OWASP Juice Shop – Security Misconfiguration
Praktikum Keamanan Jaringan

Dosen Pembimbing :
Dr. Ferry Astika Saputra, ST., M.Sc.

Disusun Oleh :

Fifin Nur Rahmawati (3122640040)

Lula Rania Salsabilla (3122640045)

1 D4 – IT B LJ

D4 TEKNIK INFORMATIKA
DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

2023

Security Misconfiguration adalah ketika pengembang tidak mengikuti dokumentasi sebuah library, framework atau komponen aplikasi, tidak menerapkan standart konfigurasi yang ada, maka aplikasi tersebut akan memiliki beberapa lobang kecil yang akan bisa dimanfaatkan oleh attacker. Kategori ini sangat lah luas, dibandingkan beberapa kategori sebelumnya, hampir 80% dari kerentanan yang ada beberapa tahun terakhir, terkena kerentanan Security Misconfiguration, ini dikarenakan web aplikasi saat ini sudah banyak teknologi framework yang dapat memberikan support / bantuan dari sisi keamanan. Jika pengembang memanfaatkan design dari framework tersebut maka akan memudahkan pengembang untuk fokus pada aplikasi tanpa harus pusing memikirkan secure coding.

Banyak hal yang menjadi penyebab sering terjadi akibat dari miskonfigurasi tersebut:

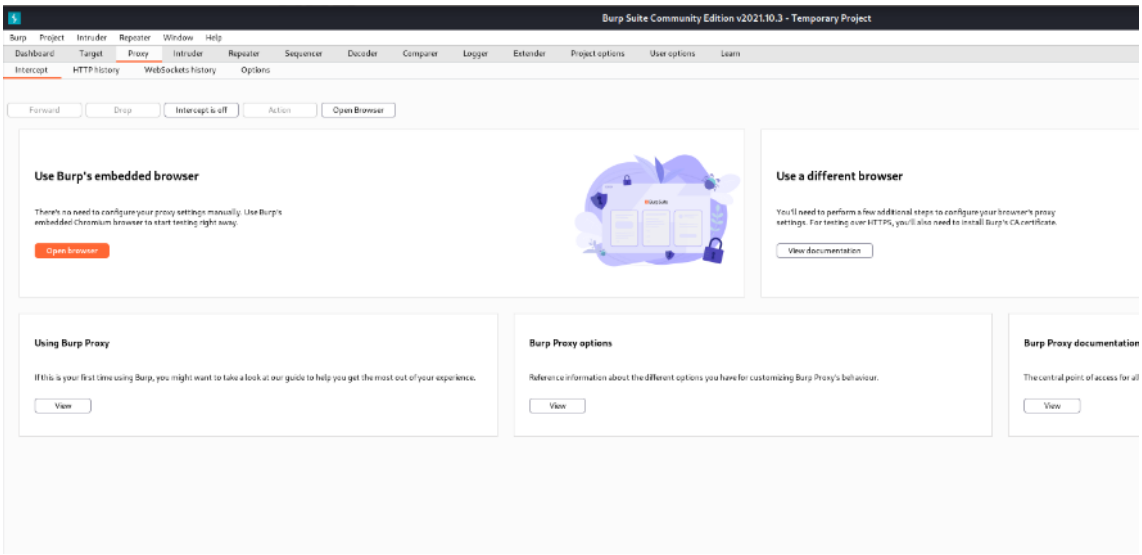
1. HTTP Only
2. Query Builder
3. X-Frame-options
4. Content-Security Policy
5. CORS
6. Acces Control
7. dll….

List diatas merupakan beberapa hal yang sering sekali di lupakan oleh beberapa pengembang.

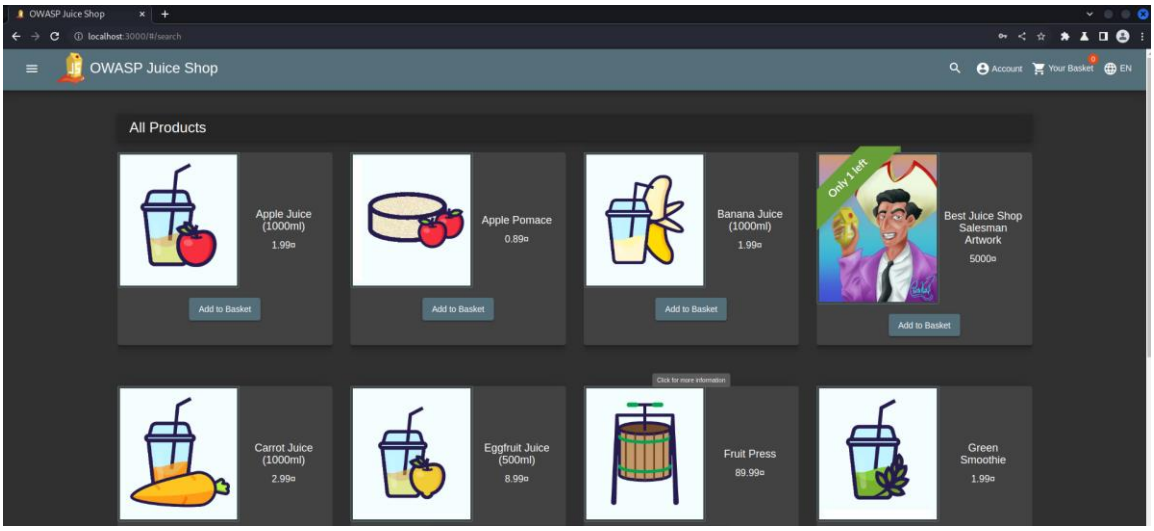
Berikut adalah contoh Security Misconfiguration yang berhasil ditemukan di aplikasi website OWASP Juice Shop:

A. **Error Handling** → Memunculkan error, namun error yang ditampilkan tidak dikemas secara konsisten dan apik.

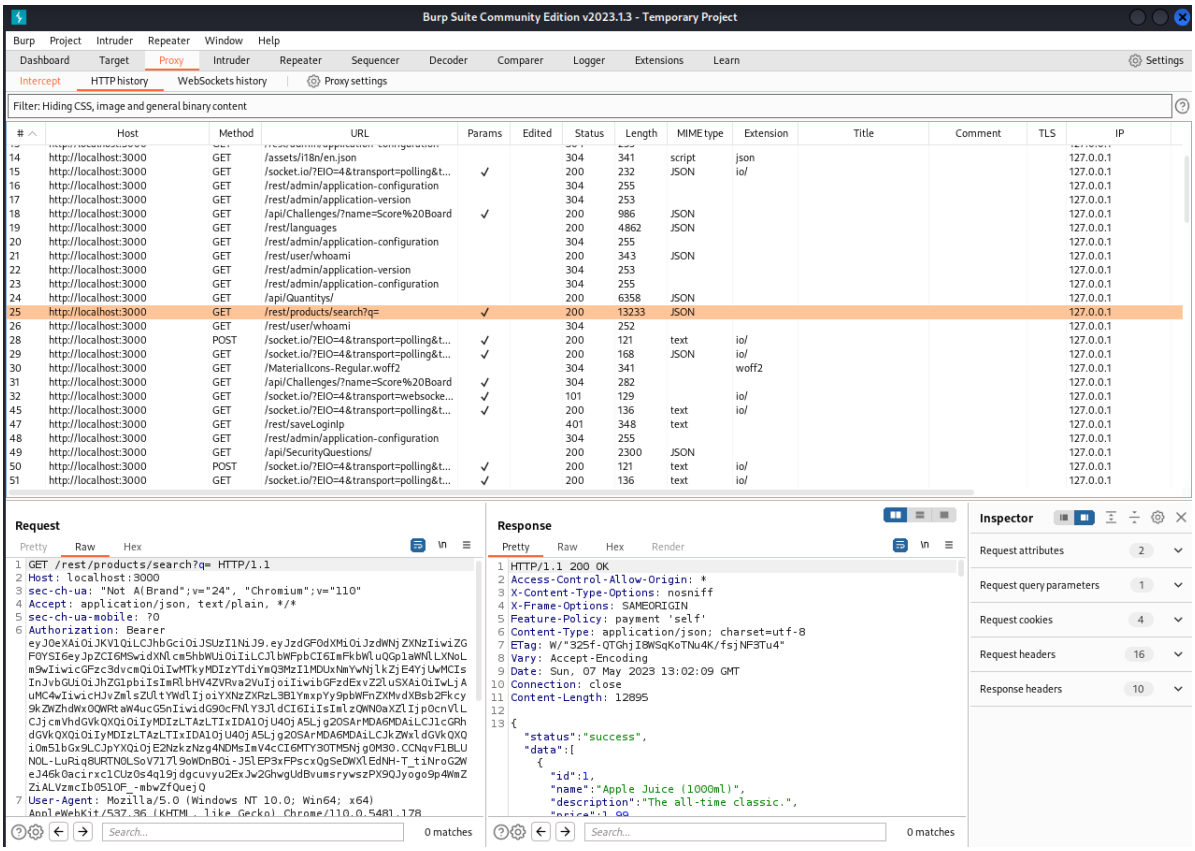
1. Buka aplikasi Burp Suite



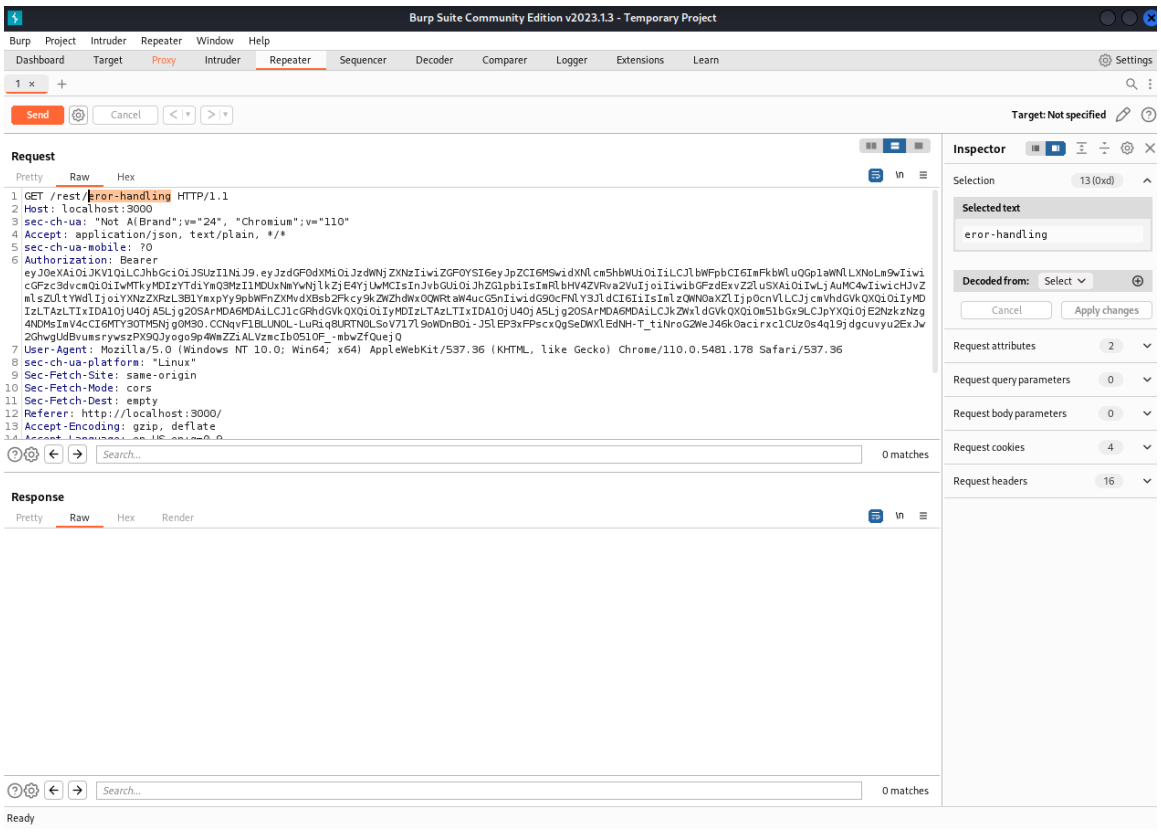
2. Buka browser dan masuk ke halaman utama OWASP Juice Shop

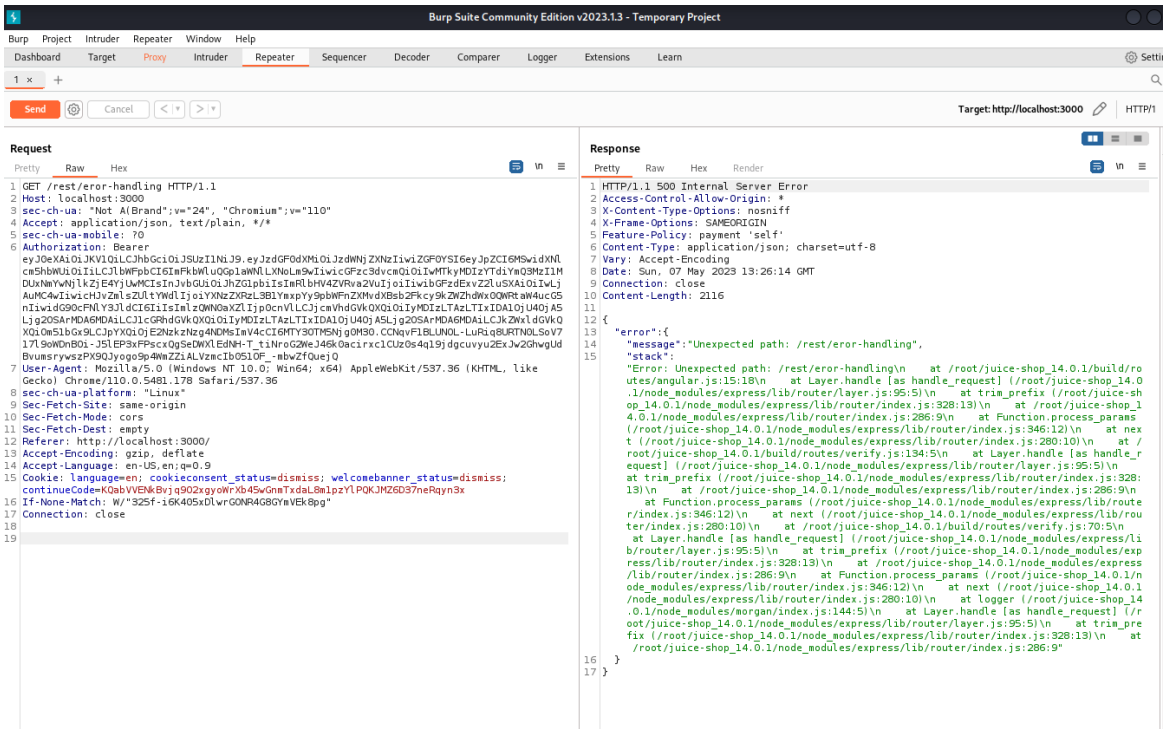


3. Buka kembali Burp Suite, maka akan muncul request baru yaitu /rest/product/search



4. Masukkan payload /rest/product/search ke repeater lalu ubah endpoint menjadi text random kemudian send



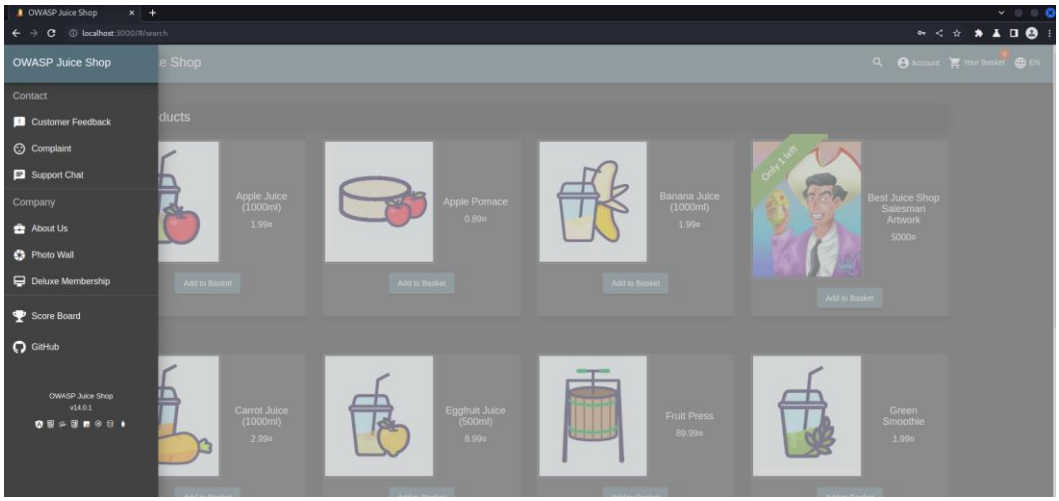


Terdapat response error 500 atau internal server error dimana pesan error sangat panjang dan tidak tertata dengan baik.

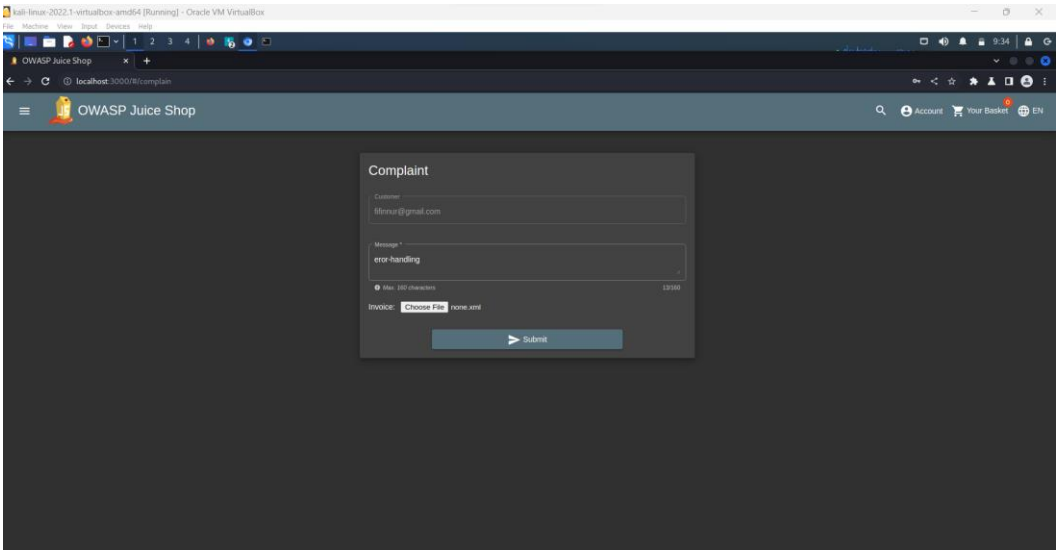
Deprecated

Menggunakan antarmuka B2B kuno yang tidak dinonaktifkan dengan benar

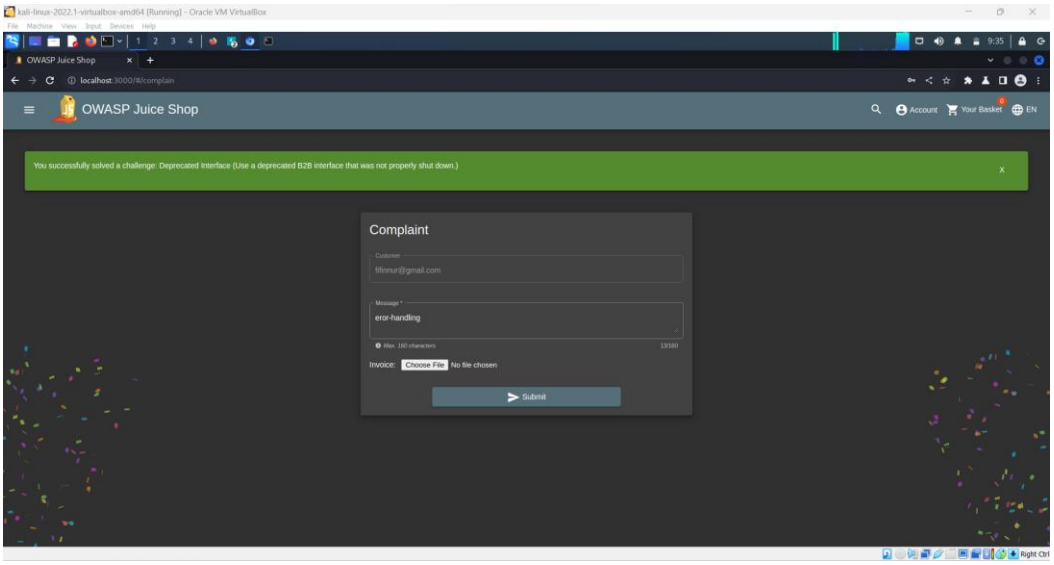
1. Pada halaman utama, tuju halaman Keluhan dengan klik menu sidebar



2. Isi form dan masukkan file dengan format .xml



3. Muncul notifikasi challenge Deprecated Interface berhasil diselesaikan



4. Lihat proxy history pada Burp Suite, akan muncul pesan error yang panjang