

A01 OWASP – BROKEN ACCESS CONTROL

Tugas Keamanan Jaringan Minggu 2



February 26, 2023

Fajar yunus afiffudin

NRP 3122640049

Broken Access Control atau disebut juga sebagai Broken Access Management adalah suatu kerentanan keamanan yang terjadi pada aplikasi web atau sistem yang dapat memungkinkan pengguna tidak sah untuk mendapatkan akses yang tidak seharusnya pada sumber daya yang dilindungi atau fitur yang terbatas.

Secara umum, Access Control adalah proses untuk memastikan bahwa hanya pengguna yang diizinkan atau memiliki otoritas untuk melakukannya yang dapat mengakses sumber daya atau fitur tertentu. Jika mekanisme Access Control tidak dirancang atau diimplementasikan dengan benar, hal ini dapat mengakibatkan celah keamanan yang memungkinkan pengguna tidak sah atau penyerang untuk mengakses sumber daya atau fitur yang dilindungi tersebut.

Berikut adalah cara pent test untuk mengetahui tentang Broken Access management

Dalam pen test ini membutuhkan aplikasi Burpsuite, namun sebelum install aplikasi tersebut cek versi java kalian karena burpsuite hanya akan beroperasi pada versi java 17 ke atas.

1. lakukan pengecekan versi java.

Text

Description automatically generated

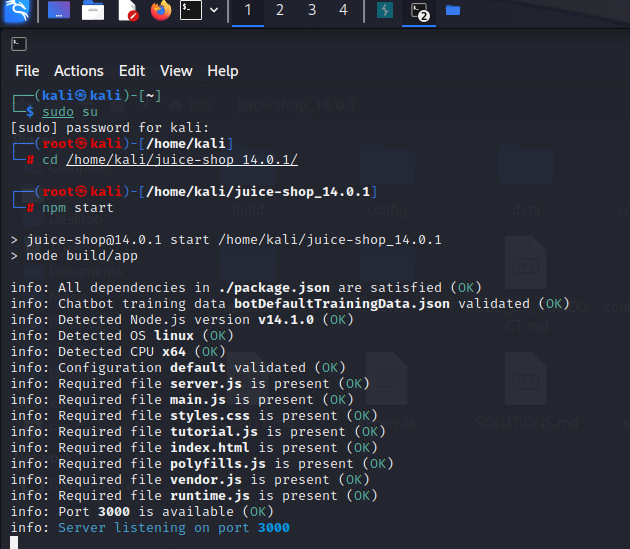
Pada OS saya sudah terinstal java versi 17 maka minimum requirement sudah terpenuhi.

2. lakukan instalasi Burpsuite

A computer screen capture

Description automatically generated with medium confidence

3. Jalankan OWASP Juice Shop



4. buka aplikasi burpsuite

Graphical user interface, text, application

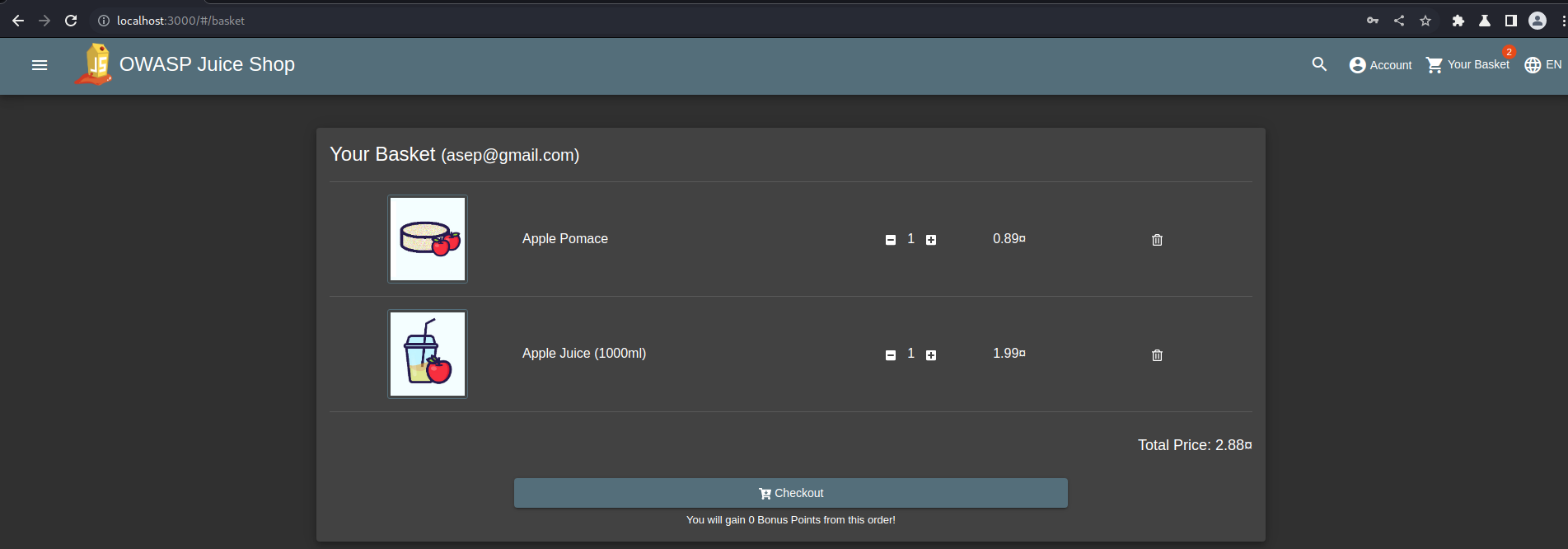
Description automatically generated

Pada pengetesan pertama saya akan mengtrace dari HTTP request. Silahkan memilih proxy dan pilih HTTP History. Setelah itu buka browser dan buka halaman juice shop

Graphical user interface

Description automatically generated

Setelah login saya akan menambahkan 1 apple juice dan1 apple pomace kedalam basket



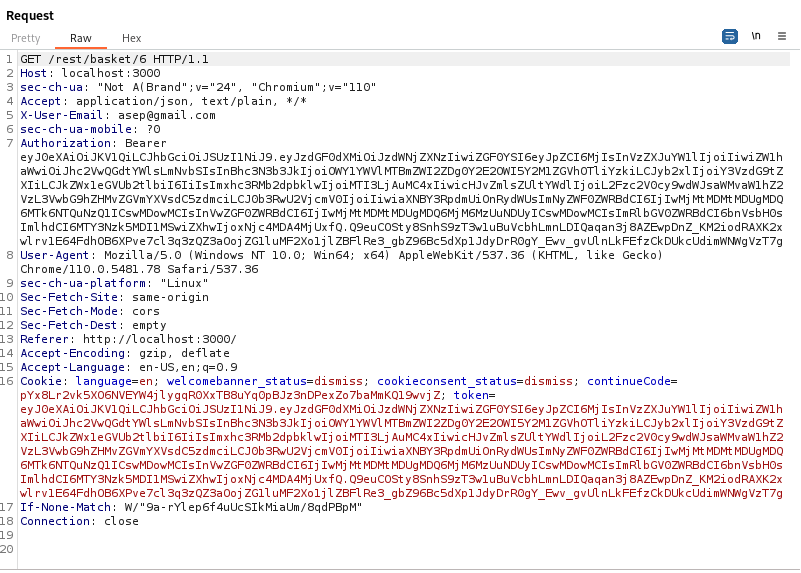
Terlihat isi basket saya adalah 2 item di atas, sekarang coba buka burp suite dan trace http requestnya.

Graphical user interface, table

Description automatically generated



Saat salah satunya di tekan maka akan keluar informasi sebagai berikut





Jika dilihat dari request ini sebenarnya ini menggunakan API dan angka 6 sepertinya adalah nomer dari user yang sudah terdaftar untuk memanggil isi basket.

Mari kita kirim request di atas ke repeater dan liat apa yang akan terjadi

Text

Description automatically generated



Disini bisa dilihat terdapat 2 item yaitu apel penance dan apple juice yang mana kedua item tersebut adalah item yang ada di dalam basket kita tadi.

Selanjutnya apa yang akan terjadi jika kita mengubah angka dari API request

Text

Description automatically generated

Dengan mengubah basket number ke angka 2 maka kita akan bisa melihat basket dari user lain dengan basket number 2.

Berikutnya kita akan mencoba menggunakan fitur intercept yang ada di burpsuite

Graphical user interface, application

Description automatically generated

Aktifkan fitur tersebut dan di juice shop tekan home page dan tekan basket

Graphical user interface, text, application, email

Description automatically generated

Terlihat itu adalah request ke basket, akan saya ubah nomer dari user ke nomer 2 dan klik forward

Graphical user interface, application

Description automatically generated

Maka di browser akan tertampil basket dari user dengan nomor 2. (**BROKEN ACCESS CONTROL VIEW BASKET)**

Selanjutnya menambahkan atau mengubah basket dari user lain **( BROKEN ACCESS CONTROL BASKET MANIPULATE)**

**A screenshot of a computer

Description automatically generated**



Sekarang user tersebut mempunyai 3 raspberry juice setelah tadinya hanya 2 buah. Untuk menampilkah hasil dari modifikasi di atas dapat mengulangi step dari intercept.

Selanjutnya menggunakan metode Burte Force untuk melakukan login Admin **(BROKEN ACCESS CONTROL ADMIN SECTION)**

Hal pertama yang harus dilakukan adalah mengetahui email dari admin terlebih dahulu

Graphical user interface, application, website

Description automatically generated



Dengan membuka informasi dari item maka kita akan menemukan informasi email dari admin

Selanjutnya tambahkan URL dari juice shop ke target site

Graphical user interface, application

Description automatically generated



Pada proxy seting centang “Is In Target Scope”

Graphical user interface, text, application

Description automatically generated



Kembali ke halaman login, masukkan email dari admin dengan password random

A screenshot of a computer

Description automatically generated with medium confidence

Sebelum itu siapkan intercept di burpsuite, aktifkan dan tekan login

Pada intercept klik forward sampai muncul username admin dan password yang kita inputkan tadi

Graphical user interface, text, application, email

Description automatically generated



Kemudian kirim ke intruder

Graphical user interface, text, application, email

Description automatically generated



Bersihkan target untuk semua burte force dengan menekan clear

Setelah itu pilih target burteforce yang mana ini adalah password dan tekan add

Graphical user interface, text, application, email

Description automatically generated



Pada menu playload, muat file berformat .txt sebagai password bank yang nantinya akan di gunakan untuk burte force

Graphical user interface, text, application, email

Description automatically generated



Disini saya sudah menyiapkan file tersebut

Graphical user interface, text, application, Teams

Description automatically generated



Setelah password sudah di load tekan start attack

Table

Description automatically generated



Pada data set password di atas terdapat 2 jenis HTTP status yaitu 401 dan 200, 401 sendiri terjadi karena saat permintaan browser ke server tidak memiliki kredensial autentik yang valid, untuk HTTP request 200 server berhasil menerima request dari browser yang kita gunakan dapat diartikan OK.

Login dengan password dari hasil brute force

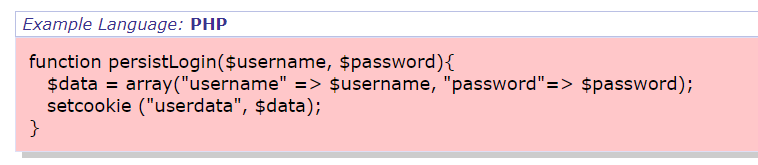
Graphical user interface

Description automatically generated

Graphical user interface, application

Description automatically generated

Burte force memiliki kaitan dengan Broken access control yang tertulis di CWE-922 Insecure Storage of Sensitive Informasion, dalam CWE 922 relevan dengan CWE-312 [Cleartext Storage of Sensitive Information](https://cwe.mitre.org/data/definitions/312.html), dapam CWE 312 memiliki kaitan dengan CWE-11 Missing Encryption of Sensitive Data.





Kode di atas sama seperti kode dari header HTTP di Burp Suite tadi dimana data dari user tertampil. Ini akan mengekspos informasi dari user jika computer mereka di serang oleh hacker.