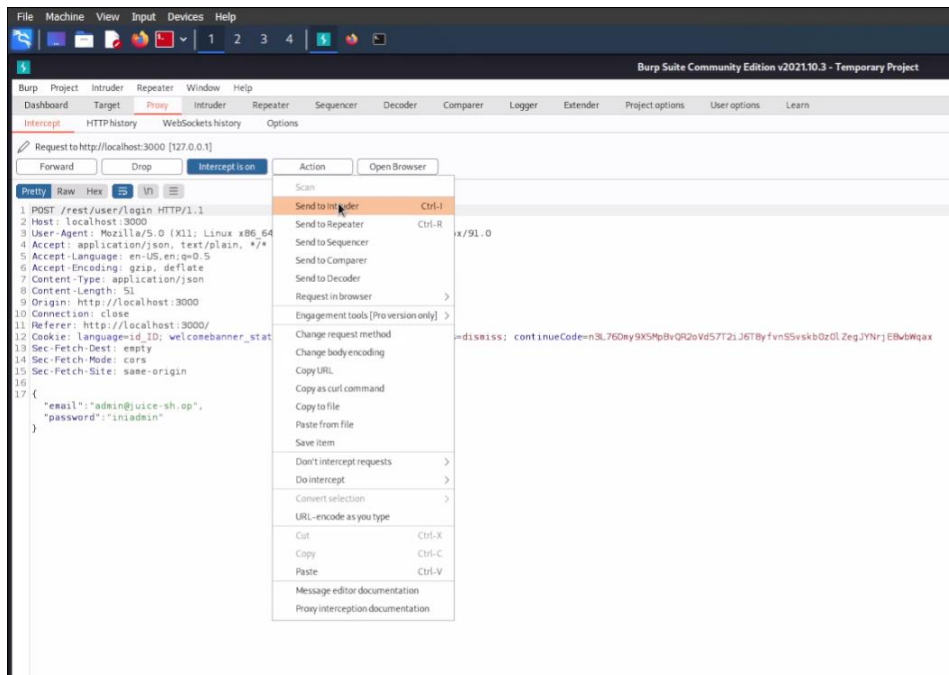
## 6. Masuk ke halaman login juice shop kemudian masukkan email admin dan password random, pastikan proxy telah menyala.



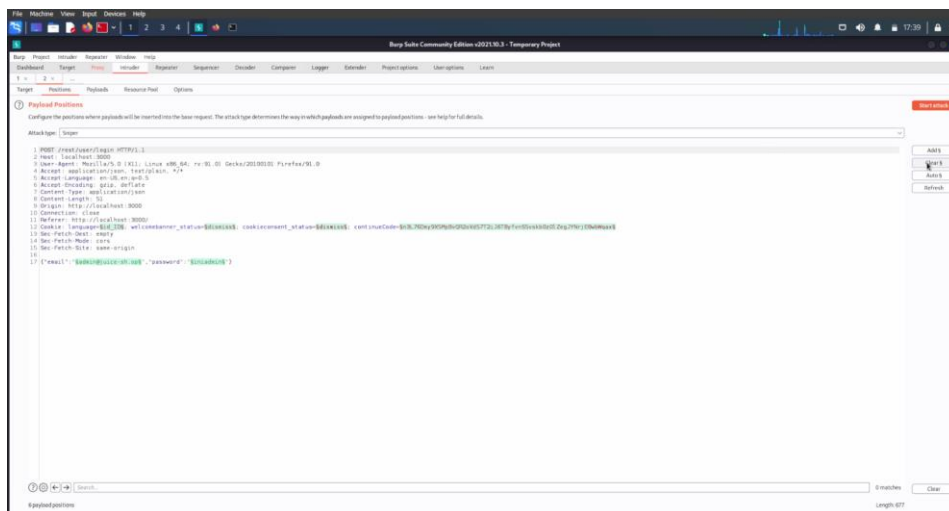
## 7. Melihat intercept dan pastikan email dan password sudah tercapture.



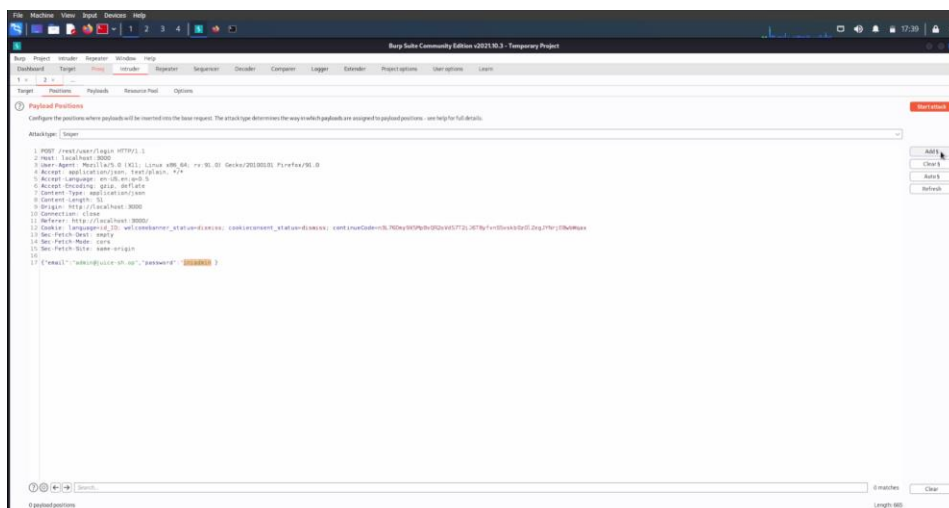
## 8. Klik action dan pilih 'Send to intruder'.



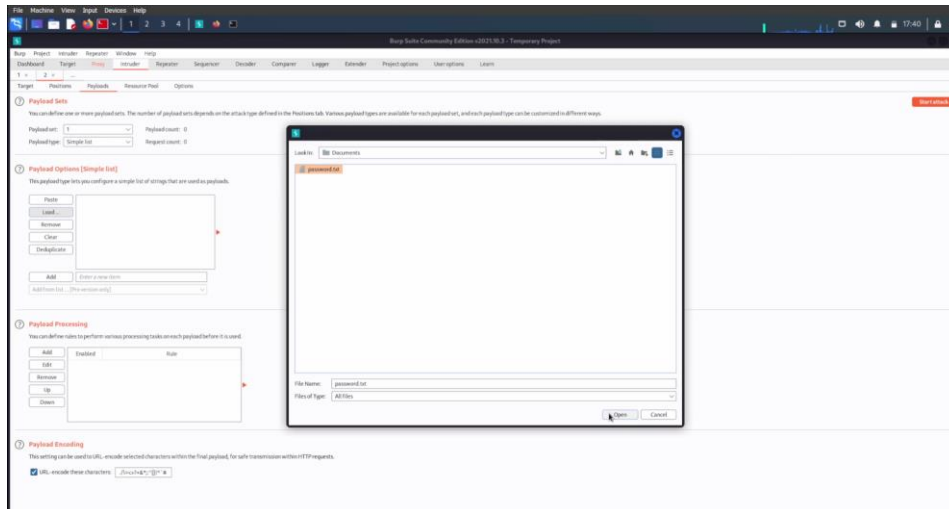
## 9. Masuk ke menu intruder -> positions, kemudian klik “Clear”.



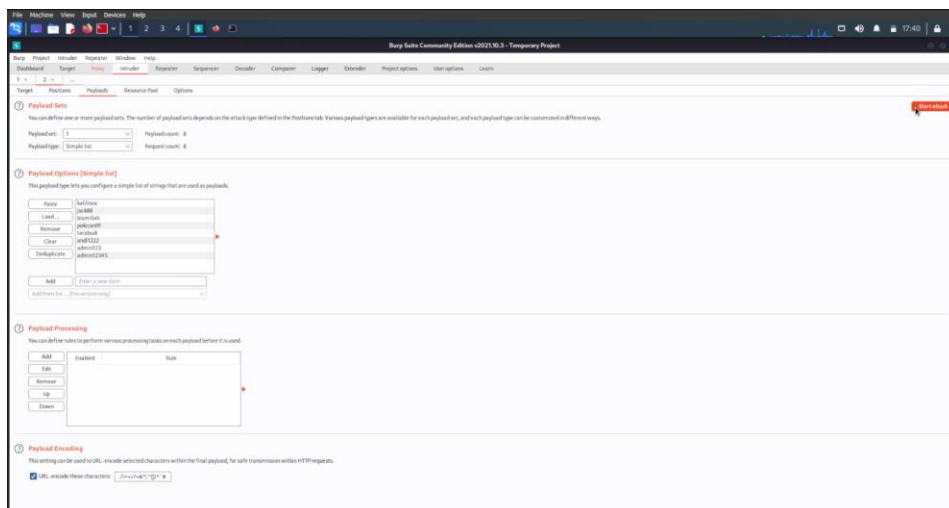
## 10. Block password kemudian klik “Add”.



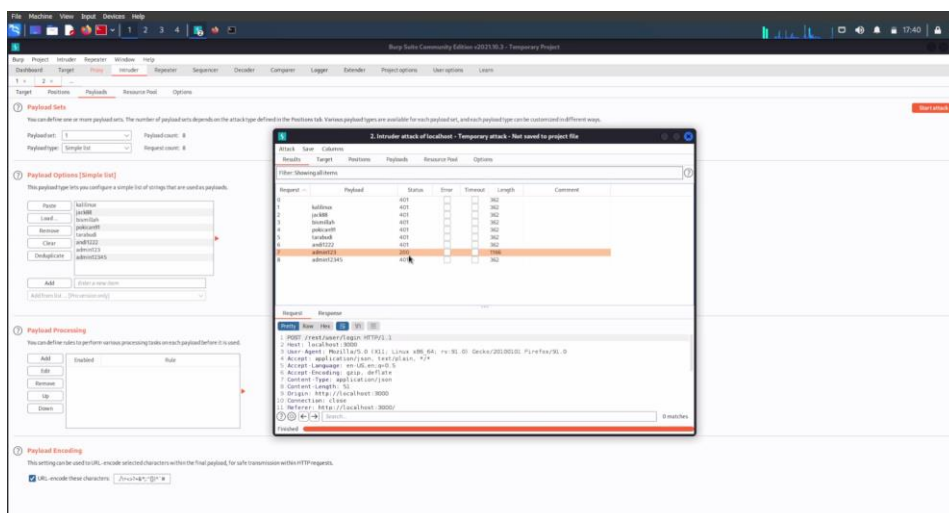
## 11. Masuk ke menu intruder -> payloads, kemudian klik load pada payload options dan pilih file berisi kumpulan password ( dapat membuat atau download file berisi kumpulan password ).



## 12. Klik start attack.

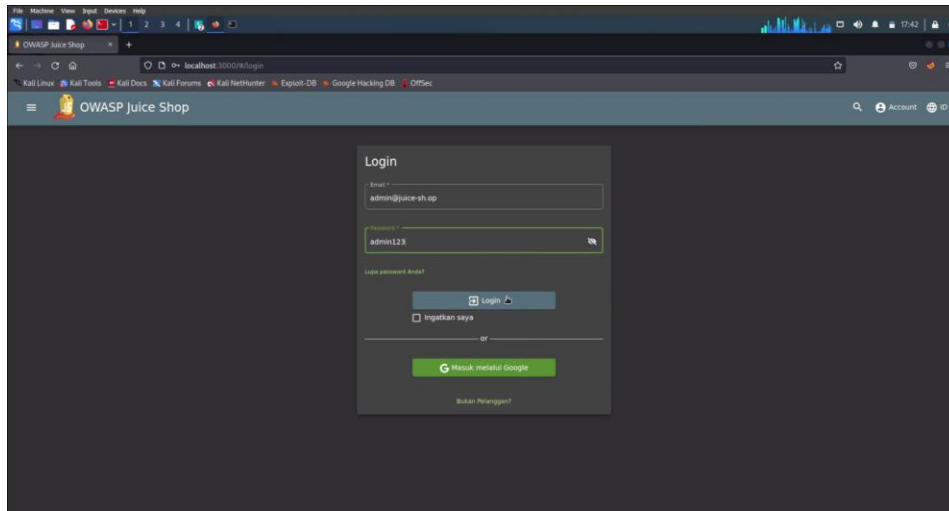


## 13. Mencari payload atau password dengan status 200





**14. Masuk ke halaman login juice shop[ dan coba login admin dengan password tersebut. Pastikan proxy telah mati.**



## **Video Demo**

<https://drive.google.com/file/d/1h4WkUVQyQrERPw1U2mRja8AW8ORE765-/view?usp=sharing>