

**Instalasi OWASP Juice Shop  
Praktikum Keamanan Jaringan**



Dosen Pembimbing :

Dr. Ferry Astika Saputra, ST., M.Sc.

Disusun Oleh :

Lula Rania Salsabilla (3122640045)

**1 D4 – IT B LJ**

**D4 TEKNIK INFORMATIKA**

**DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER**

**POLITEKNIK ELEKTRONIKA NEGERI SURABAYA**

**2023**

## **Broken Access Control**

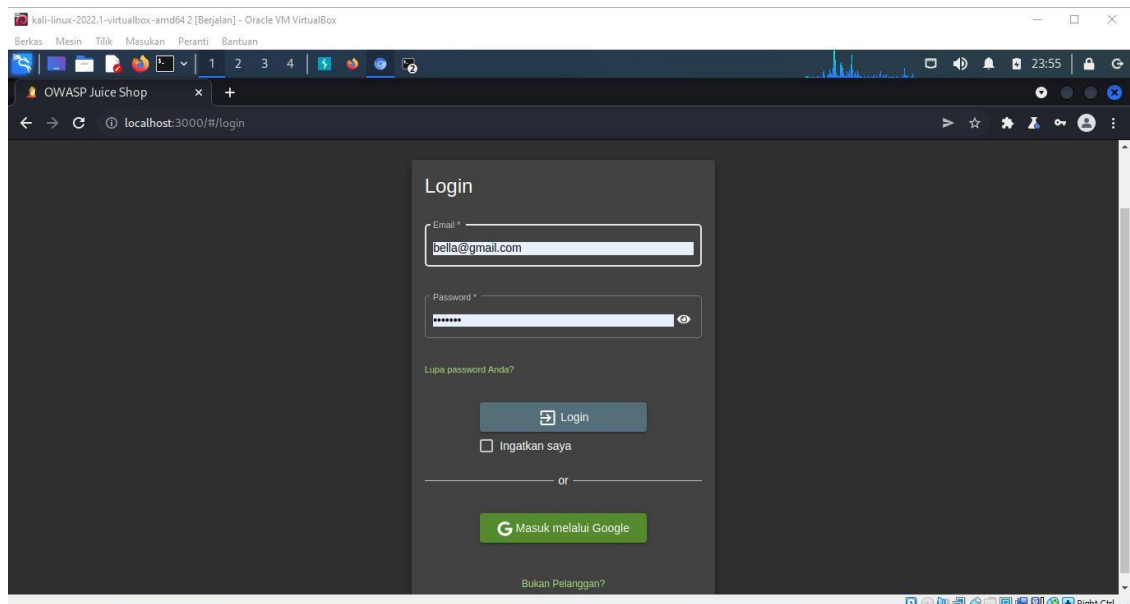
- **Informasi Dasar**

**Deskripsi :** Penyerang dan peretas 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.

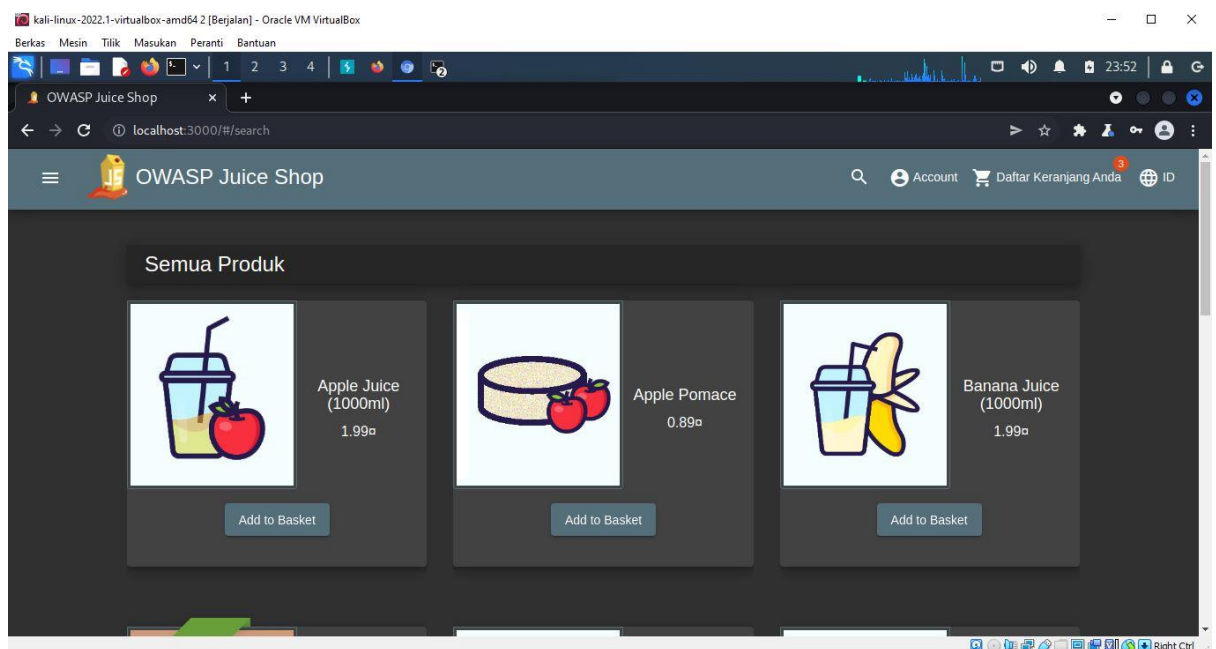
**Target Serangan :** Semua jenis Web Server, application server, dan web application rentan dan mudah untuk terkena beberapa permasalahan ini. Bahkan website yang hanya bersifat statis, jika tidak diatur dengan baik, dapat diretas oleh hacker, seperti akses terhadap file - file penting, deface, ataupun beberapa perbuatan merusak lainnya.

**Bagaimana cara mengetahui keamanan Access Control :** Semua website dipastikan membutuhkan access control. Oleh karena itu aturan dan desain nya sendiri harus secara jelas dan terdokumentasi. Jika tidak ada dokumentasi hampir dipastikan, website tersebut kemungkinan besar rentan. Code yang digunakan harus terstruktur, modular, dan sebagian besar terpusat. Review secara mendetail terhadap code harus dilakukan untuk memvalidasi keabsahan dari implementasi Access Control. Selain itu melakukan test dengan cara membobol code yang digunakan juga akan sangat membantu mengetahui ada atau tidaknya permasalahan pada Access Control.

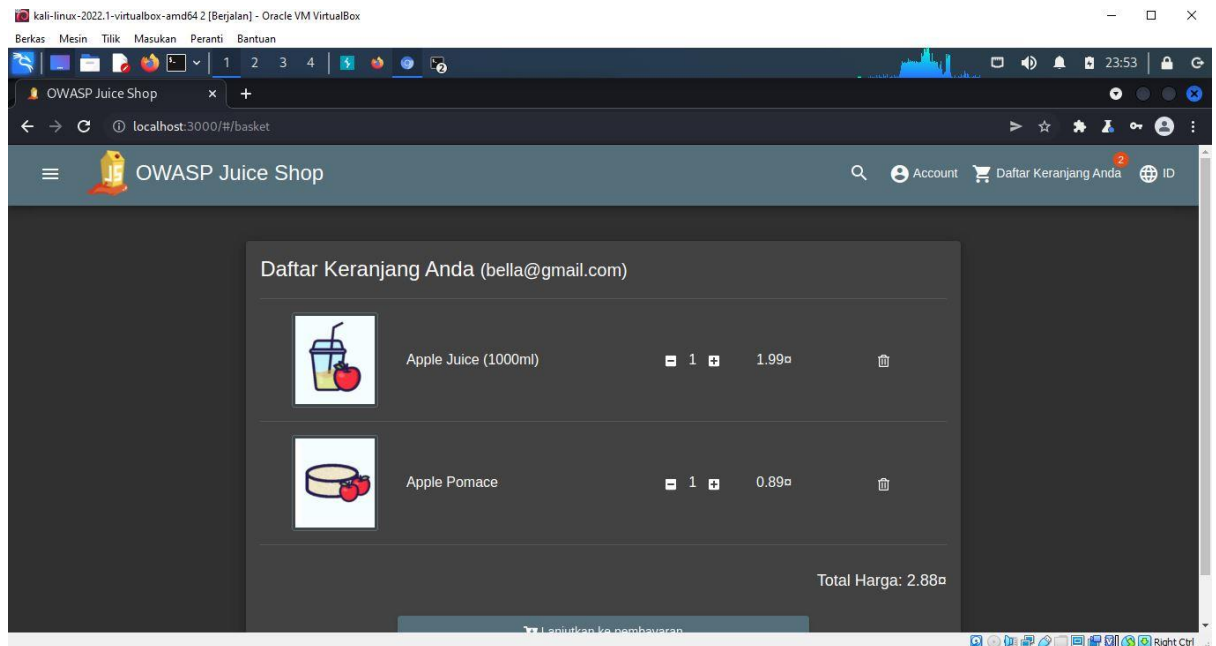
- Percobaan : Mengubah Isi Keranjang User
- Setelah melakukan pengaksesan localhost 3000 di terminal dan mempersiapkan aplikasi burpsuite di sini, saya melakukan login dengan menggunakan akun yang sudah di daftarkan sebelumnya.



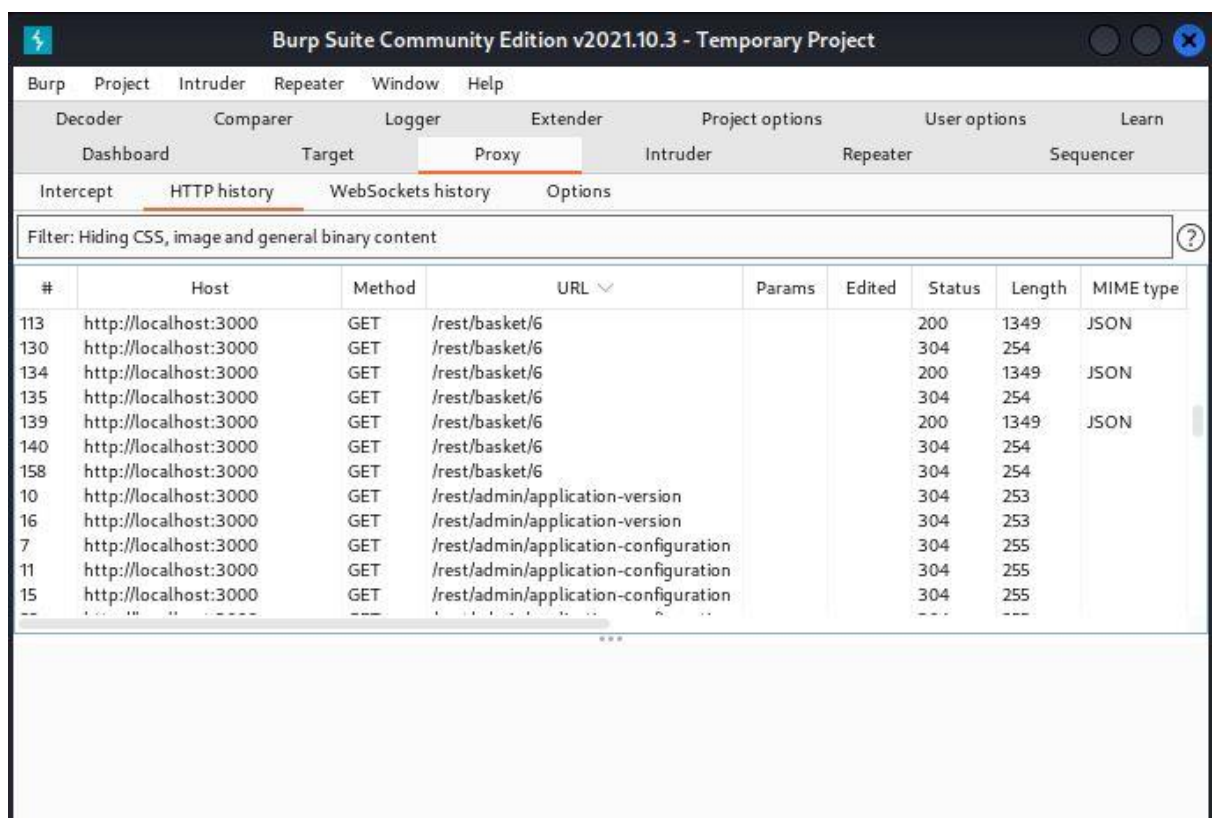
- Kemudian setelah melakukan proses login disini akan di arahkan ke halaman dashboard untuk dapat memilih beberapa item dan nantinya akan disimpan ke keranjang.



- Kemudian menuju halaman keranjang untuk dapat melihat yang telah ditambahkan yaitu aple juice dan apple pomance masing masing 1 buah.

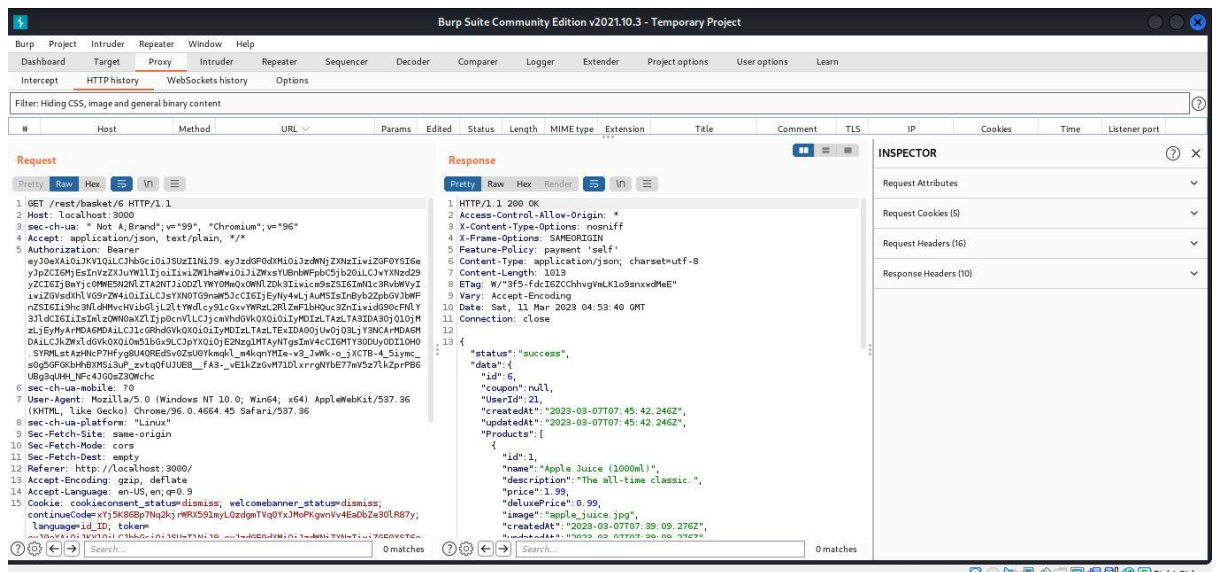


- Kemudian disini saya membuka halaman proxy di dalam http history untuk melihat track http history. Terdapat informasi host, method, url, status, length dan informasi pendukung lainnya.

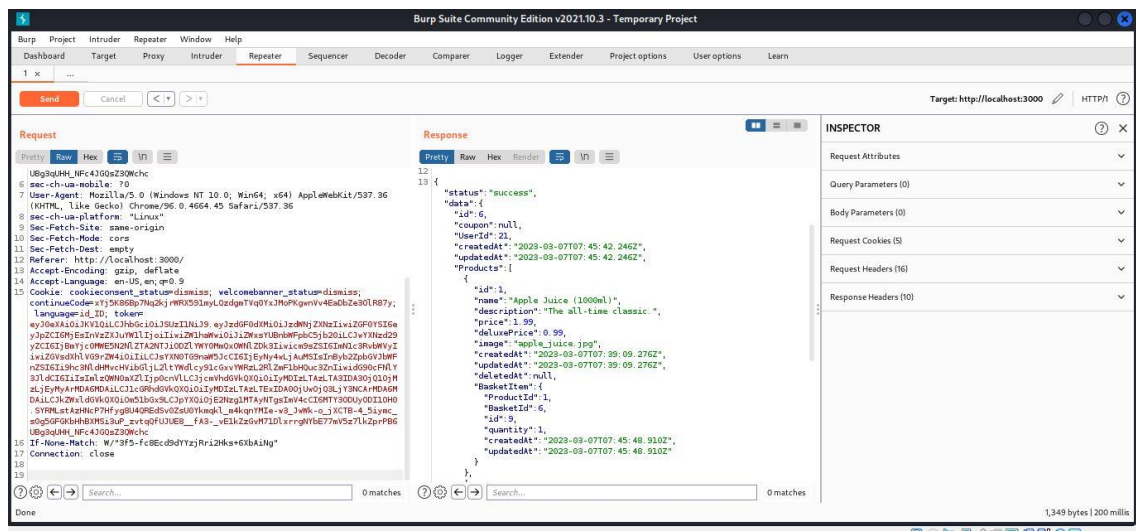


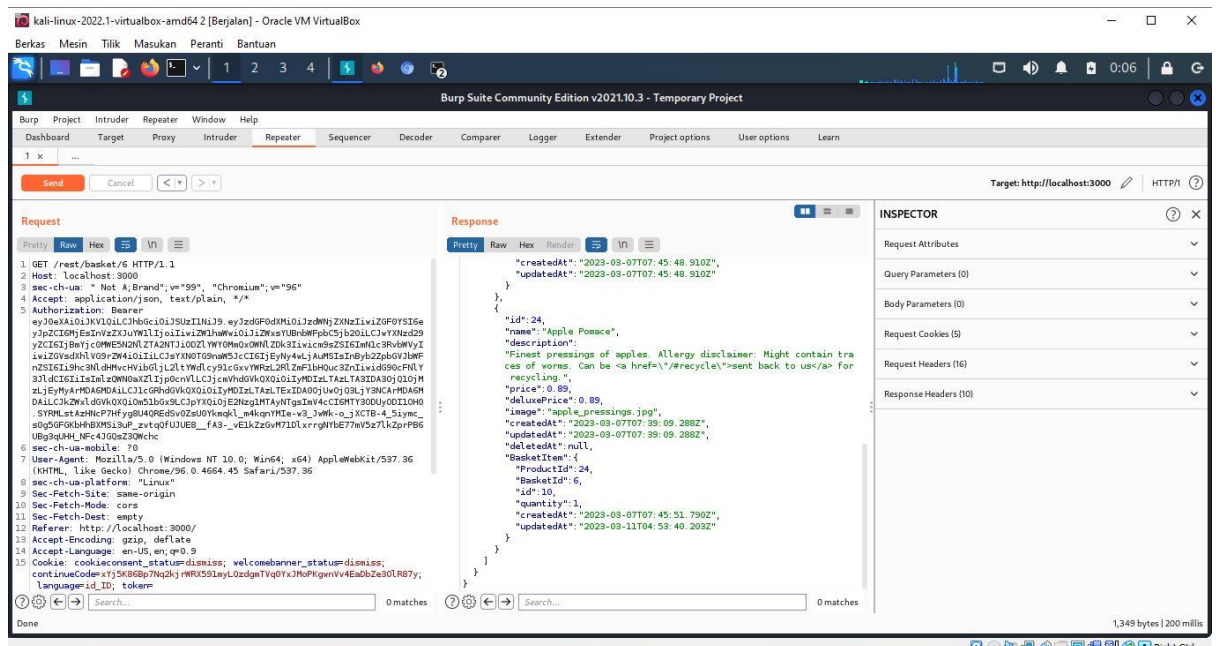
- Kemudian setelah itu saya pilih http history yang memiliki params json dengan get /rest/basket/6. Kemudian saya lihat mengenai request dan response yang tertampil di halaman tersebut. Dimana response berisi informasi isi keranjang yang telah saya pilih

sebelumnya.

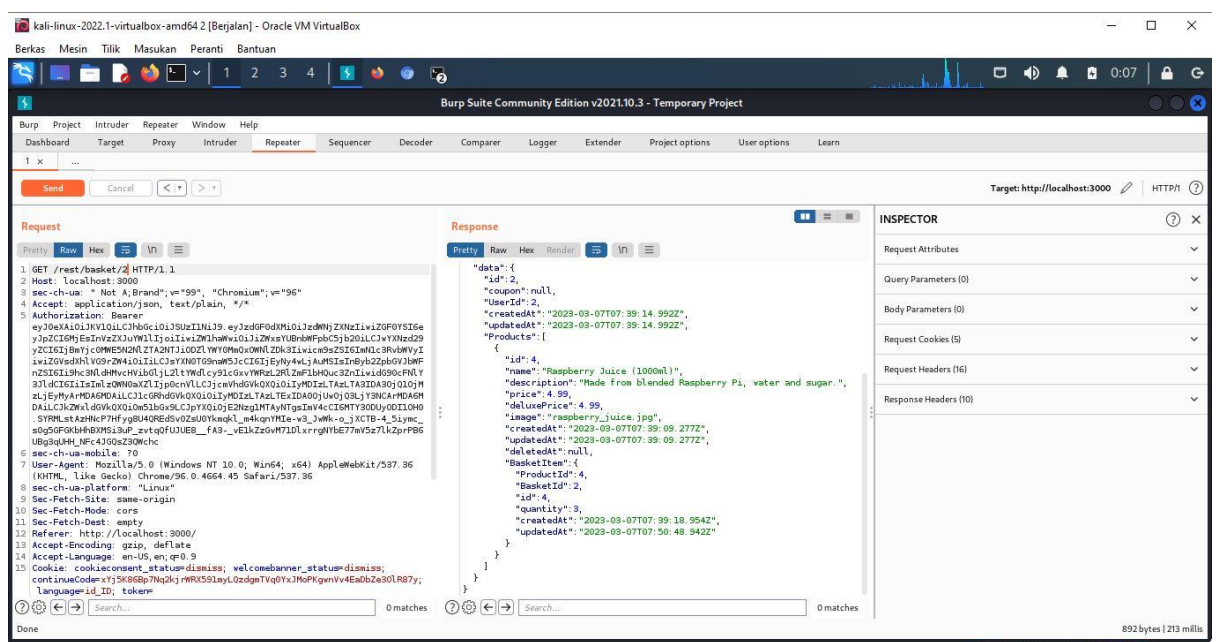


- Kemudian saya pindahkan list request yang saya amati sebelumnya menuju repeater, kemudian saya send dan pada response terlihat data keranjang yang sudah sesuai dengan apa yang diinputkan sebelumnya.



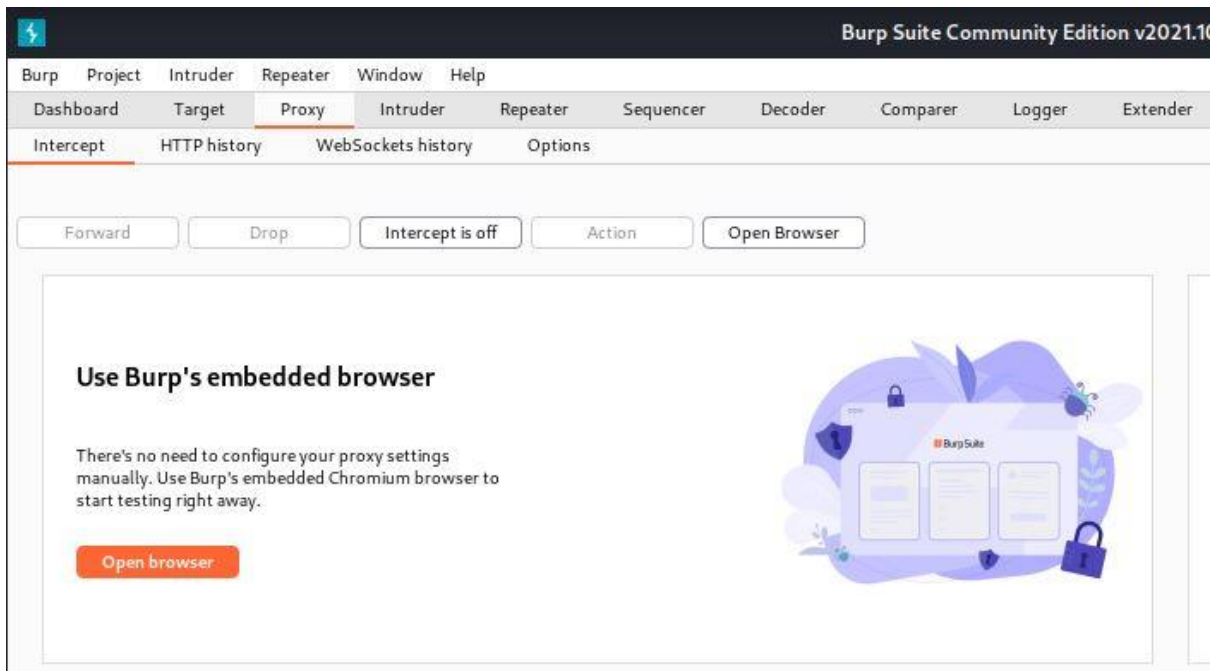


- Setelah melihat informasi response di repeater, saya mencoba untuk mengganti data id 6 menjadi 2 untuk melihat apakah terdapat perubahan yang ditampilkan response. Dan ternyata response memberikan informasi berbeda dari sebelumnya yang mana ternyata menunjukkan isi keranjang id 2.

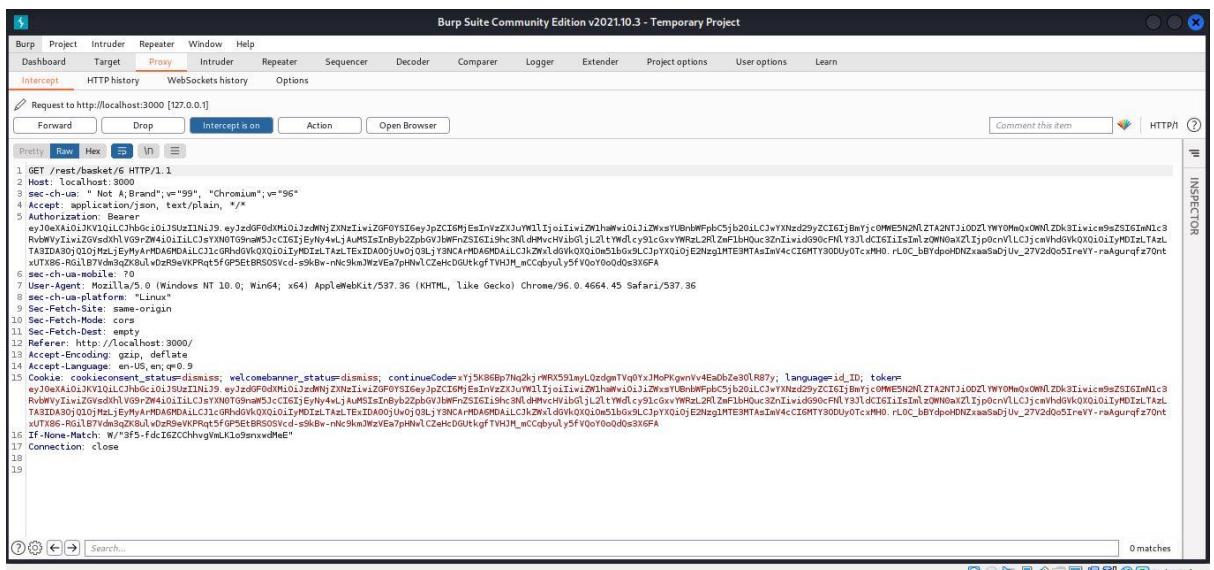


- Kemudian disini saya akan menggunakan fitur intercept untuk menampilkan data keranjang user lain di dalam website owasp juice shop. Dimana saya merubah status intercept yang tadinya off menjadi on.

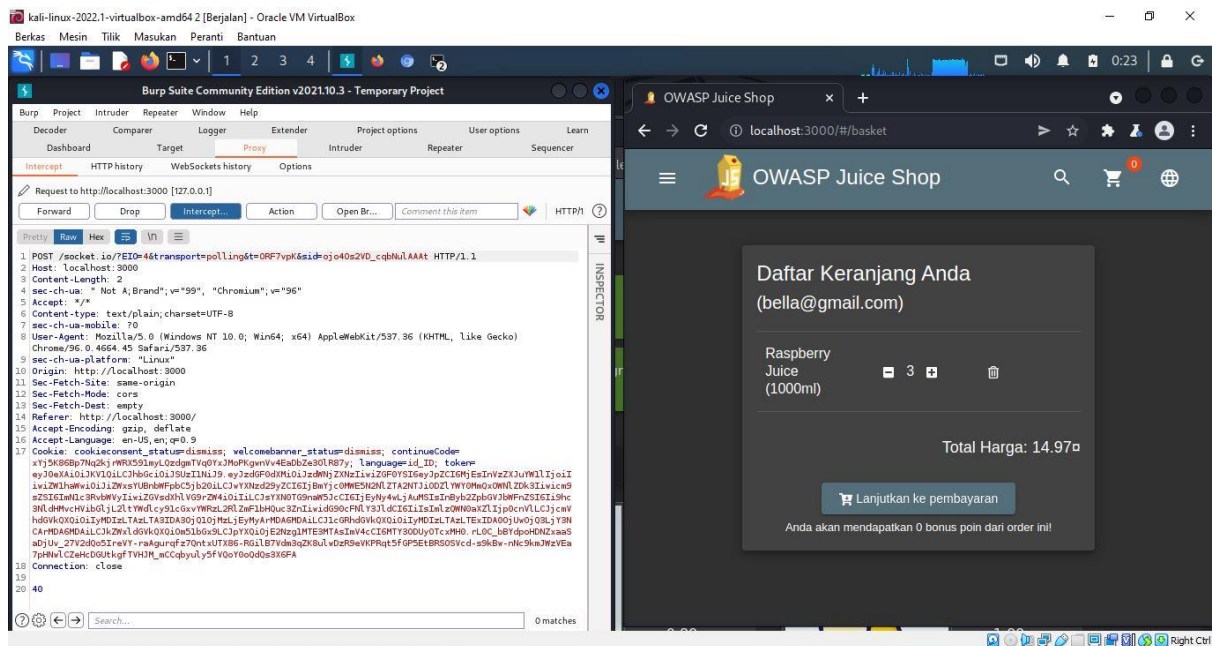




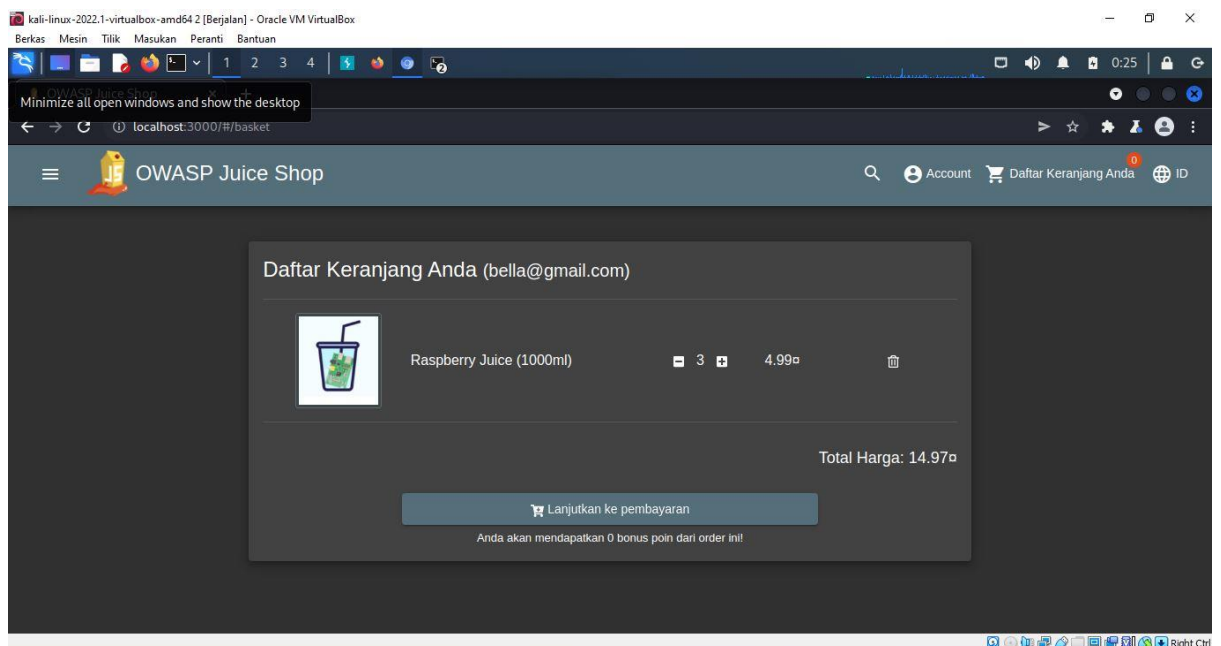
- Ketika intercept on disini terdapat baris informasi request terkait owasp juice shop. Kemudian saya forward data tersebut hingga menemukan data get /rest/basket/6, kemudian saya ganti data uuiidnya dengan id lain selain id 6 kemudian saya forward kembali informasi tersebut.



- Website berhasil menampilkan isi keranjang pengguna lainnya berikut adalah isi keranjang pengguna : id (2).

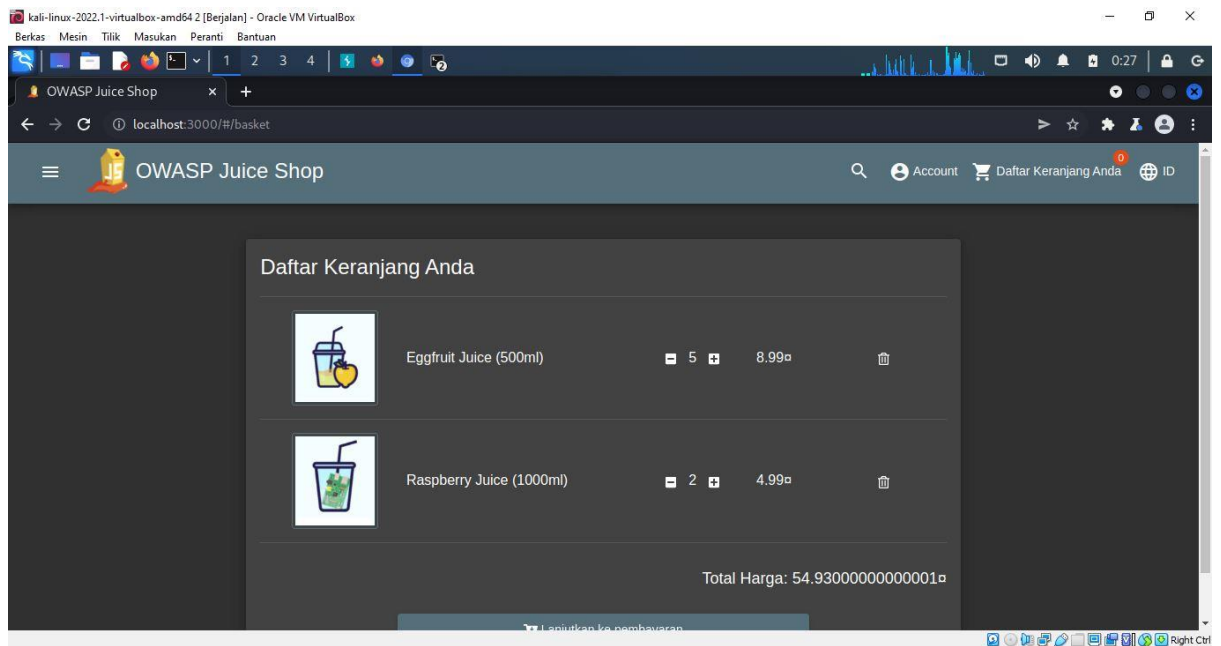


- Website berhasil menampilkan isi keranjang pengguna lainnya berikut adalah isi keranjang pengguna : id (4).

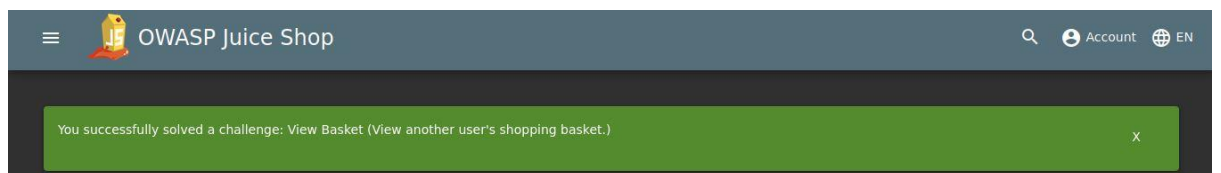


- Website berhasil menampilkan isi keranjang pengguna lainnya berikut adalah isi keranjang pengguna : id (5).

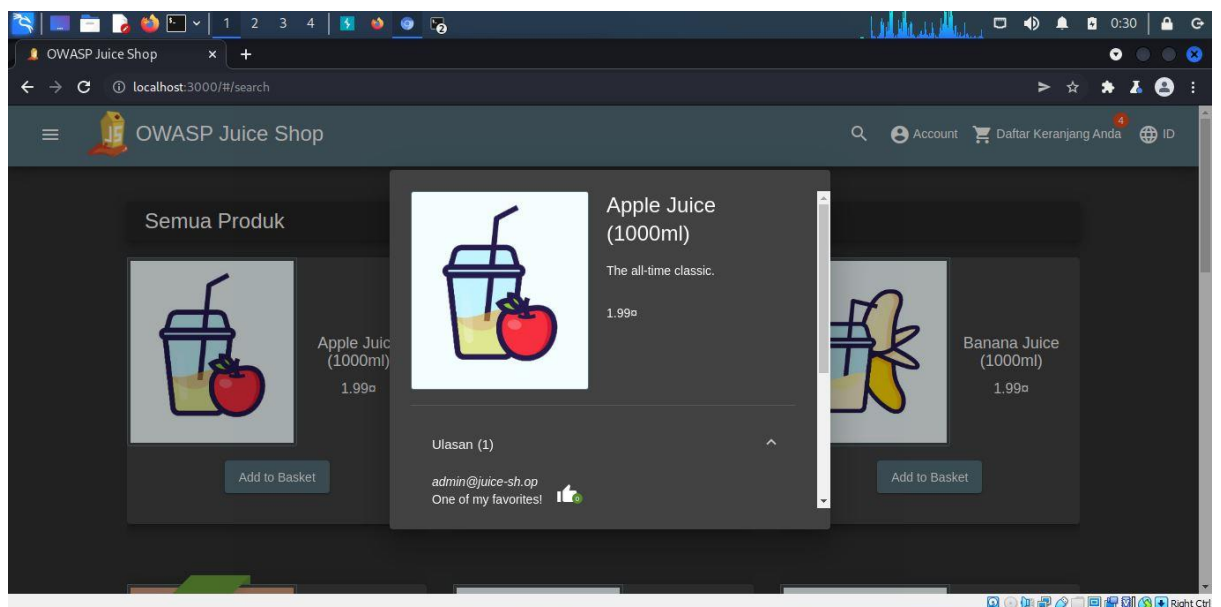




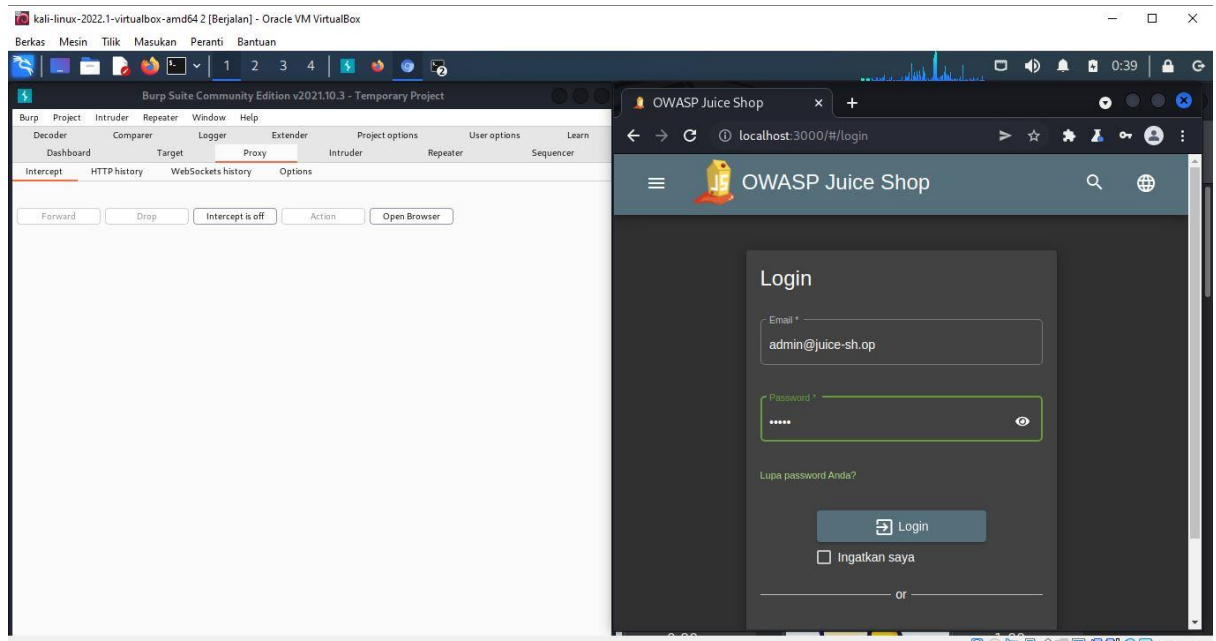
- Disini saya sudah berhasil untuk melakukan challenge melihat keranjang orang lain.



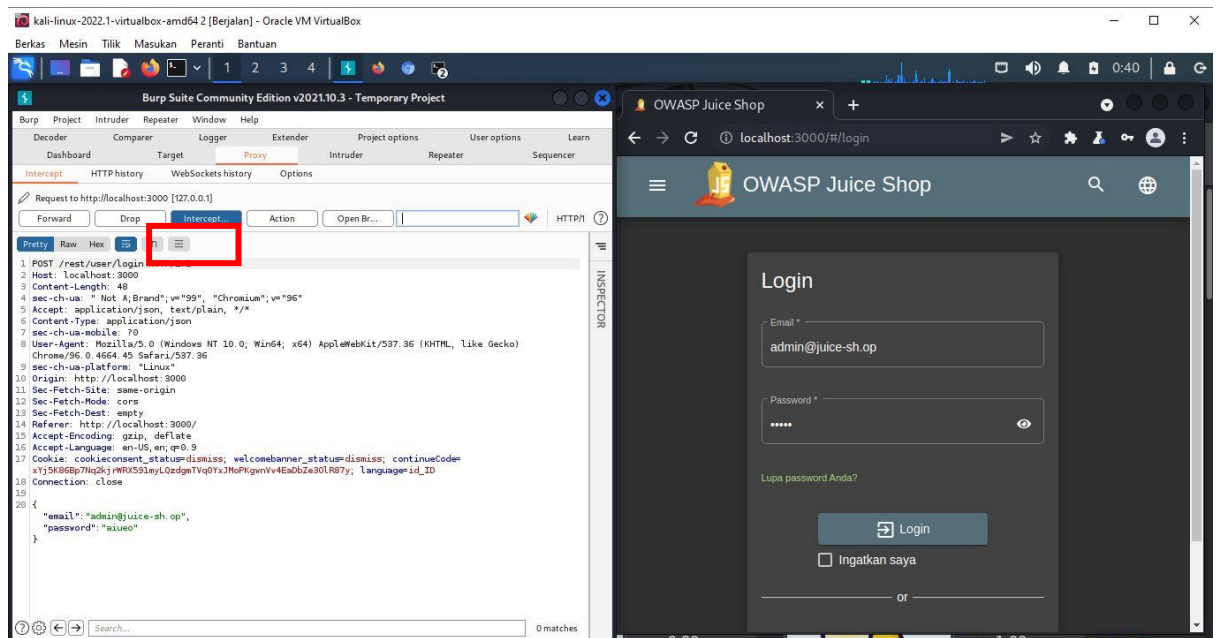
- Percobaan : Login Admin
- Disini saya bermaksud ingin mencari data email, yang mana ditemukan di komentar ulasan. Dimana ada informasi email admin disana.



- Kemudian saya melakukan login dengan menggunakan password dummy, namun sebelumnya saya melakukan perubahan status menjadi on di intercept.

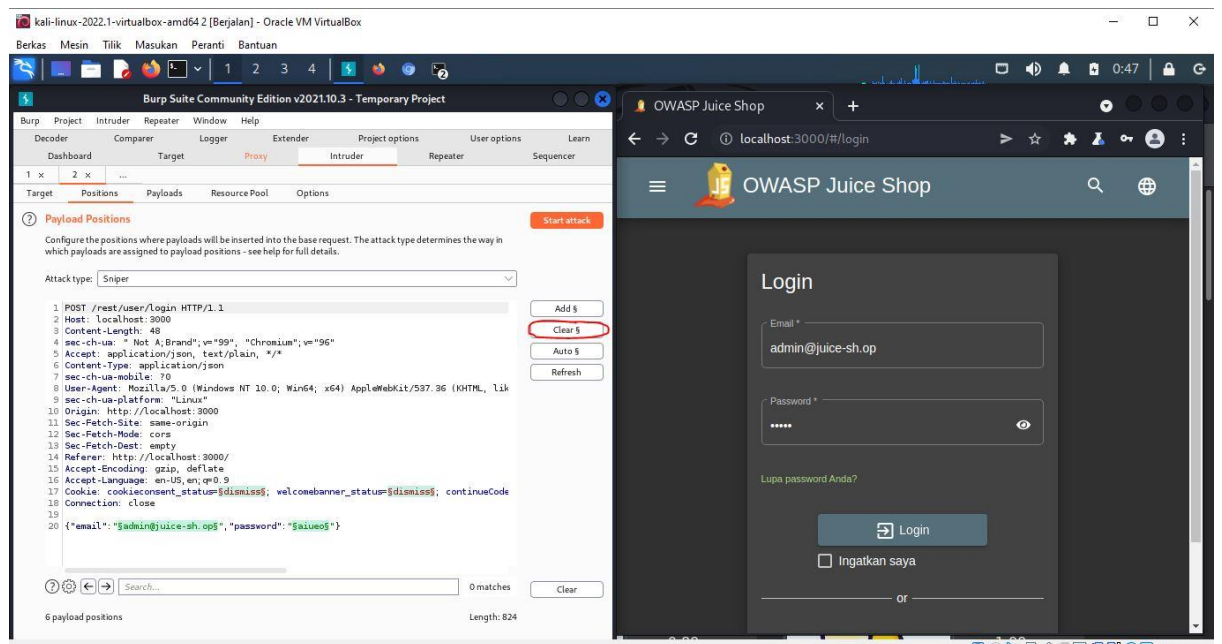


- Ketika melakukan submit login, intercept memberikan informasi berupa baris informasi yang mana memuat email dan password.
- Kemudian setelah melihat informasi tersebut, saya menggunakan ikon yang dikotaki warna merah untuk melakukan pengiriman menuju intruder, positions.

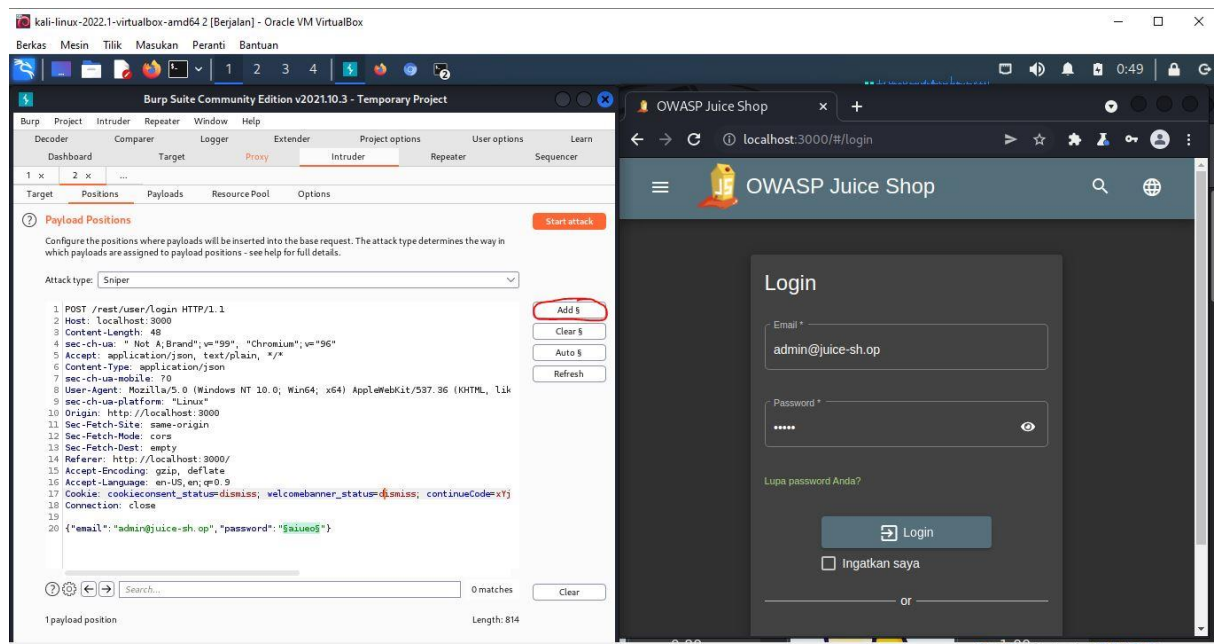


- Kemudian kita berpindah ke halaman intruder, positions dan melihat data informasi yang ada disana, kemudian klik clear. Ada penambahan beberapa data ketika proses melakukan clear

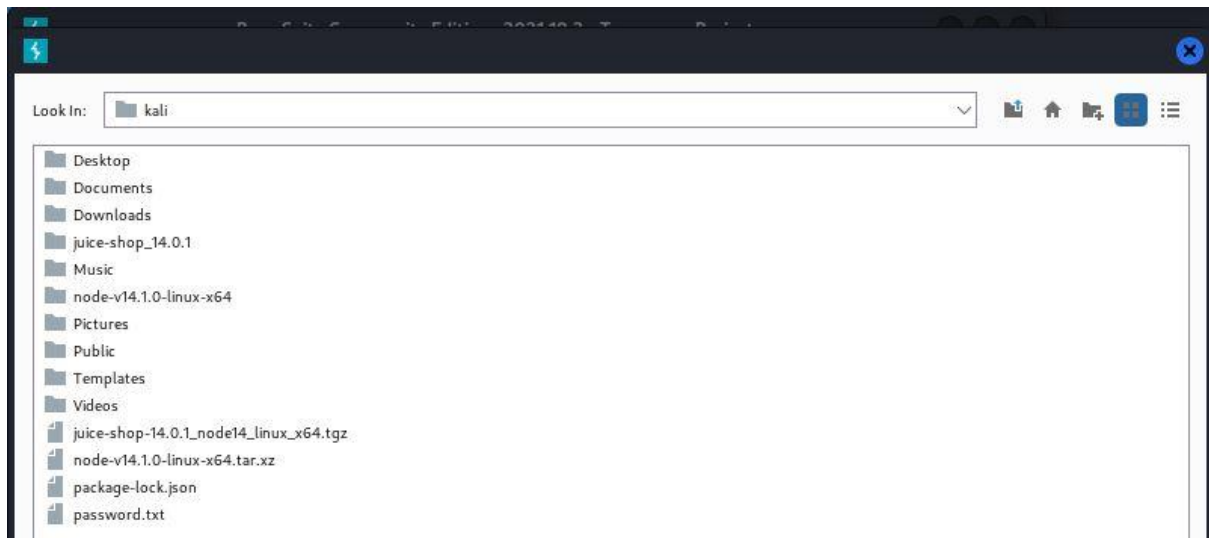
data.



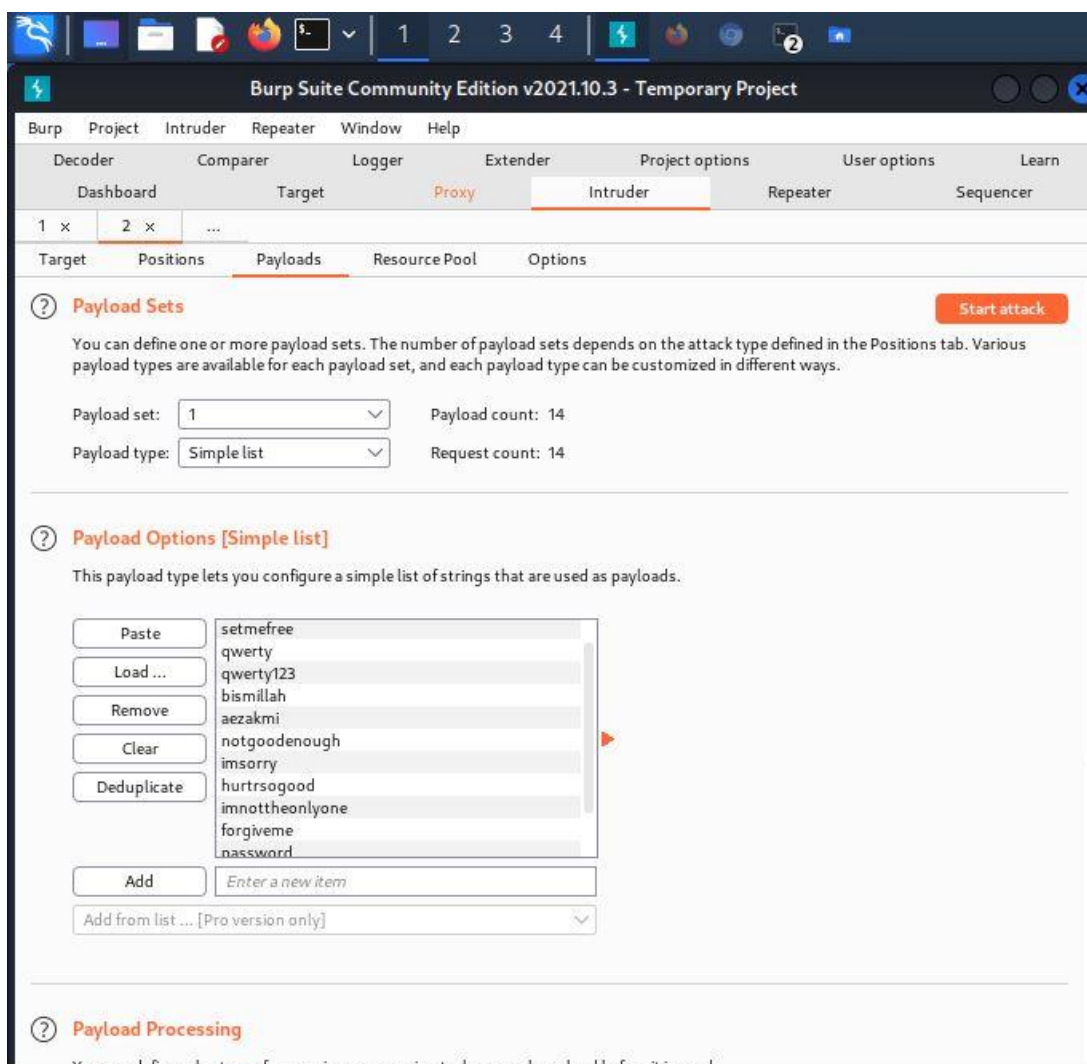
- Kemudian klik add, yang mana dalam hal ini akan membuat data email memiliki tambahan sign dollar didepannya. Hal ini membuat adanya perubahan yang ada.



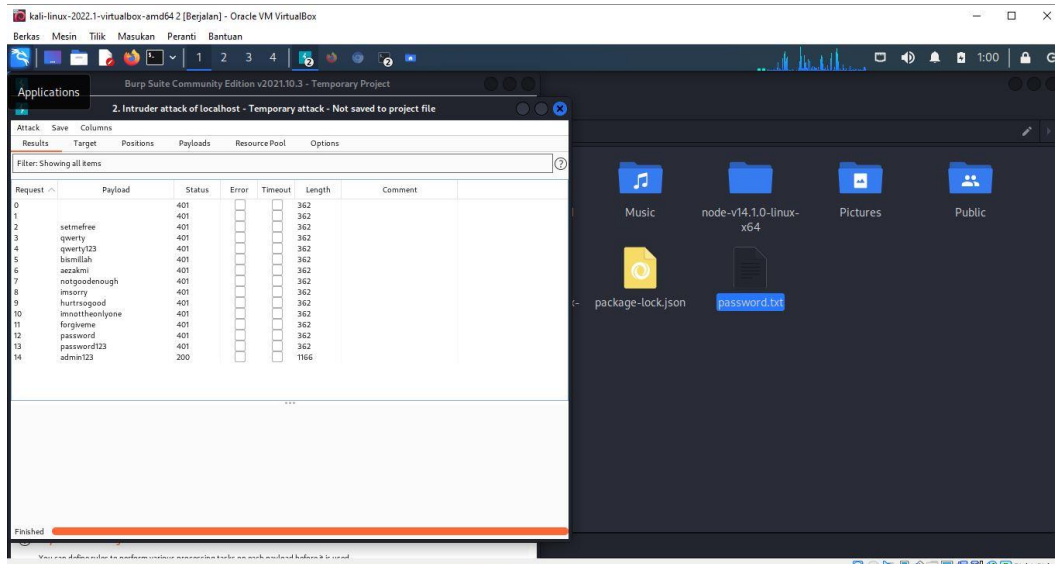
- Proses berikutnya saya menuju ke payloads dan melakukan load data file password.txt yang sebelumnya sudah dibuat.



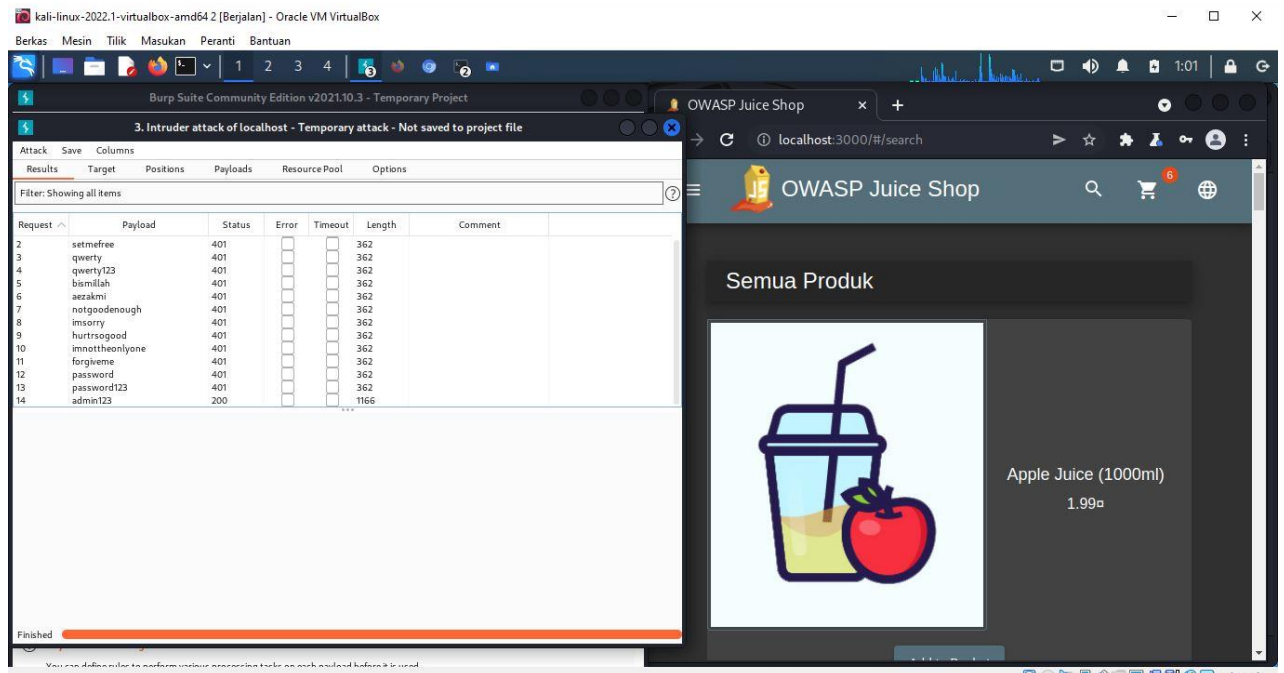
- Setelah itu kemudian data yang diinputkan pada txt akan muncul di dalam kotak putih sebagai list data password, kemudian klik button start attack.

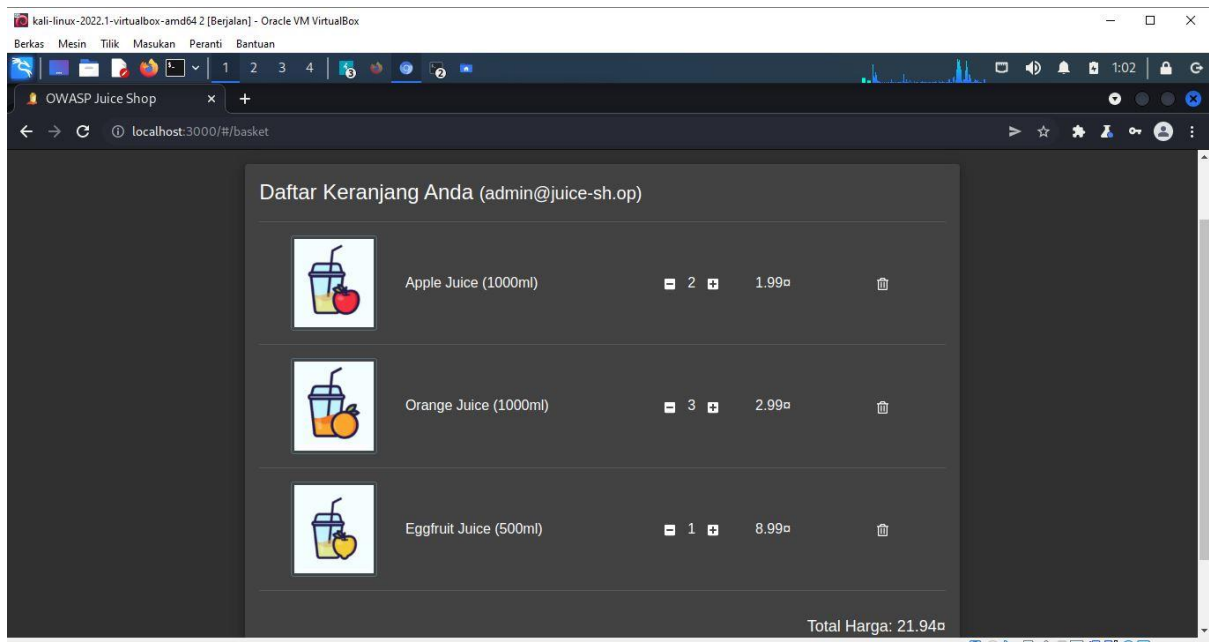
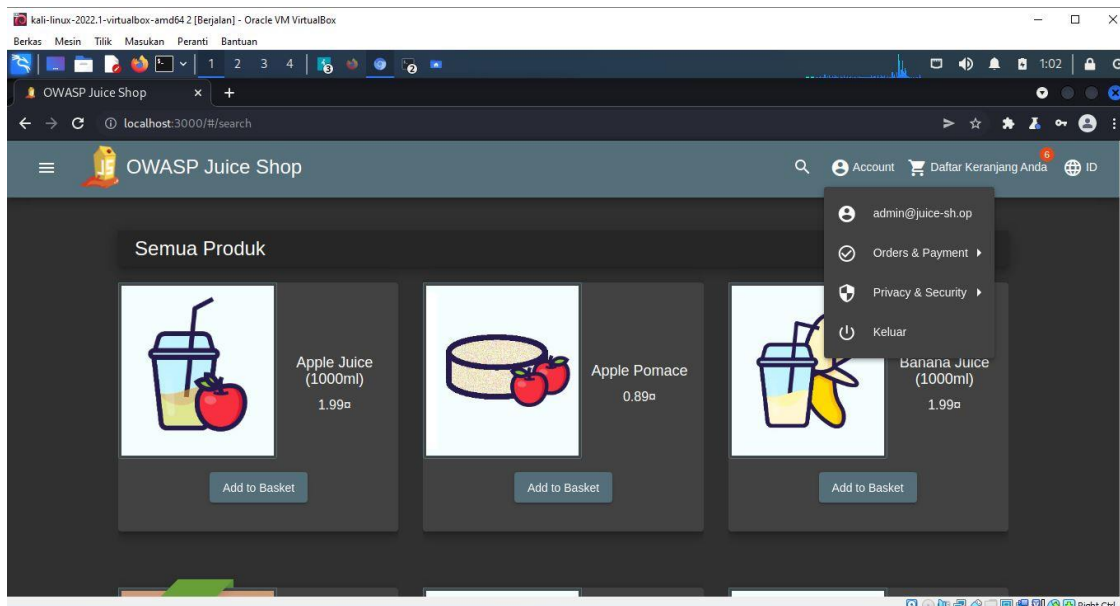


- Setelah itu, akan tertampil sebuah moodal yang menampilkan list password yang dicoba sebelumnya, dan memuat informasi status dan length dan data lain. Disini semua 400 hasilnya kecuali data terakhir “admin123” yang memiliki status 200.



- Kemudian saya mencoba untuk login menggunakan “admin123” disini saya berhasil untuk login sebagai admin dan dapat mengakses keranjang serta profile dari akun admin yang ada di dalam owasp juice shop.





## Kesimpulan

Disini saya berhasil membuktikan bahwa website owasp juice shop ini masih memiliki kerentanan yang mana disebutkan dalam owasp 10 yakni broken access control dimana saya dapat melihat keranjang dari user lain dan login sebagai admin padahal saya tidak terdaftar dan belum mengetahui password admin sebelumnya.