

KEAMANAN JARINGAN

Praktikum Broken Anti Automation



Disusun Oleh :

Choirun Annas 3122640032

Muhammad Dzaky Mahfuzh 3122640050

D4 LJ B

Teknik Informatika

Politeknik Elektronika Negeri Surabaya

Kampus ITS Keputih Sukolilo Surabaya 60111

Telp. 031-5947280, 031-5946114, Fax:031-5946114

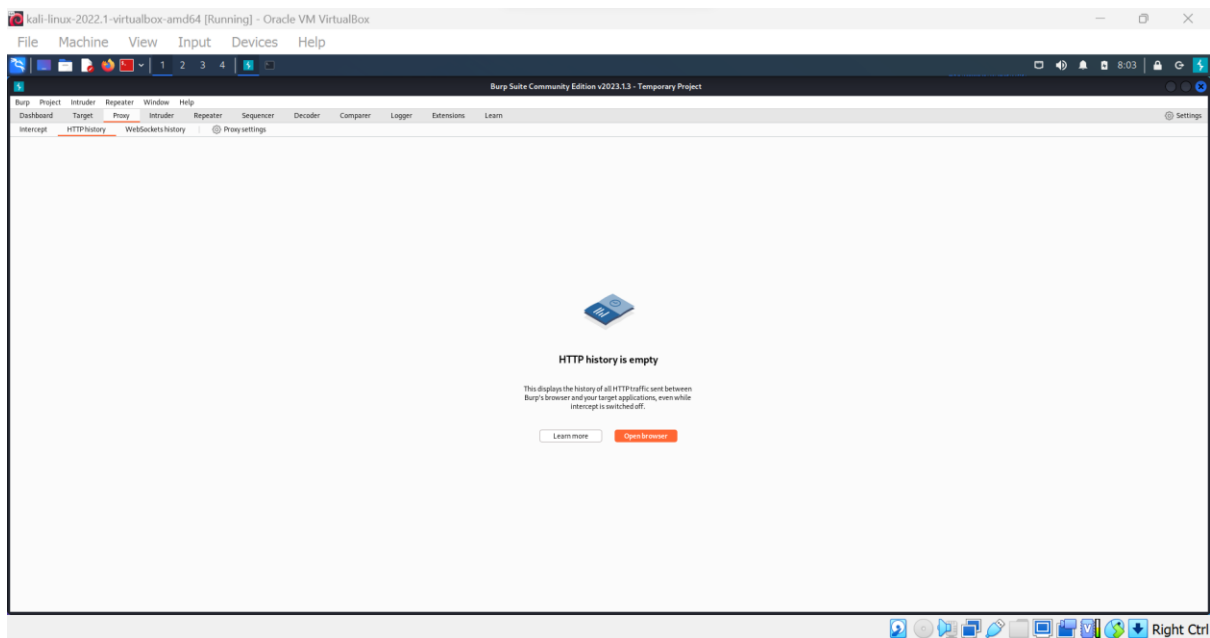
Laporan Praktikum

Broken Anti Automation

Broken Anti Automation merupakan penggunaan otomatis web yang tidak diinginkan seringkali berhubungan dengan penyalahgunaan fungsionalitas valid yang melekat, daripada upaya eksploitasi kerentanan yang tidak dikurangi. Juga, penyalahgunaan yang berlebihan biasanya keliru dilaporkan sebagai penolakan layanan aplikasi (DoS) seperti HTTP-flooding,

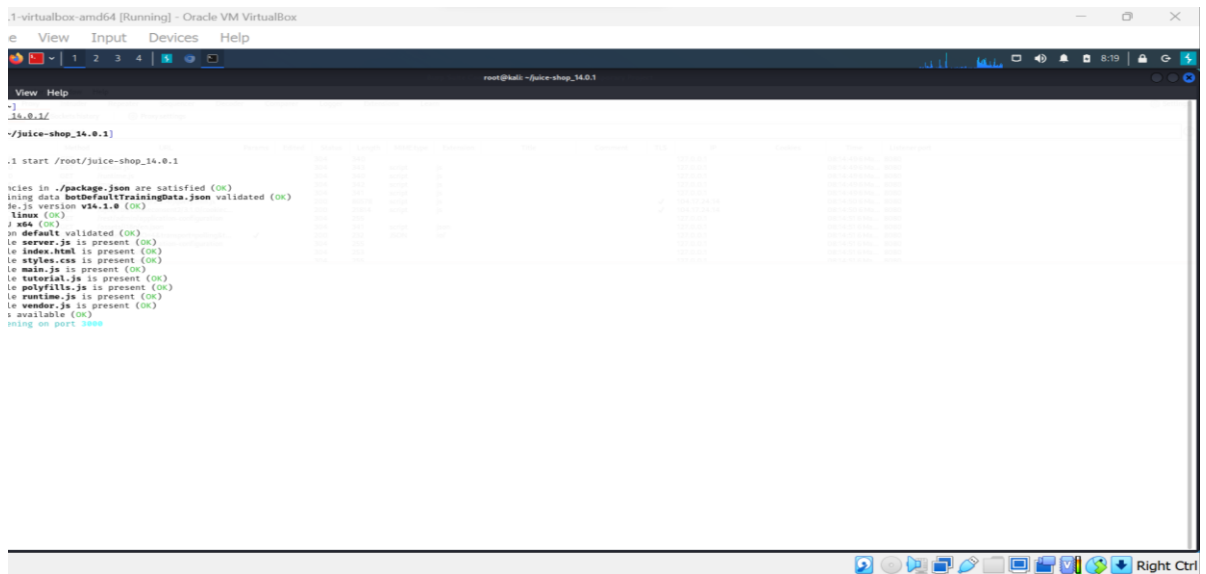
CAPTCHA Bypass

1. Buka burp suite kemudian open browser



Pada percobaan install burp suite . Burp suite merupakan tools ini digunakan untuk meng-intercept data yang dikirim (request) atau diterima (response) oleh aplikasi atau browser dari server melalui jalur proxy yang sudah disetting pada browser maupun pada android atau ios. Sehingga seorang hacker dapat melakukan manipulasi data yang dikirim maupun yang diterima oleh browser atau mobile apps. Selain itu juga tools ini juga dilengkapi dengan semi automasi dalam menemukan celah pada suatu aplikasi website.

2. Ketik npm start pada terminal untuk



```
.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
e View Input Devices Help

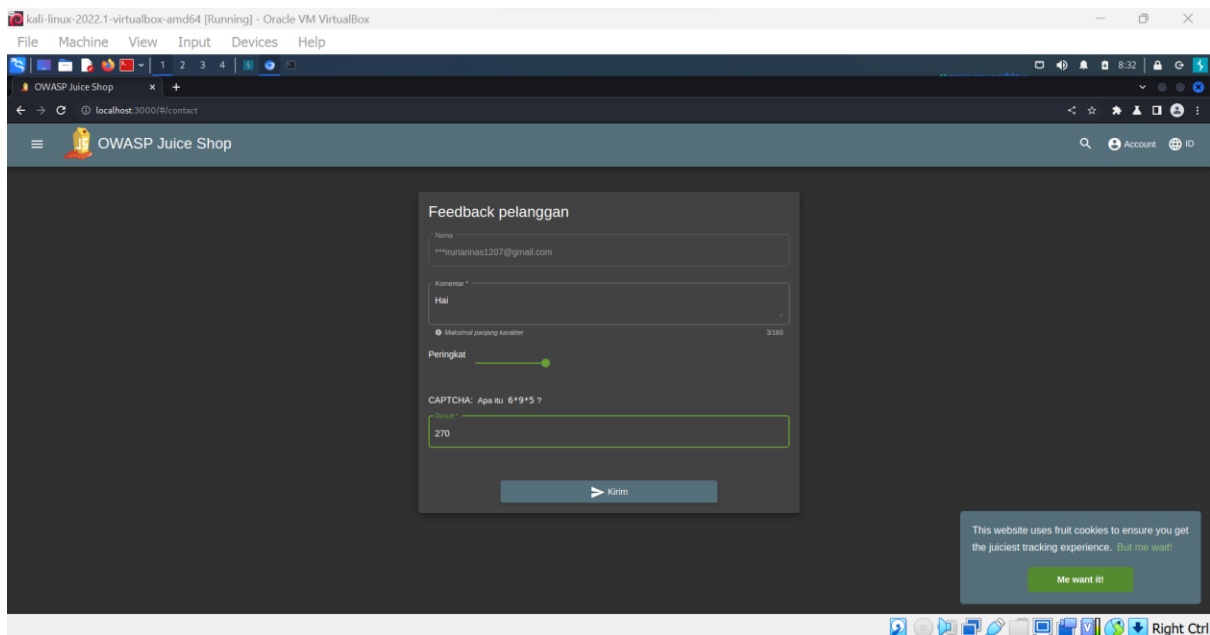
root@kali: ~/juice-shop_14.0.1

~/juice-shop_14.0.1
.1 start /root/juice-shop_14.0.1

files in ./package.json are satisfied (OK)
initial data botDefaultTrainingData.json validated (OK)
Node.js version v14.1.0 (OK)
time (OK)
in default validated (OK)
JSS4 (OK)
le server.js is present (OK)
le index.html is present (OK)
le styles.css is present (OK)
le main.js is present (OK)
le tutorial.js is present (OK)
le polyfills.js is present (OK)
le runtime.js is present (OK)
le vendor.js is present (OK)
s available (OK)
ning on port 3000
```

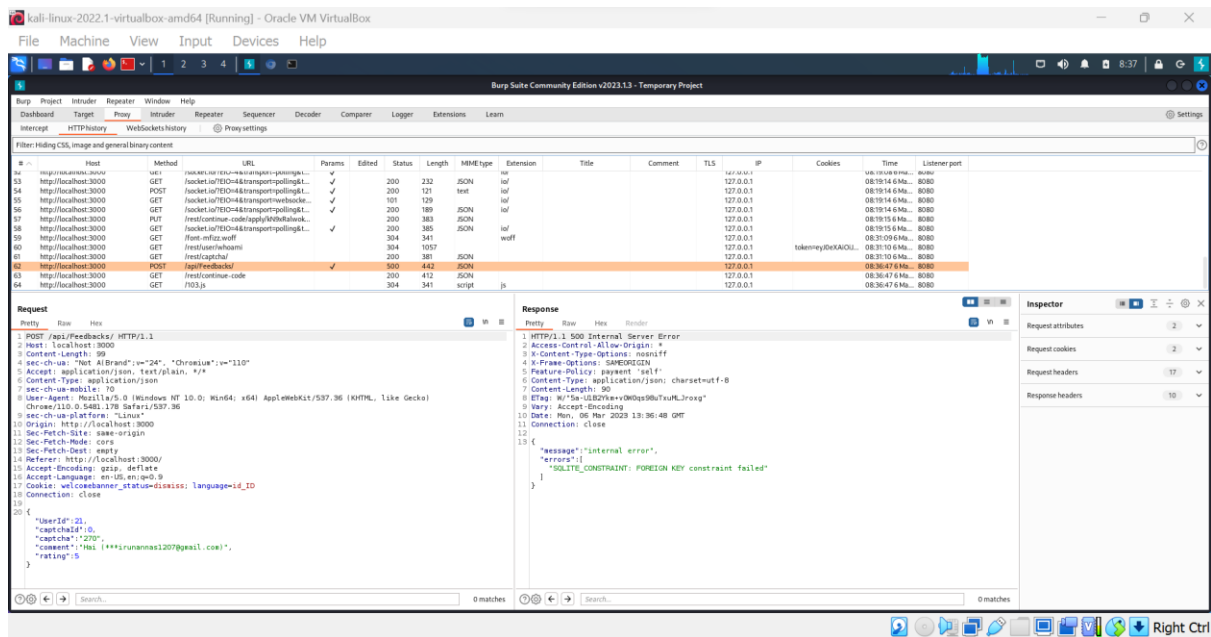
Sebelum melakukan perintah npm start masuk ke folder juice shop dengan mengetik ls maka akan muncul nama folder kemudian ketik cd <nama folder> maka akan masuk ke direktori folder juice shop.

3. Buka Juice Shop pada browser burp suite feedback



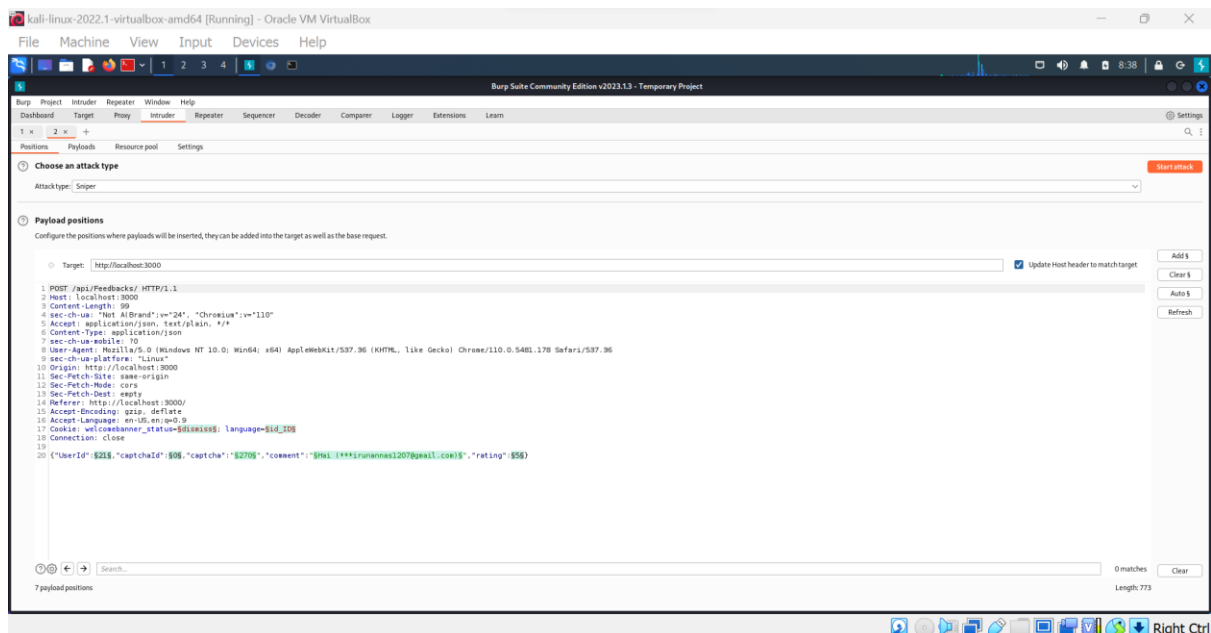
Pada tahap ini lakukan percobaan mengisi feedback. Kemudian isi CAPTCHA dan klik kirim. Fungsinya untuk mengirimkan history feedback agar muncul ke burpsuite.

4. Buka burp suite cari history feedback



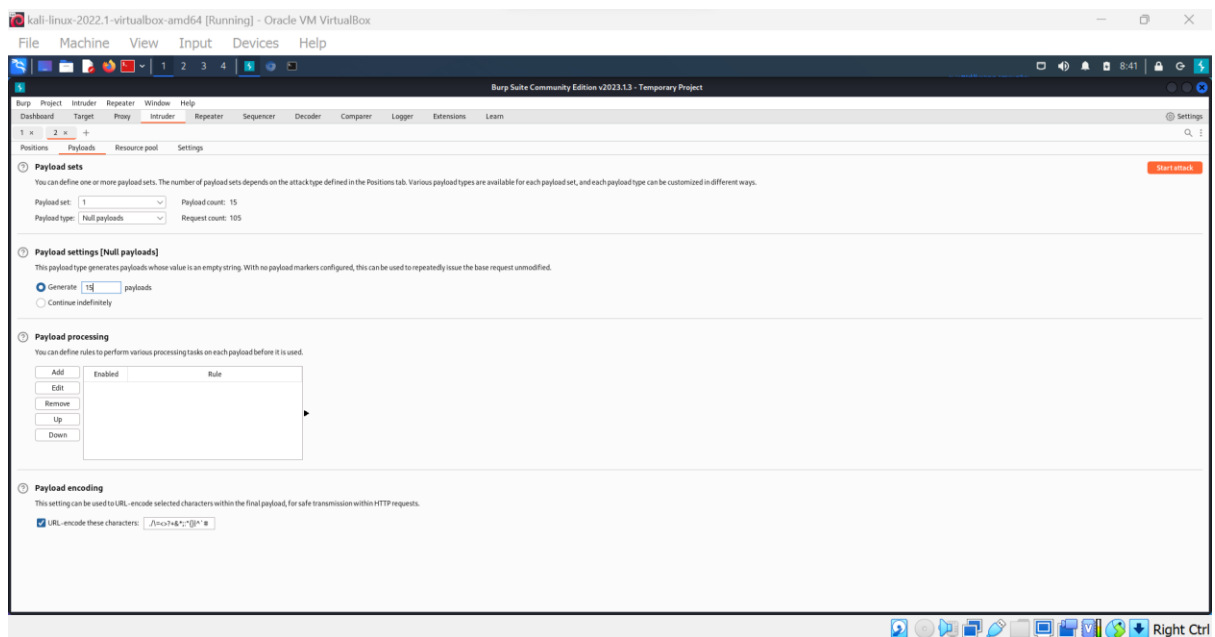
Pada proses ini cari pada HTTP history feedback yang kalian kirimkan seperti gambar diatas. Jadi feedback yang telah kita inputkan akan muncul pada history proxy di burp suite.

5. Send ke intruder



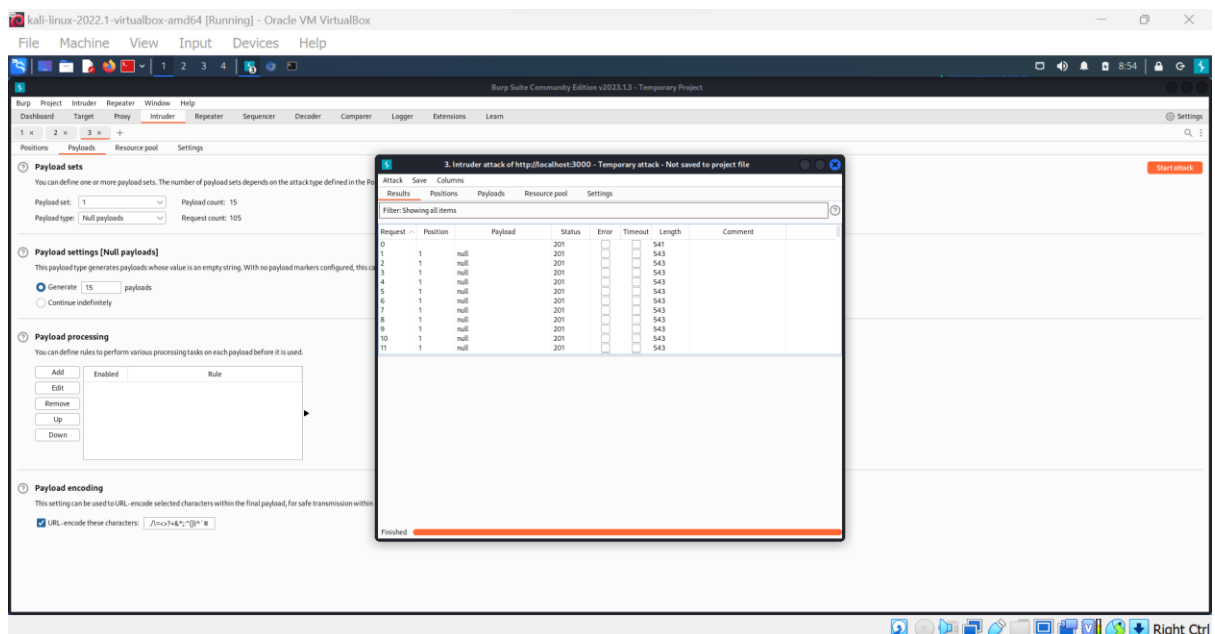
Burp Intruder merupakan untuk mengotomatisasi serangan khusus terhadap aplikasi web. Ini memungkinkan Anda mengonfigurasi serangan yang mengirim permintaan HTTP yang sama berulang kali, memasukkan muatan yang berbeda ke posisi yang telah ditentukan setiap saat.

6. Atur Intruder Payloads



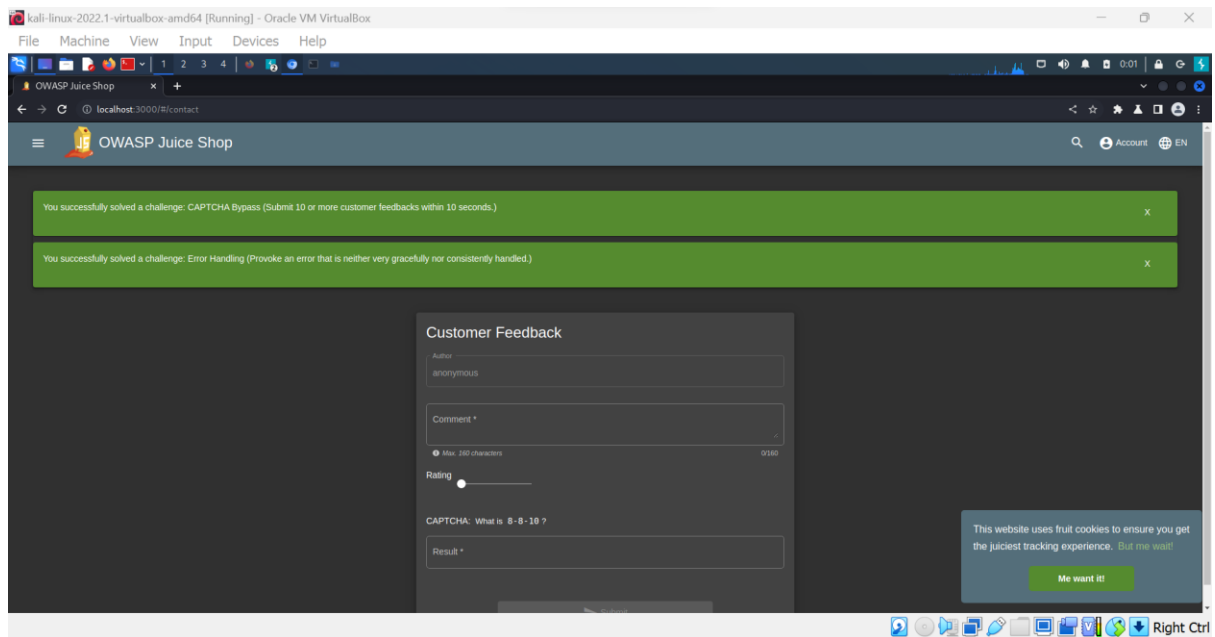
Ini memungkinkan Anda menghasilkan payloads dengan panjang tertentu yang berisi semua permutasi dari rangkaian karakter tertentu. Disini kami mengatur payloads ke 15.

7. Klik Start Attack



Informational responses (100 – 199), Successful responses (200 – 299), Redirection messages(Pengalihan) (300 – 399), Client error responses (400 – 499), Server error responses (500 – 599) Status 201 berarti respon sukses.

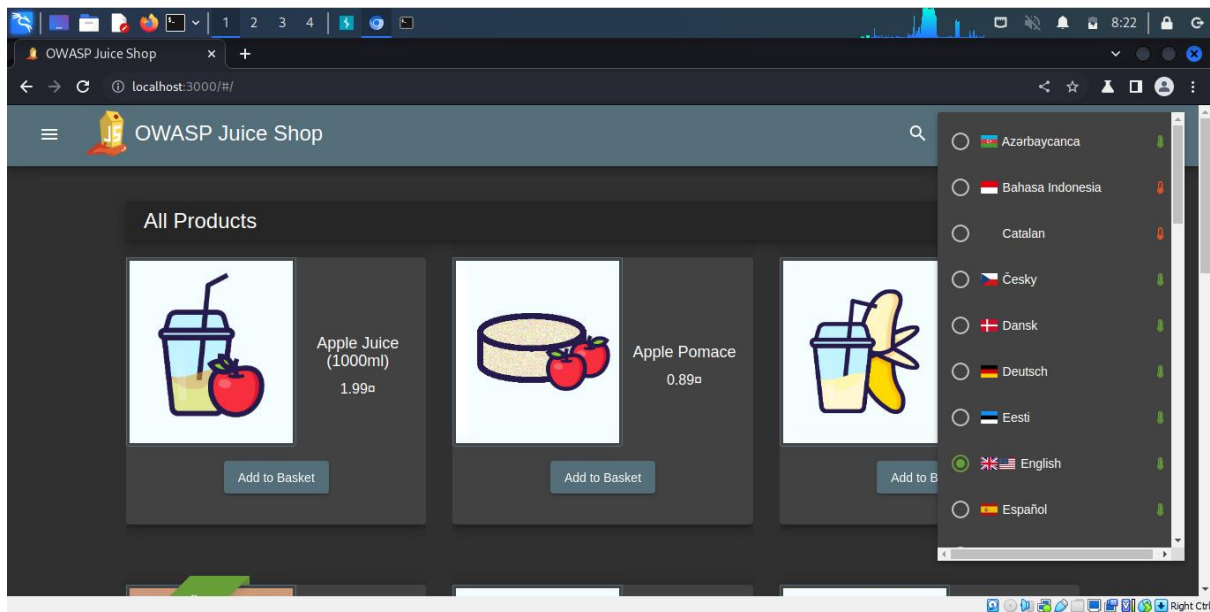
8. Tampilan Ketika Berhasil



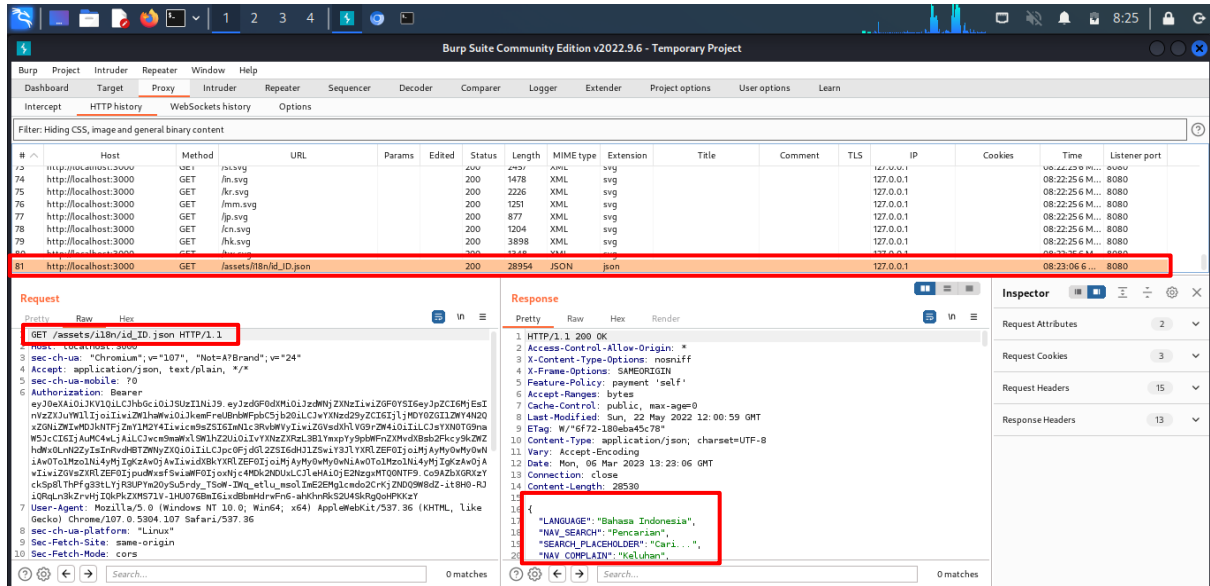
Jika berhasil maka pada web juice shop akan muncul notifikasi percobaan chaptcha bypass sukses mengirimkan 10 feedback user dalam 10 detik.

EXTRA LANGUAGE

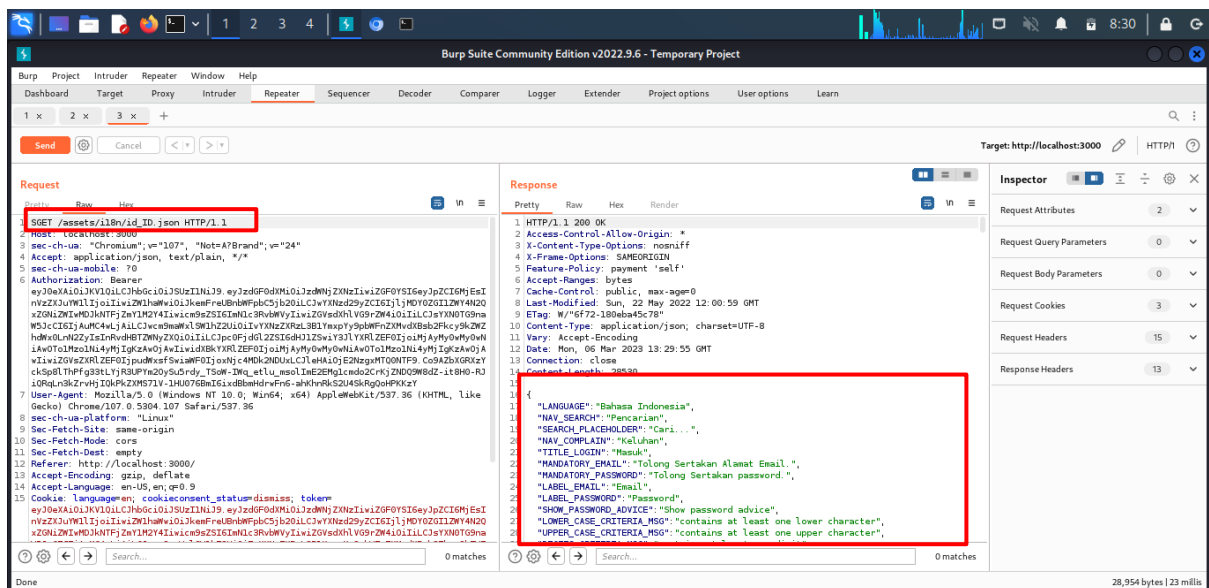
1. pertama masuk ke halaman juice shop, lalu cari menu pilih bahasa. silahkan pilih bahasa sesuai preferensi masing masing.



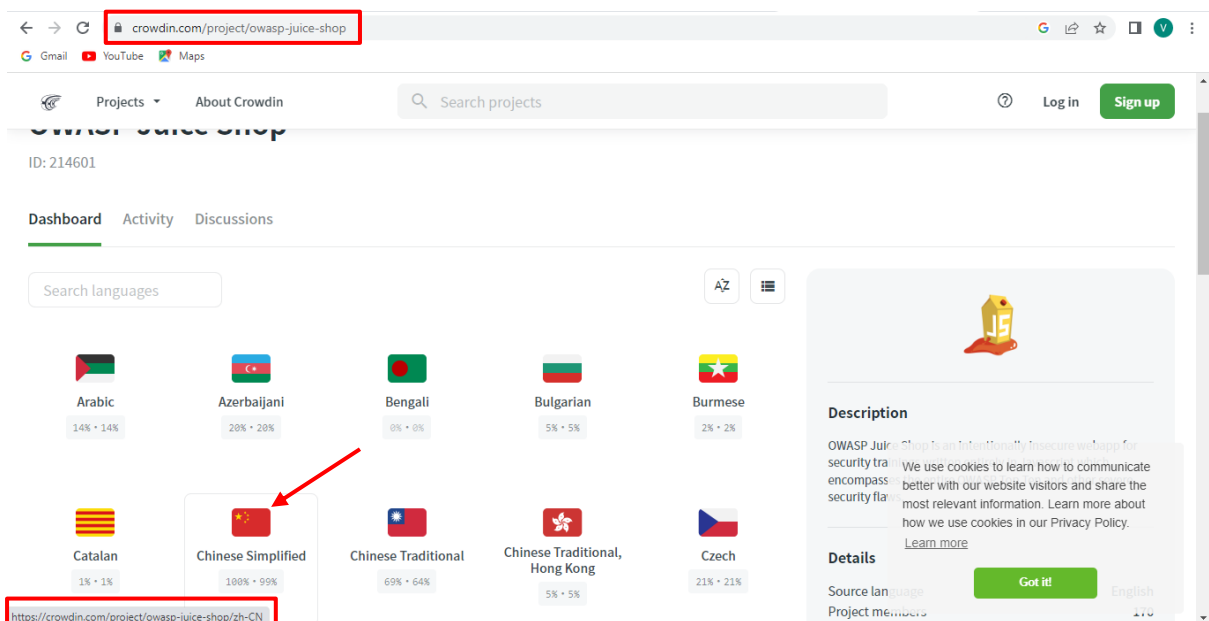
2. lalu masuk ke burpsuite dan masuk ke menu Proxy > HTTP Proxy untuk melihat transaksi yang dijalankan, disana terlihat bahwa web mencoba GET di asset json bahasa Indonesia yang berisikan kosakata untuk setiap menu.



3. setelah itu, tekan ctrl+r untuk mengirim data ke repeater



4. lalu selanjutnya kita harus mencari daftar bahasa yang ada didalam juice shop dengan keyword **owasp juice shop language** atau langsung masuk ke website berikut **crowdin.com/project/owasp-juice-shop** yang dibuat oleh Bjorn kimminich, beliau adalah Owasp Juice Shop Project Leader. Ketika kursor kita arahkan pada salah satu bahasa, maka di pojok kiri bawah terdapat link yang keluar dan terdapat singkatan dari file json dari bahasa tersebut.



5. disini kita akan mencoba bahasa cina, perhatikan singkatan yang terdapat pada akhir link yang muncul.

op/zh-C

7. apabila telah berhasil silahkan kembali ke juice shop dan disana akan muncul notifikasi bahwa telah menyelesaikan tantangan extra language.

