

**TUGAS**

**KEAMANAN JARINGAN**

**“OWASP:BROKEN ACCESS CONTROL”**



Nama : Akhmad Mufti Ali Wafa

Kelas : D4 LJ IT B

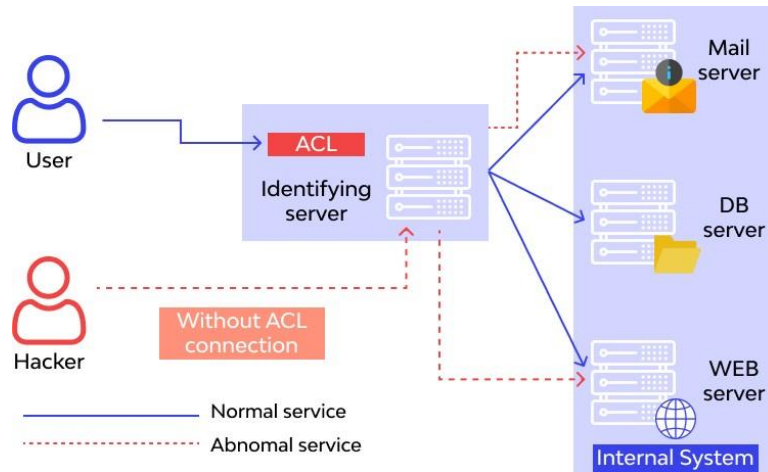
NRP 3122640048

**POLITEKNIK ELEKTRONIKA NEGERI SURABAYA**

**TAHUN AJARAN 2022/2023**

## A. PENDAHULUAN

Orang lain dapat mengakses sebuah sistem ketika autentikasi dan pembatasan akses tidak diterapkan dengan baik. Dengan kata lain, **Broken Access Control** memungkinkan entri yang tidak sah yang dapat mengakibatkan kerentanan data dan file yang bersifat sensitif. Kontrol akses yang lemah terkait manajemen kredensial dapat dihindari dengan metode coding yang unik dan tindakan khusus seperti mematikan akun administratif dan penggunaan autentikasi multi-faktor. Berikut ini ilustrasi gambaran BAC (Broken Access Control) secara general:

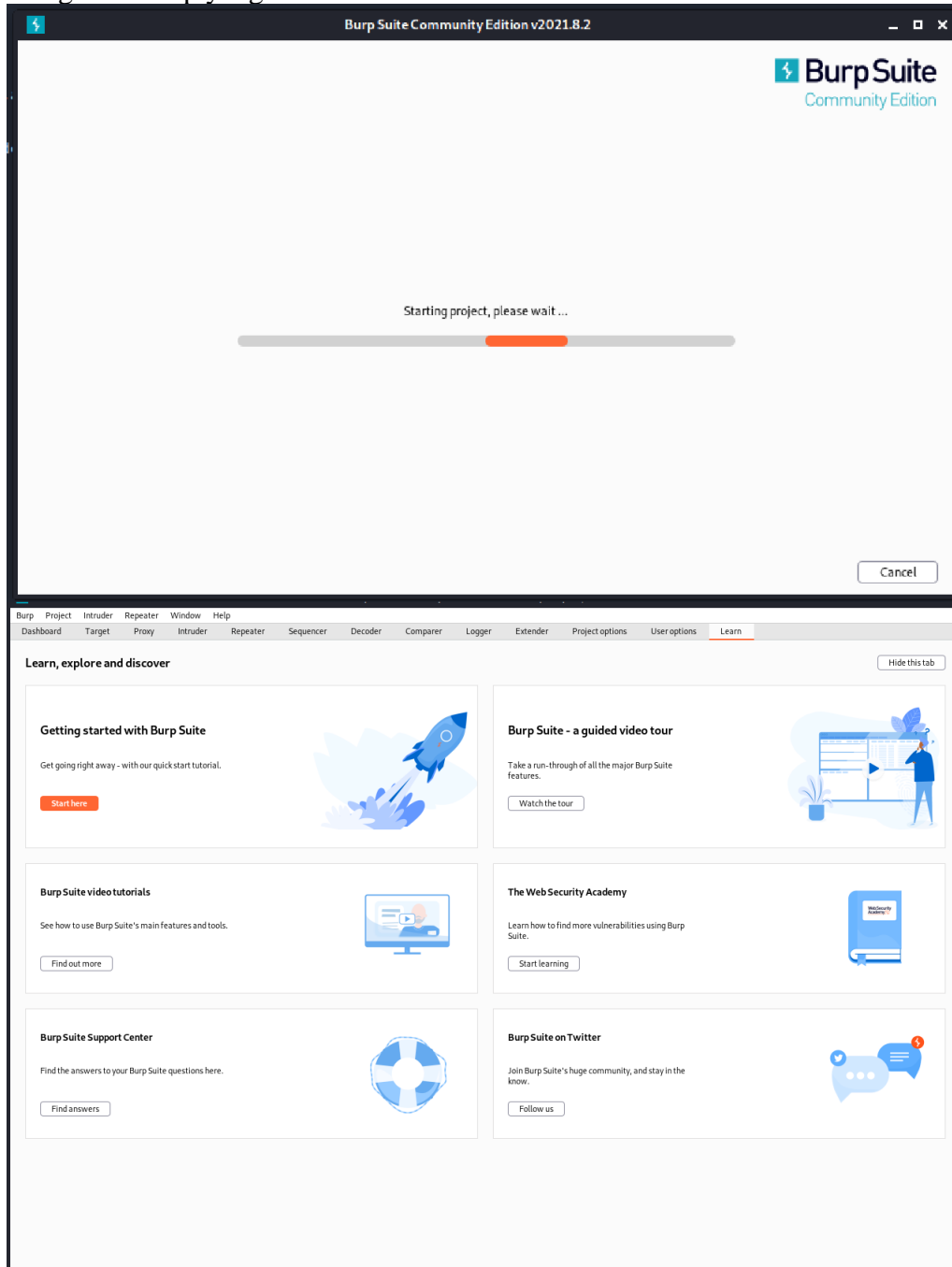


Gambar diatas memperlihatkan orang yang tidak punya akses bisa mengakses.

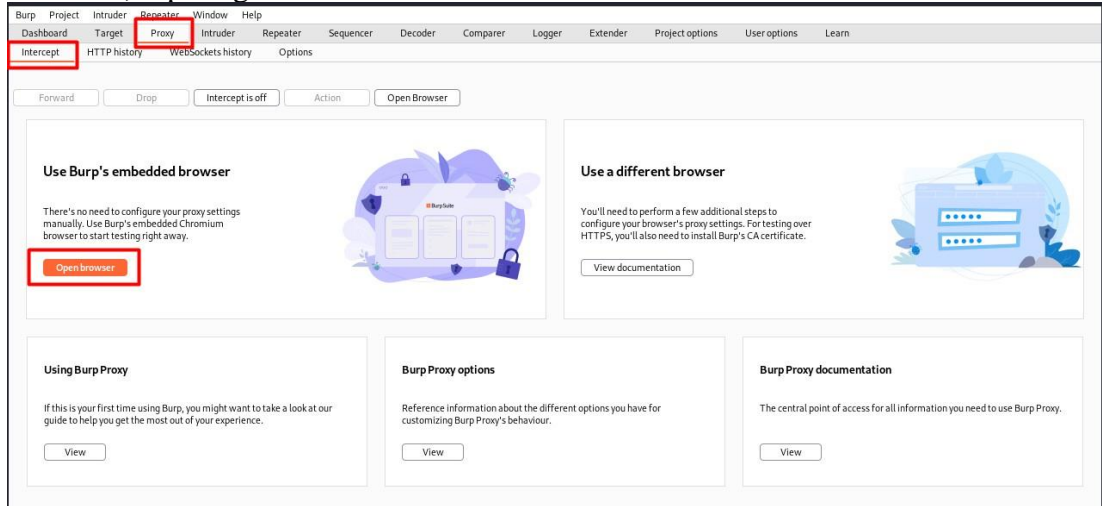
## B. PERCOBAAN

### a) Mengakses Keranjang Belanja dari User Lain

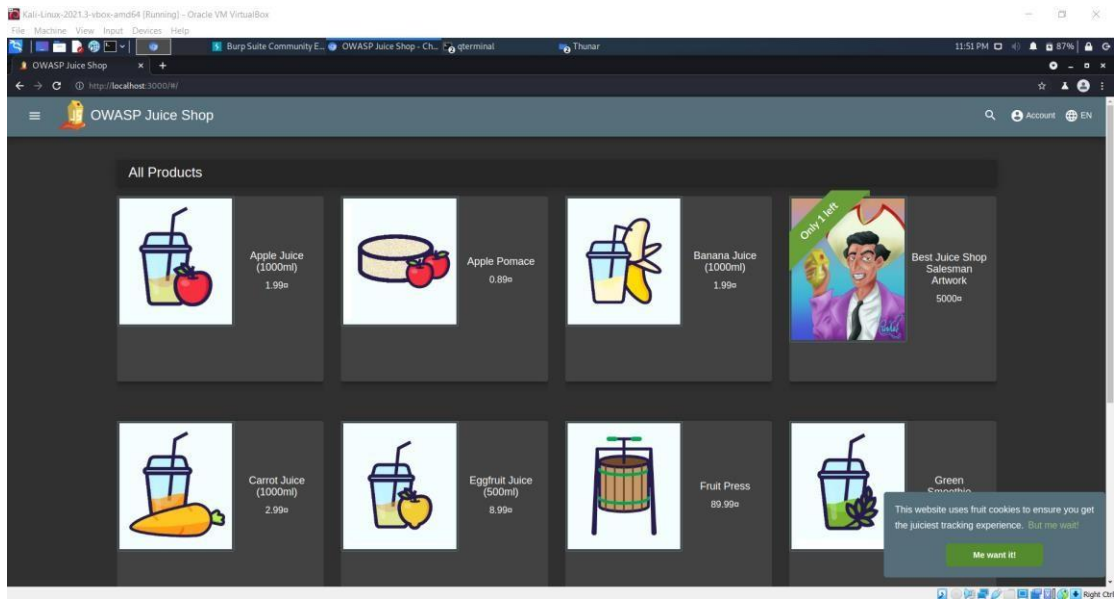
1. Pertama yang harus dilakukan adalah membuka aplikasi burp suite yang sudah terpasang pada kali linux. fungsinya sebagai http proxy. Aplikasi ini berfungsi untuk mengetrace http yang keluar dan masuk



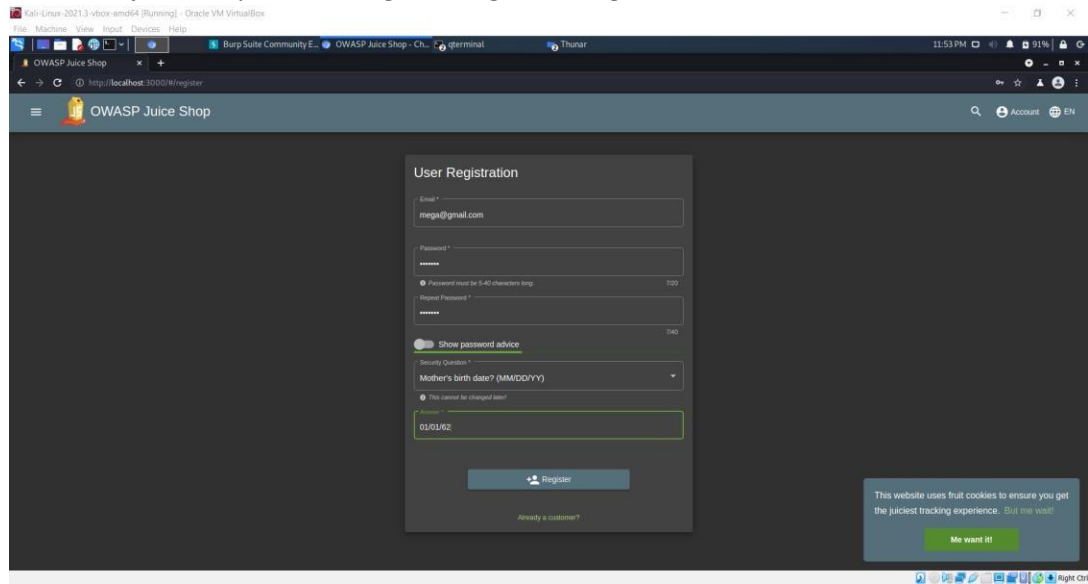
2. Pada aplikasi ini , buka tab “Proxy” kemudian pilih “Intercept” lalu klik “Open browser”, seperti gambar dibawah ini :



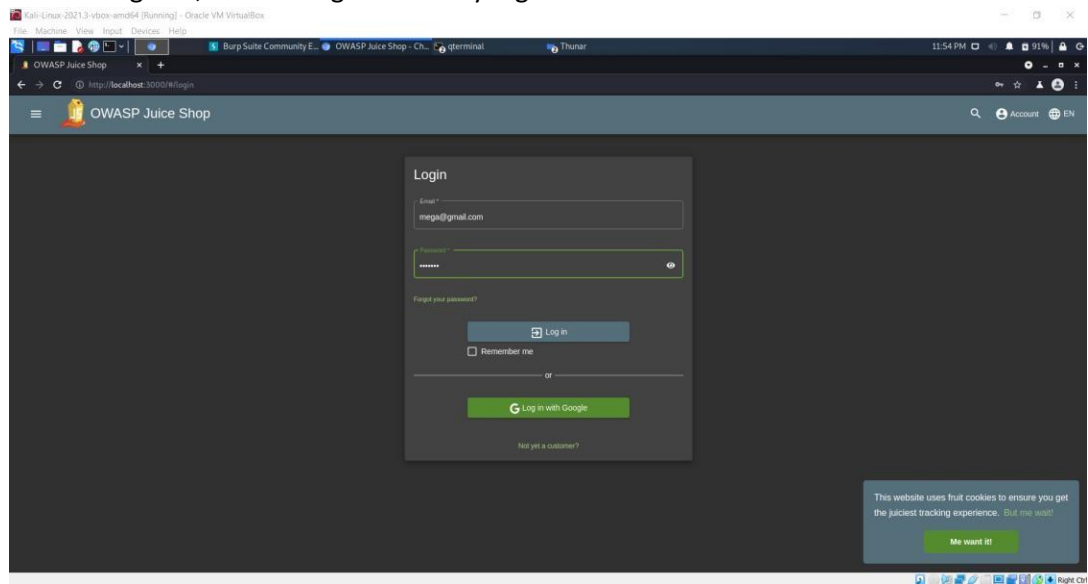
3. Pada terminal masuk ke folder juice-shop yang sebelumnya sudah pernah didownload, kemudian jalankan dengan cara “npm start” dan pada halaman browser burp suite tuliskan url localhost dan port yang menjalankan aplikasi juice shop.



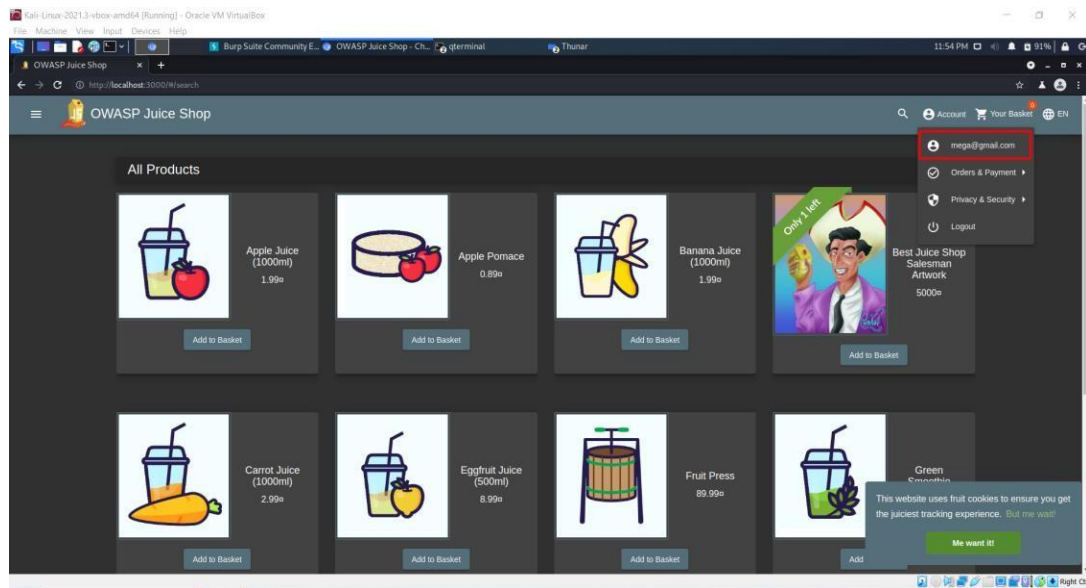
4. Pada web juice shop lakukan registrasi agar bisa login ke web tersebut



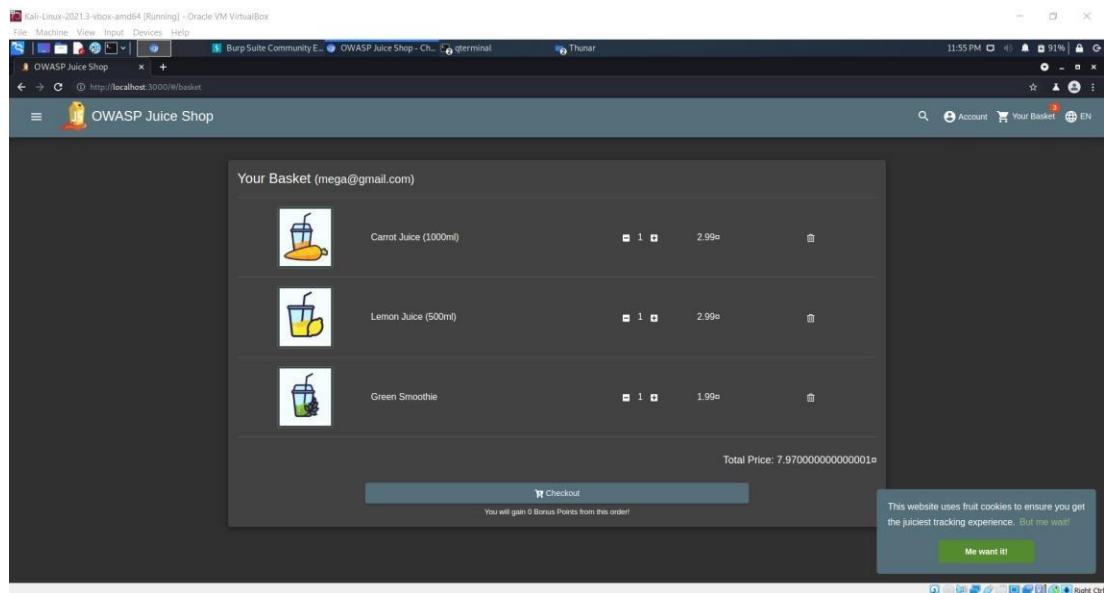
5. Setelah register, lakukan login ke akun yang sudah didaftarkan



6. Jika berhasil login maka pada menu account akan tampil email yang digunakan untuk login



7. Memasukkan beberapa produk kedalam keranjang dengan cara klik “add to basket”, kemudian cek pada menu “your basket”. Disini saya memasukkan 3 produk seperti gambar di bawah ini :



- Burp Project Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Dashboard Target Proxy Includer WebSockets history Options

Intercept HTTP history

Filter: Hiding CSS, Image and general binary content

#	Host	Meth.. ^		URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
111	http://localhost:3000	GET	/rest/basket/6				200	1787	JSON				✓	127.0.0.1
112	http://localhost:3000	GET	/rest/basket/6				304	254					✓	127.0.0.1
113	http://localhost:3000	GET	/rest/user/wsoami				304	253					✓	127.0.0.1
31	http://localhost:3000	POST	/socket.io/?EIO=4&transport=polling&		✓		200	121	text	io/			✓	127.0.0.1
60	https://play.google.com	POST	/log?format=json&hasfast=true		✓		200	984	JSON				✓	74.125.200.101
62	https://play.google.com	POST	/log?format=json&hasfast=true		✓		200	984	JSON				✓	74.125.200.101
67	https://play.google.com	POST	/log?format=json&hasfast=true		✓		200	582	JSON				✓	74.125.200.101
71	http://localhost:3000	POST	/socket.io/?EIO=4&transport=polling&		✓		200	121	text	io/			✓	127.0.0.1
77	http://localhost:3000	POST	/api/users/		✓		201	670	JSON				✓	127.0.0.1
78	http://localhost:3000	POST	/api/SecurityAnswers/		✓		201	600	JSON				✓	127.0.0.1
80	http://localhost:3000	POST	/rest/login		✓		200	1159	JSON				✓	127.0.0.1
101	http://localhost:3000	POST	/api/BasketItems/		✓		200	491	JSON				✓	127.0.0.1
105	http://localhost:3000	POST	/api/BasketItems/		✓		200	491	JSON				✓	127.0.0.1
109	http://localhost:3000	POST	/api/BasketItems/		✓		200	492	JSON				✓	127.0.0.1

Request Inspector

Pretty Raw Hex In Out

Inspector

Request Attributes

Request Cookies (3)

Response Headers (17)

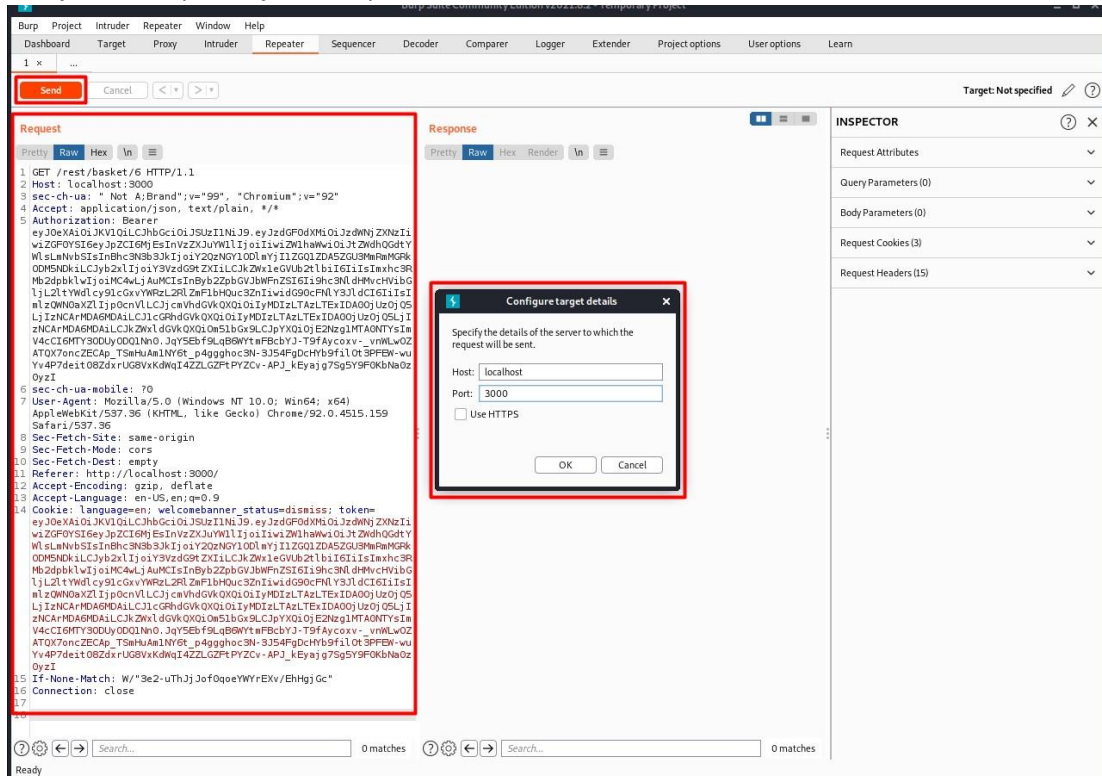
Response Headers (10)

```
{
  "status": "success",
  "data": {
    "id": 9,
    "ProductId": 30,
    "BasketId": "6",
    "quantity": 1,
    "updatedAt": "2023-03-11T04:54:50.897Z",
    "createdAt": "2023-03-11T04:54:50.897Z"}
}
```

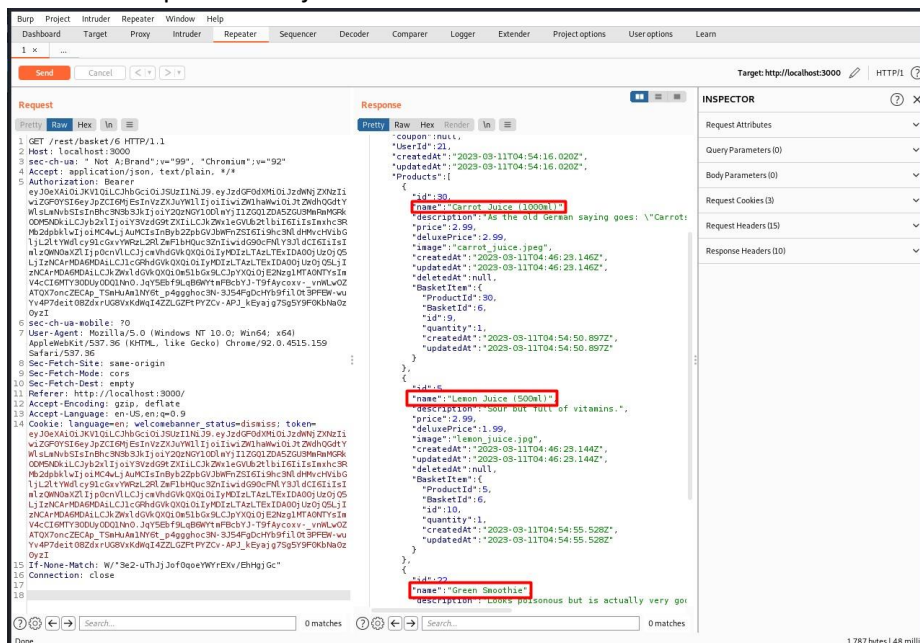
- [illegible]



10. Kemudian selanjutnya masuk ke tab “Repeater” copy request dari tahap sebelumnya, salin pada request yang ada di tab “Repeater”. Jika sudah klik “send” dan akan muncul pop up mengisikan host dan port, disini diisi sesuai host dan port yang digunakan dalam menjalankan aplikasi juice shop

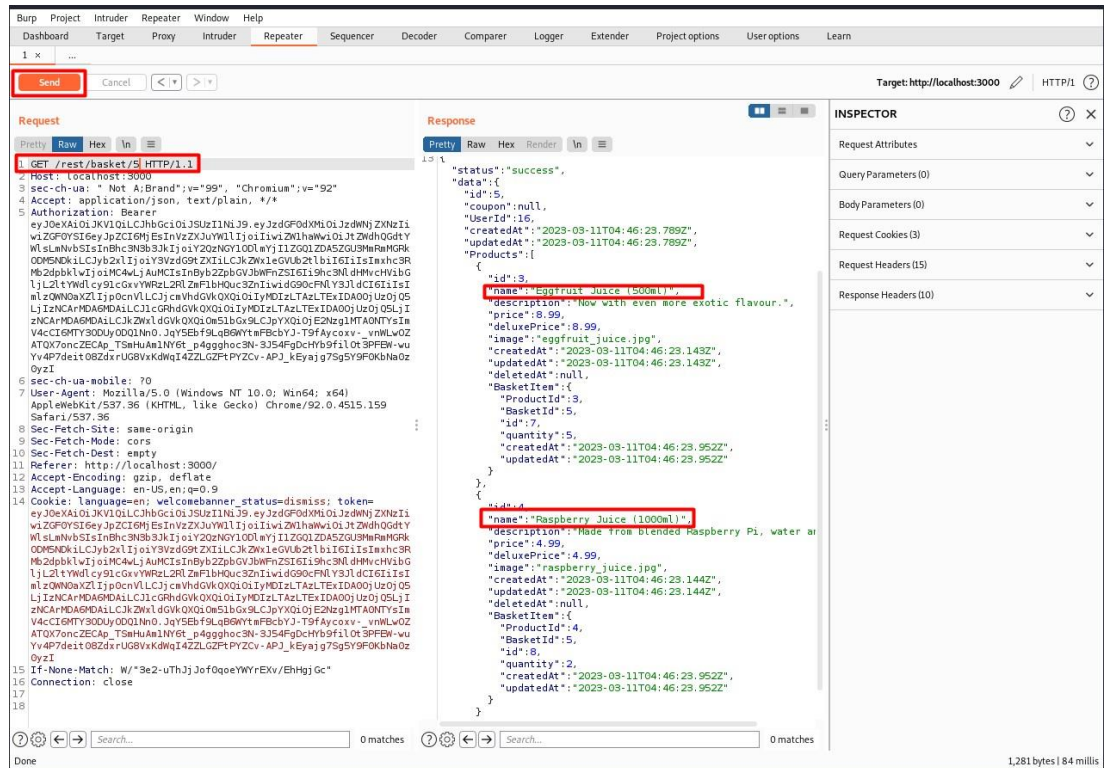


11. Berikut merupakan hasil jika sudah berhasil klik “send”



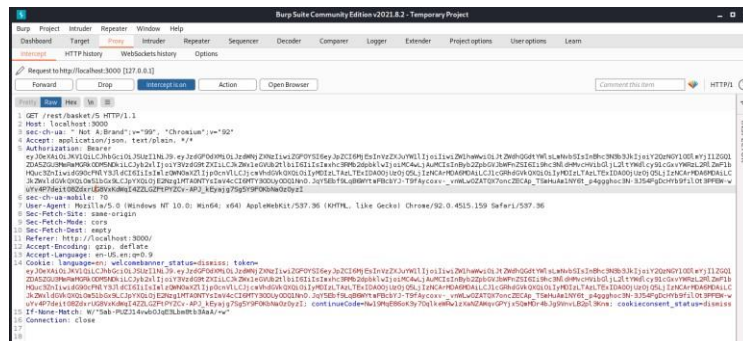


12. Untuk mencoba broken access control , disini saya mencoba untuk mengakses id keranjang dari user yang lain. Sehingga saya akan mengubah id yang sebelumnya “6” menjadi “5”. Seperti gambar di bawah ini :



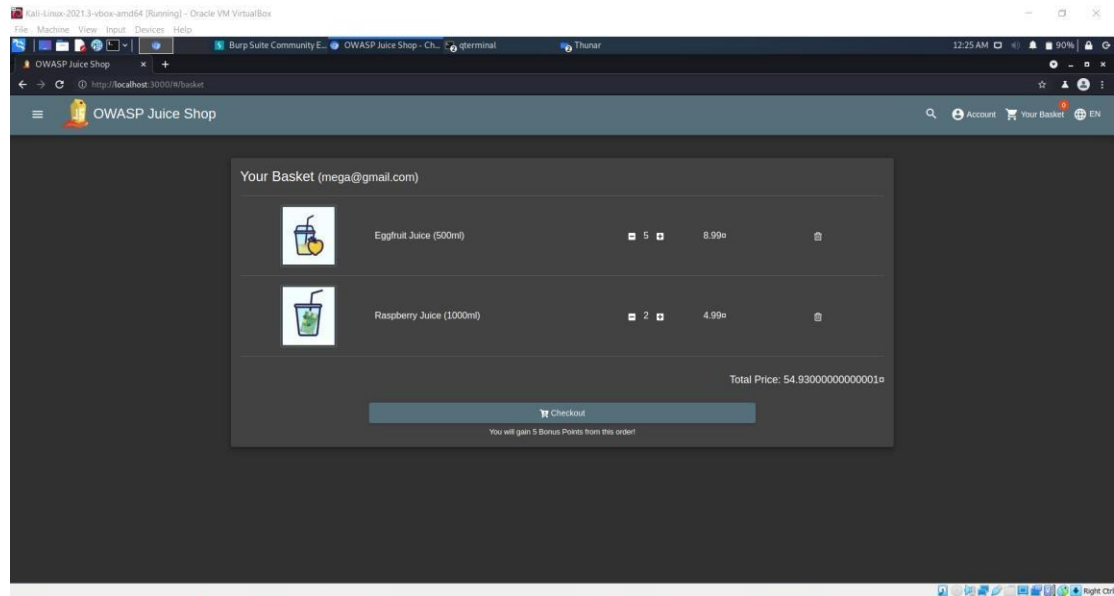
Dari gambar diatas dapat dilihat, saya dapat melihat produk dari keranjang 5 yang berbeda dari produk yang saya inputkan tadi. Disini hanya ada 2 produk dengan nama dan kuantitas yang berbeda dari yang saya inputkan.

13. Untuk dapat melihat respon tersebut di juice shop, disini mencoba menggunakan fitur dari burpsuite yaitu intercept. Dengan cara masuk ke tab “proxy” lalu masuk ke tab “intercept”. Jika sudah di halaman seperti gambar di bawah ini , klik “intercept of” sehingga nanti akan berubah menjadi “intercept on”.



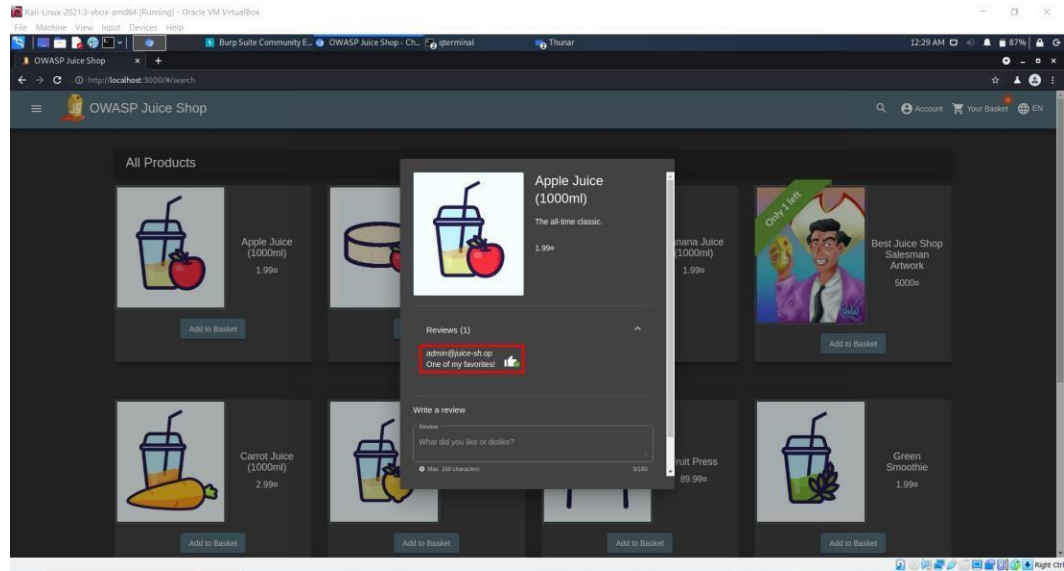
Setelah menyalakan intercept, buka kembali website juice shop masuk ke halaman “home page” dan buka kembali halaman “keranjang”.

Lalu buka burpsuite dan klik tombol “forward” hingga pada bagian raw muncul header memanggil keranjang id 5. Jika di klik forward lagi, maka tampilan website akan berubah menjadi informasi dari keranjang 5 seperti gambar di bawah ini :

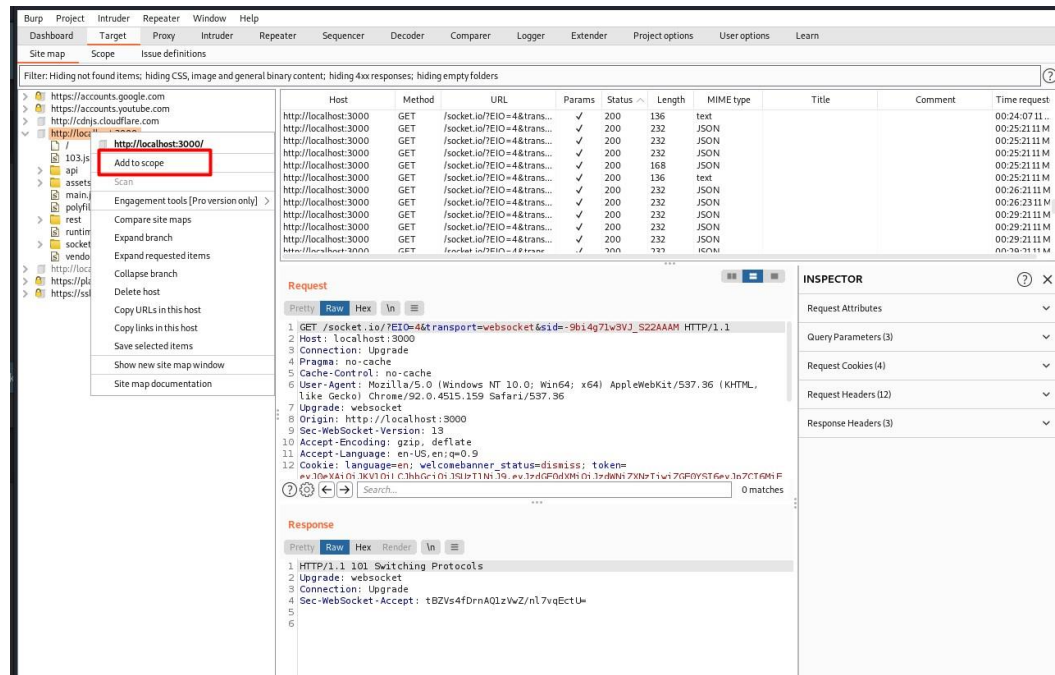


## b) Percobaan 2, Control Admin Section

- Langkah pertama yang dilakukan adalah mencari tau info email admin, dengan cara klik salah satu produk. Disana akan ditampilkan email admin seperti gambar di bawah ini :



- Lalu pada burpsuite tambahkan hostname dan port yang digunakan untuk menjalankan juice shop ini kedalam scope, dengan cara masuk ke tab “target” lalu pada “site map” klik kanan url dan pilih “add to scope”.



3. Jika sudah di klik add to scope maka tampilannya akan menjadi seperti ini :

The screenshot shows the Burp Suite Community Edition v2021.8.2 interface. The 'Target' tab is selected, and the 'Scope' section is highlighted. A red box indicates the message 'Logging of out-of-scope Proxy traffic is disabled' with a 'Re-enable' button. Below this, a table lists HTTP requests. The first request is a GET to /socket.io/?EIO=4&transport=websocket&sid=-9b14g7lw8VJ\_S22AAAM. The 'Inspector' panel on the right shows the details of the selected request, including headers and cookies.

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time request
http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket&sid=-9b14g7lw8VJ_S22AAAM		200	136	text			00:24:07.11...
http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket&sid=-9b14g7lw8VJ_S22AAAM		200	232	JSON			00:25:21.11 M
http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket&sid=-9b14g7lw8VJ_S22AAAM		200	232	JSON			00:25:21.11 M
http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket&sid=-9b14g7lw8VJ_S22AAAM		200	168	JSON			00:25:21.11 M
http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket&sid=-9b14g7lw8VJ_S22AAAM		200	136	text			00:25:21.11 M
http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket&sid=-9b14g7lw8VJ_S22AAAM		200	232	JSON			00:26:21.11 M
http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket&sid=-9b14g7lw8VJ_S22AAAM		200	232	JSON			00:26:23.11 M
http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket&sid=-9b14g7lw8VJ_S22AAAM		200	232	JSON			00:29:21.11 M
http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket&sid=-9b14g7lw8VJ_S22AAAM		200	232	JSON			00:29:21.11 M
http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket&sid=-9b14g7lw8VJ_S22AAAM		200	232	JSON			00:29:21.11 M
http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket&sid=-9b14g7lw8VJ_S22AAAM		200	232	JSON			00:29:21.11 M

The screenshot shows the 'Target Scope' configuration window in Burp Suite. It allows users to define the in-scope targets for their current work. The 'Include in scope' section is active, showing a list of targets. The first target is 'http://localhost:3000/' with the 'Enabled' checkbox checked. The 'Exclude from scope' section is empty.

**Target Scope**

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to configure scope is to browse to your target and use the context menus in the site map to include or exclude URL paths.

☐ Use advanced scope control

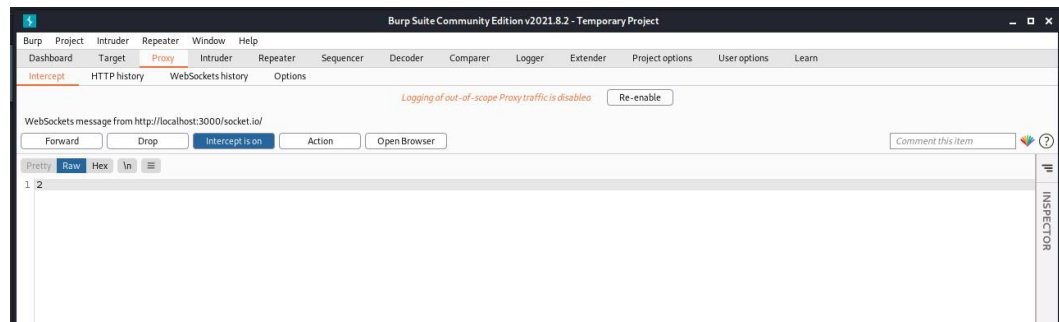
**Include in scope**

Enabled	Prefix
<input checked="" type="checkbox"/>	http://localhost:3000/

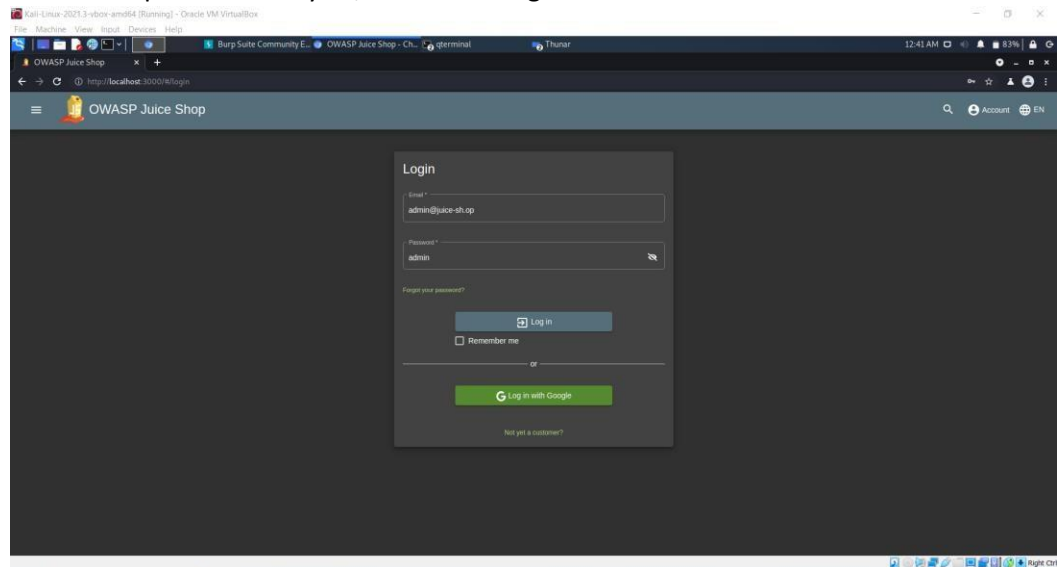
**Exclude from scope**

Enabled	Prefix
---------	--------

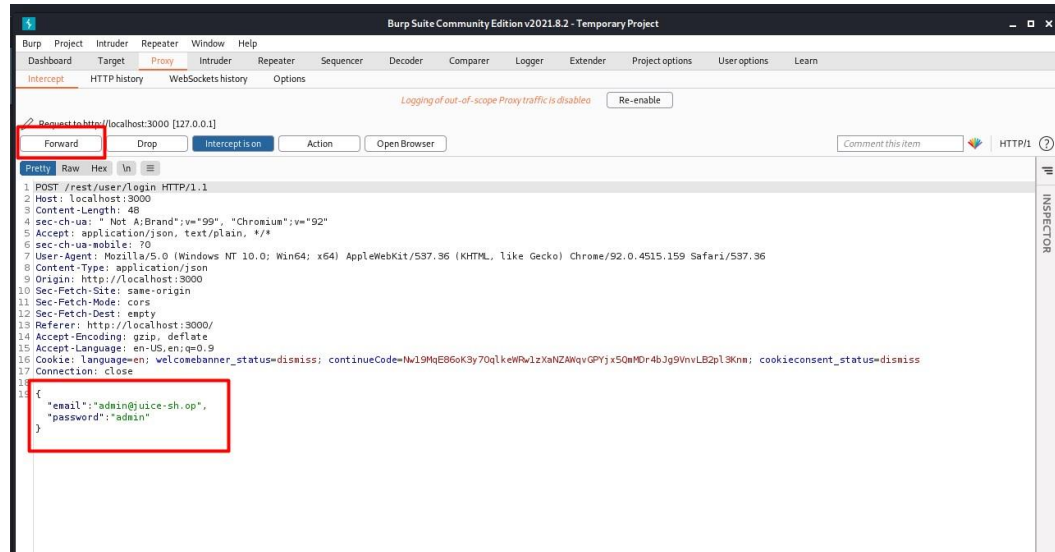
- Langkah selanjutnya adalah menuju ke halaman login dan mengisi email admin dengan password bebas. Namun sebelum klik button “Login” saya harus menyalakan intercept seperti cara yang sebelumnya, hal ini digunakan untuk tracking.



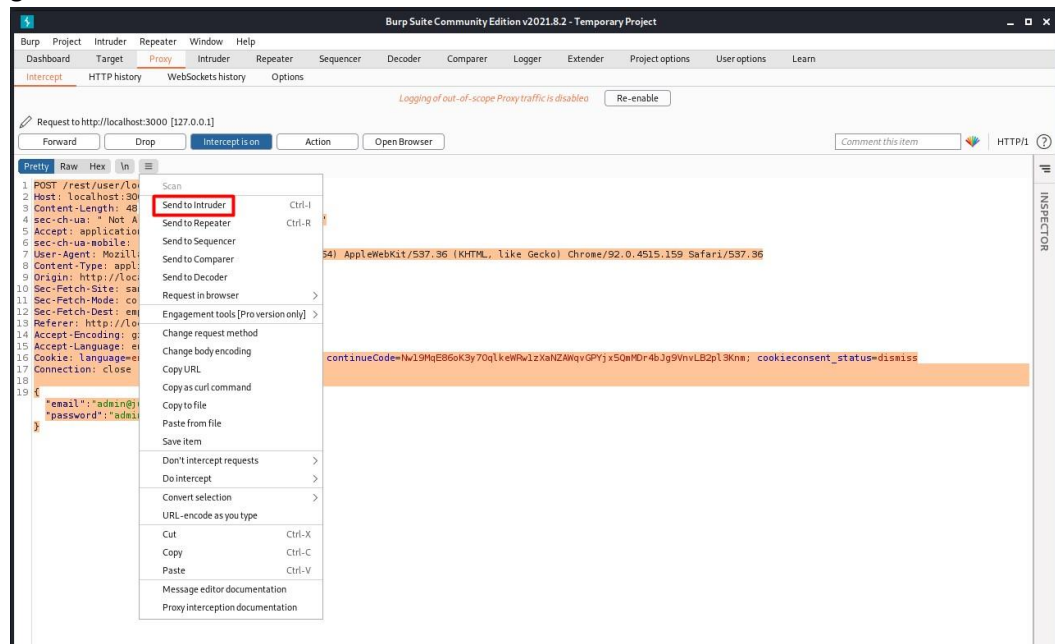
Jika intercept sudah menyala, maka klik “Login”



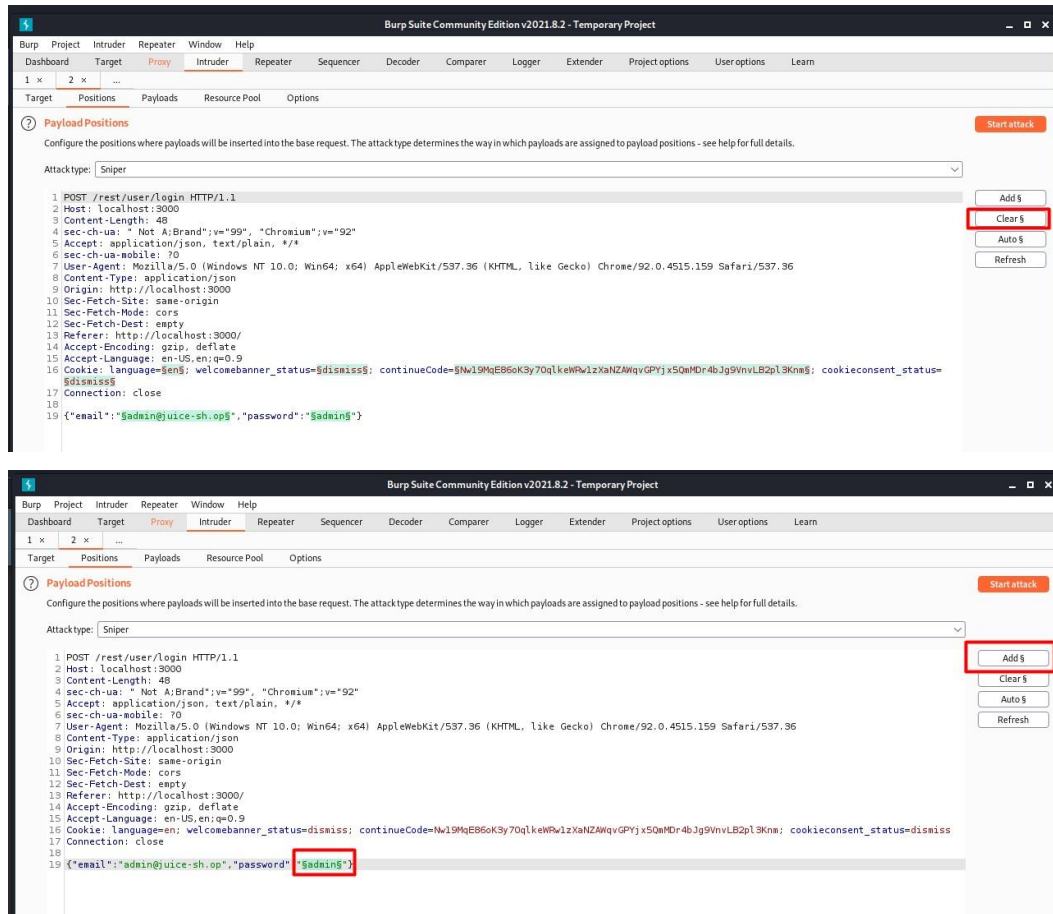
5. Setelah klik “Login” kembali ke burpsuite dan klik “forward” hingga dapat dilihat raw yang menampilkan email dan password.



6. Lalu response ini dikirimkan pada intruder dengan cara “send to intruder”, seperti gambar di bawah ini :



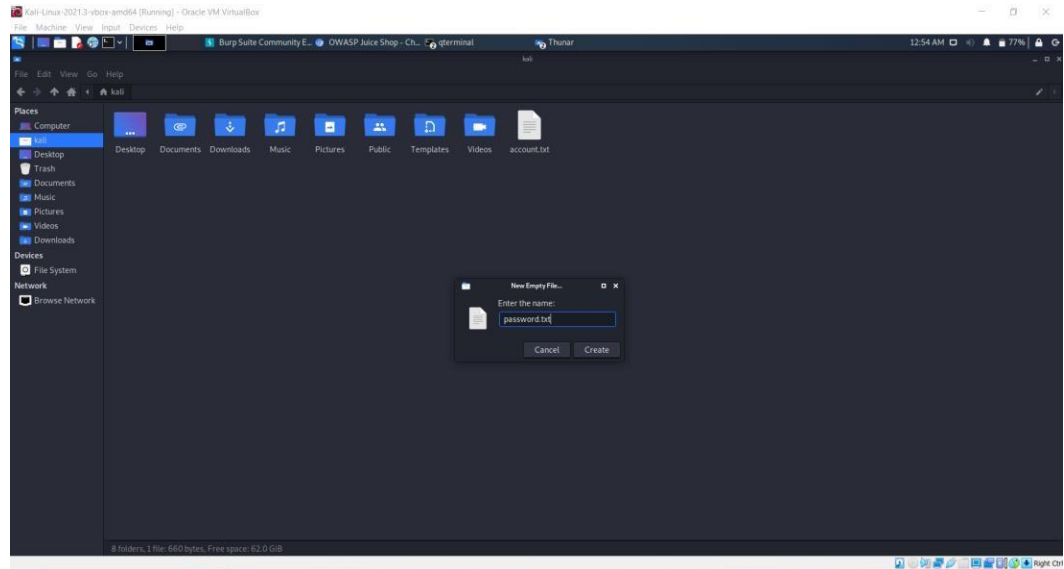
7. Setelah itu masuk ke tab “intruder” dan pilih tab “positions”. Maka akan tampil seperti gambar di bawah ini. Kemudian klik “clear” untuk membersihkan format dari cookie, berikut perbedaanya :



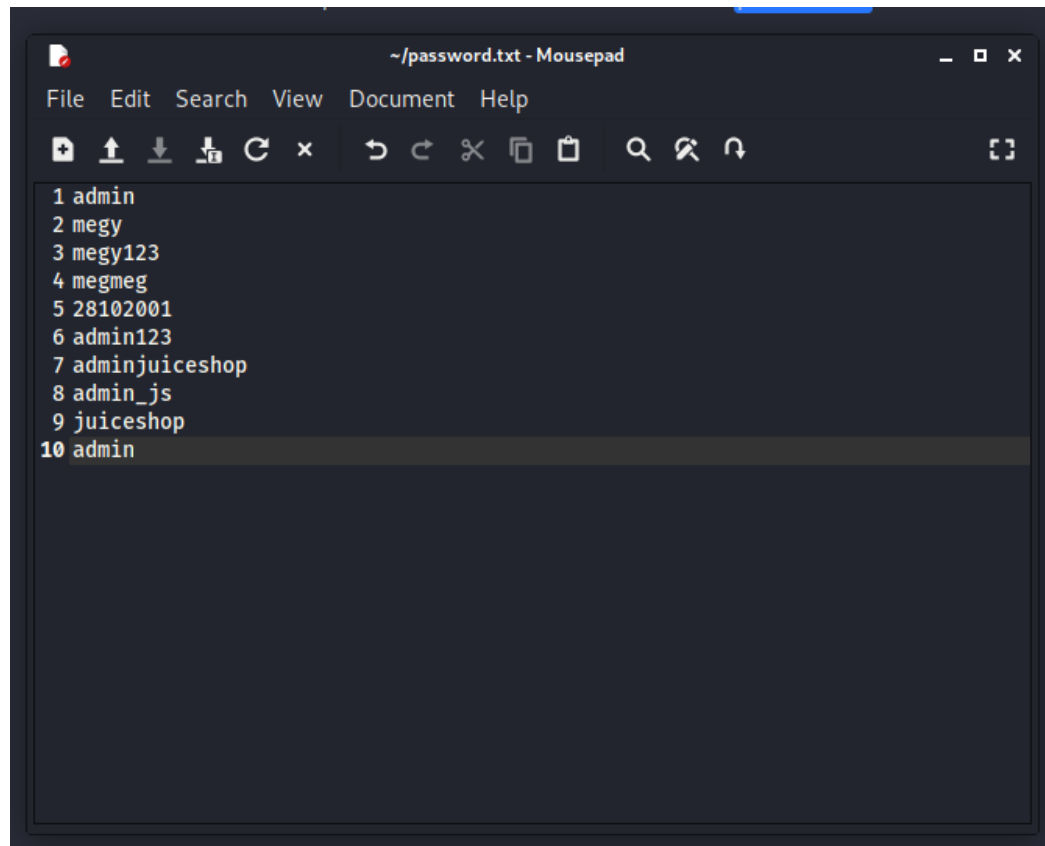
Setelah di clear maka akan tampil seperti gambar diatas, langkah selanjutnya adalah blok password lalu klik add. Sehingga yang isian password menjadi seperti gambar diatas.



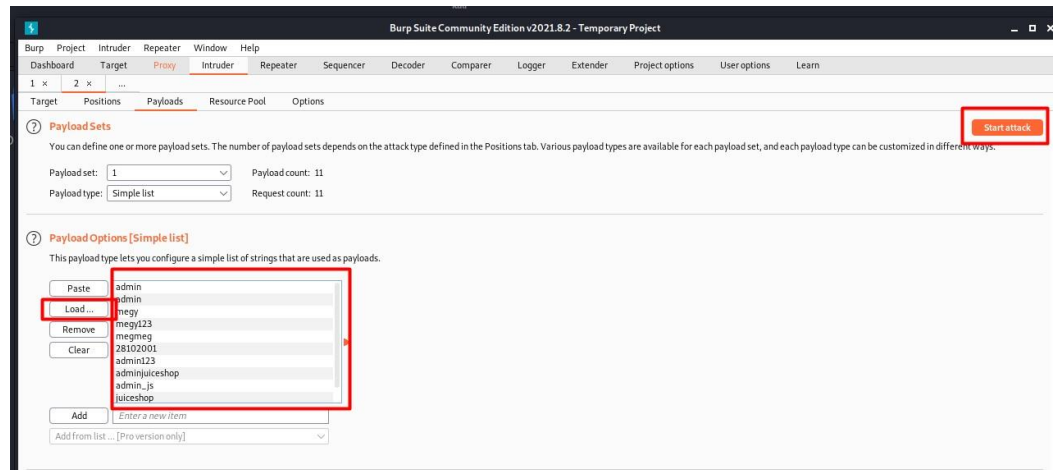
8. Lalu menyiapkan satu file bertipe txt, yang berisikan list password yang sering digunakan atau password yang memungkinkan menjadi password admin.



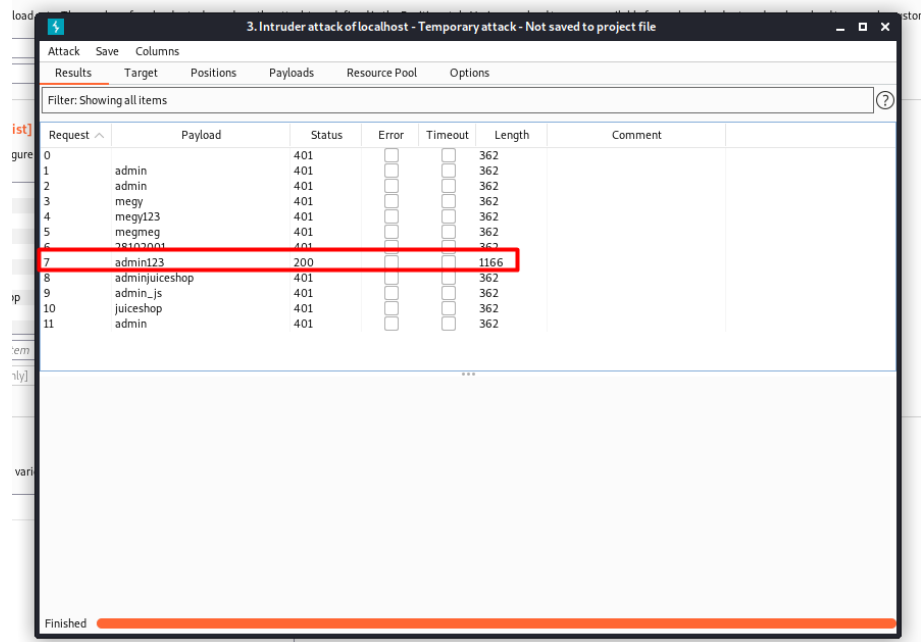
9. Isi merupakan list password yang coba saya buat



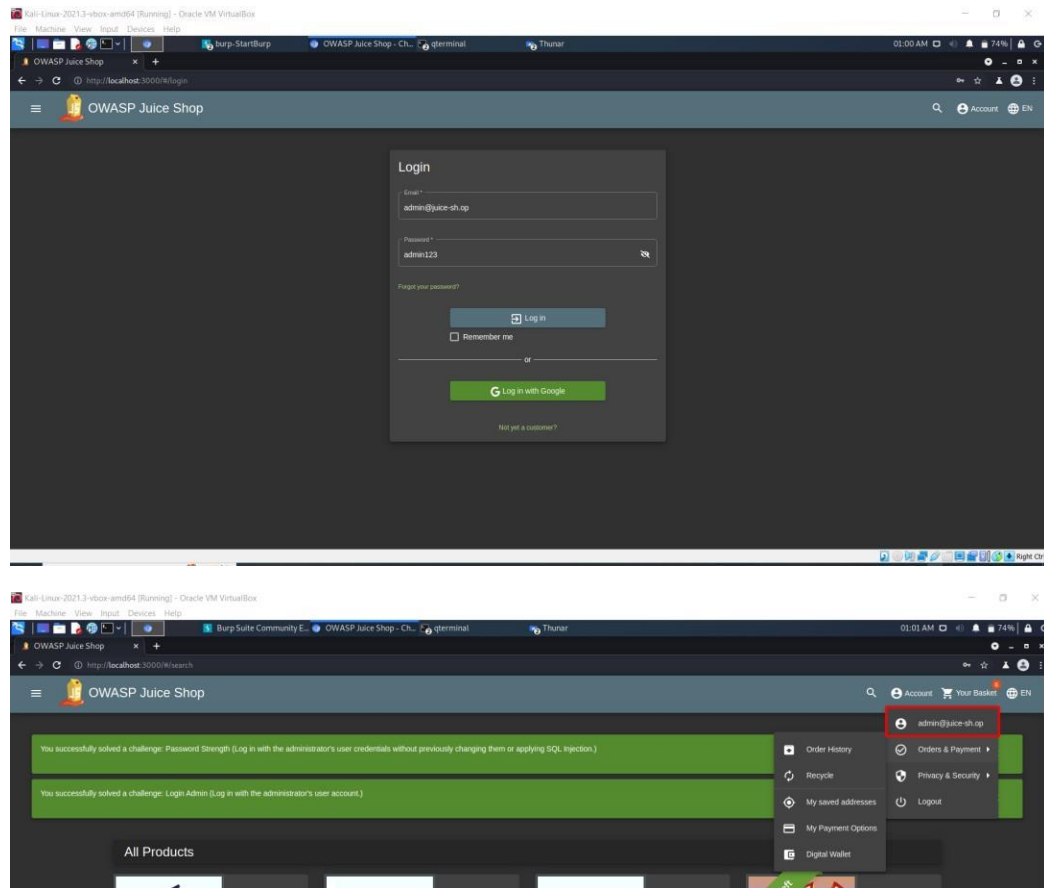
10. Lalu pada burpsuite klik tab “intruder” dan pilih “payloads”, lalu upload file txt tersebut hingga muncul pada list. Jika sudah klik “start attack”.



11. Lalu hasil dari attack adalah gambar dibawah ini, dapat dilihat disini yang memiliki status 200 adalah admin123, sedangkan yang lainnya memiliki status 401. Hal ini mengartikan bahwa password yang benar adalah “admin123”



12. Selanjutnya mencoba login pada juice shop dengan password yang sudah dianggap benar tadi , berikut merupakan hasil loginnya :



Dapat dilihat bahwa saya bisa login akun admin dengan password yang tadi di attack pada aplikasi burpsuite.

Link :

[https://youtu.be/ebi\\_izN6vNA](https://youtu.be/ebi_izN6vNA)