

LAPORAN RESMI
PRAKTIKUM KEAMANAN JARINGAN
A05 SECURITY MISCONFIGURATION



Oleh :

Tarisa Dinda Deliyanti 3122640037

Fisabili Maghfirona Firdaus 3122640051

D4 LJ Teknik Informatika B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
TAHUN AJARAN 2022/2023

Security misconfiguration adalah terjadinya suatu kesalahan pada sistem aplikasi web dikarenakan adanya kode program yang salah ataupun sistem melakukan proses yang tidak perlu dilakukan. Hal ini membuat peretas bisa melakukan penetrasi kepada aplikasi web dengan cara menyisipkan virus, membuat url palsu untuk mencari hidden url, dan lain sebagainya. Security Misconfiguration juga dapat terjadi 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. Jika pengembang memanfaatkan design dari framework tersebut maka akan memudahkan pengembang untuk fokus pada aplikasi tanpa harus pusing memikirkan secure coding.

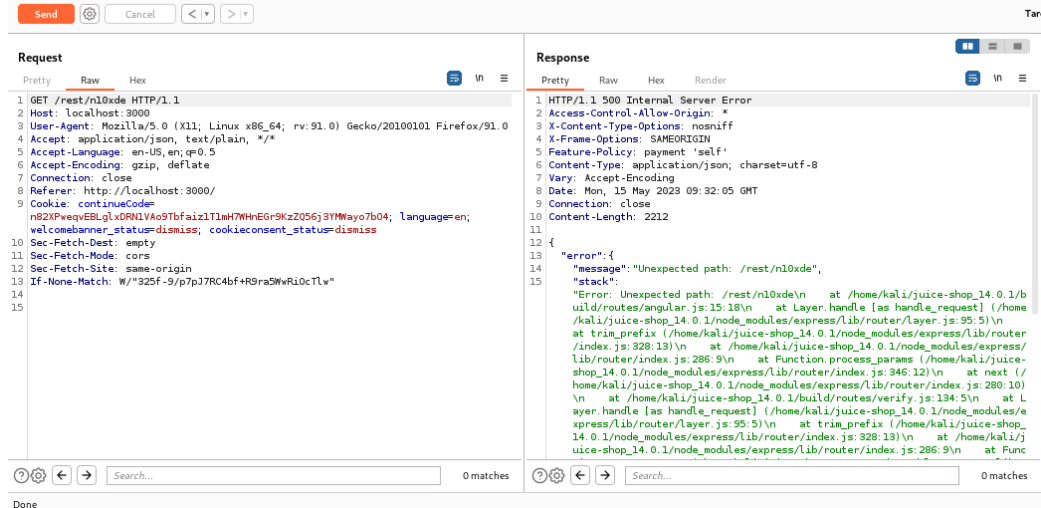
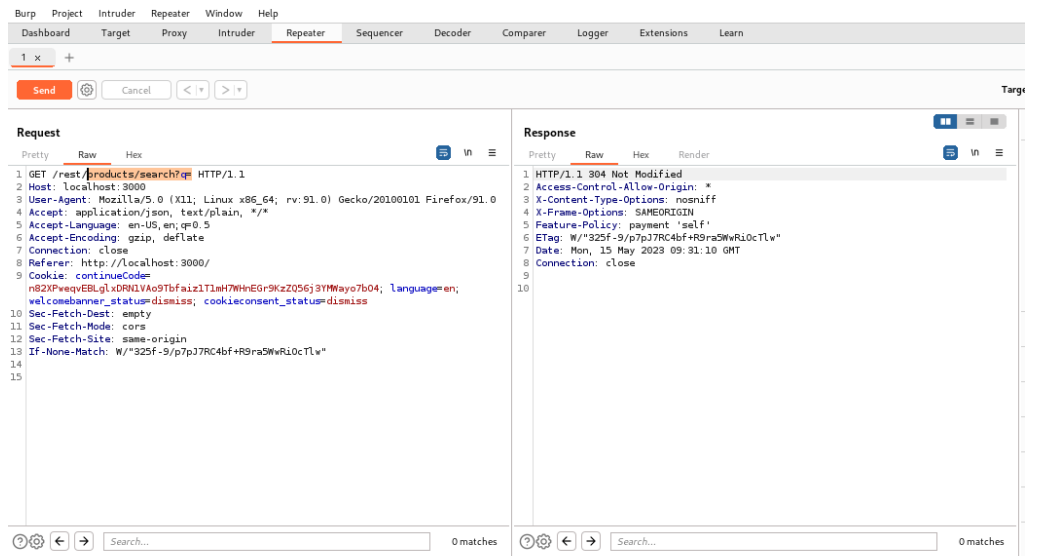
Percobaan 1

1. Masuk ke halaman website OWASP Juice Shop. Tambahkan produk di keranjang dan buka burp suite. Pilih url `/rest/products/search?q=` lalu cek request dan response nya.

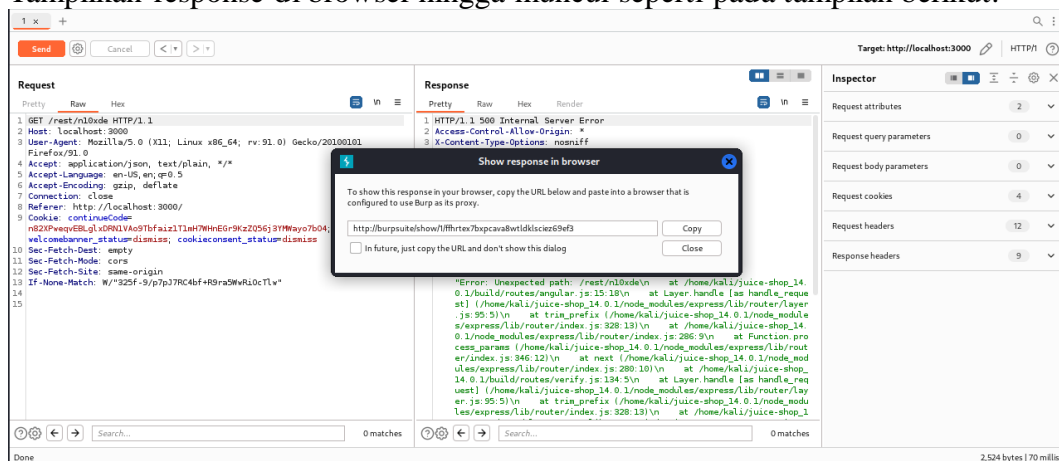
Kirim data tersebut ke Repeater.

The screenshot shows the Burp Suite interface with the Repeater tab active. A table of intercepted requests is displayed, with the following columns: #, Host, Method, URL, Params, Edited, Status, Length, MIME type, Extension, Title, Comment, and TLS. The 49th request is highlighted in orange, showing a GET request to `/rest/products/search?q=` with a status of 304 and length of 255. Below the table, the 'Request' and 'Response' panels are shown. The 'Request' panel displays the raw HTTP request, including headers like `Host: localhost:3000`, `User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0`, and `Accept: application/json, text/plain, */*`. The 'Response' panel displays the raw HTTP response, including headers like `HTTP/1.1 304 Not Modified`, `Access-Control-Allow-Origin: *`, and `ETag: W/"325f-9/p7p37RC4bf+R9ra5WwRi0cTlw"`.

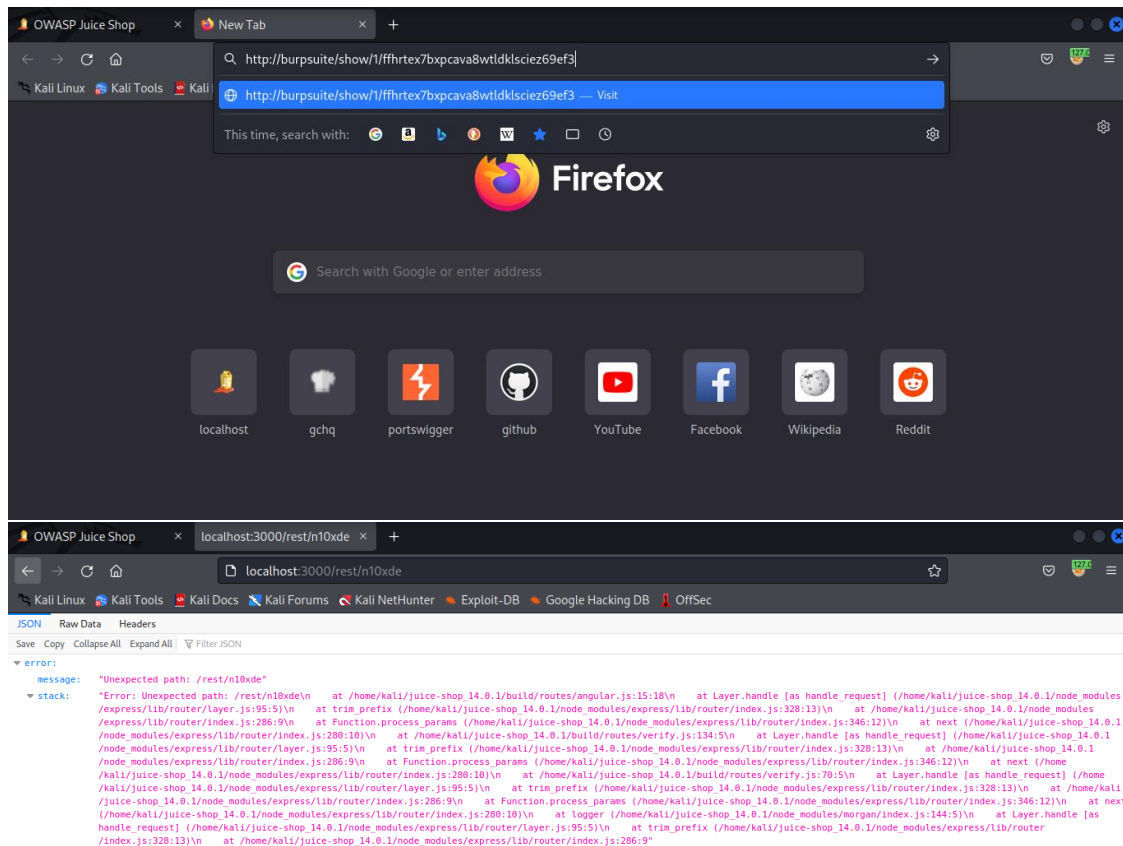
2. Cek request dan response dari url terkait di dalam Repeater. Pada teks yang dihighlight, kemudian ubah endpoint tersebut menjadi text random dan klik Send lagi lalu muncul response.



3. Tampilkan response di browser hingga muncul seperti pada tampilan berikut.



4. Paste link ke browser dan jalankan lalu akan muncul seperti tampilan di bawah ini.

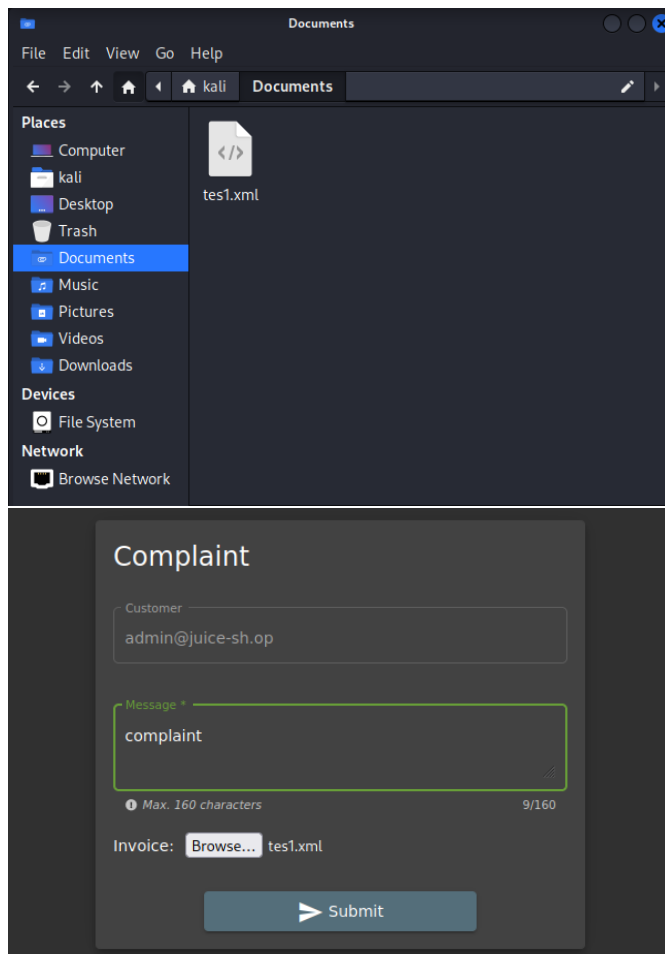


Percobaan 2

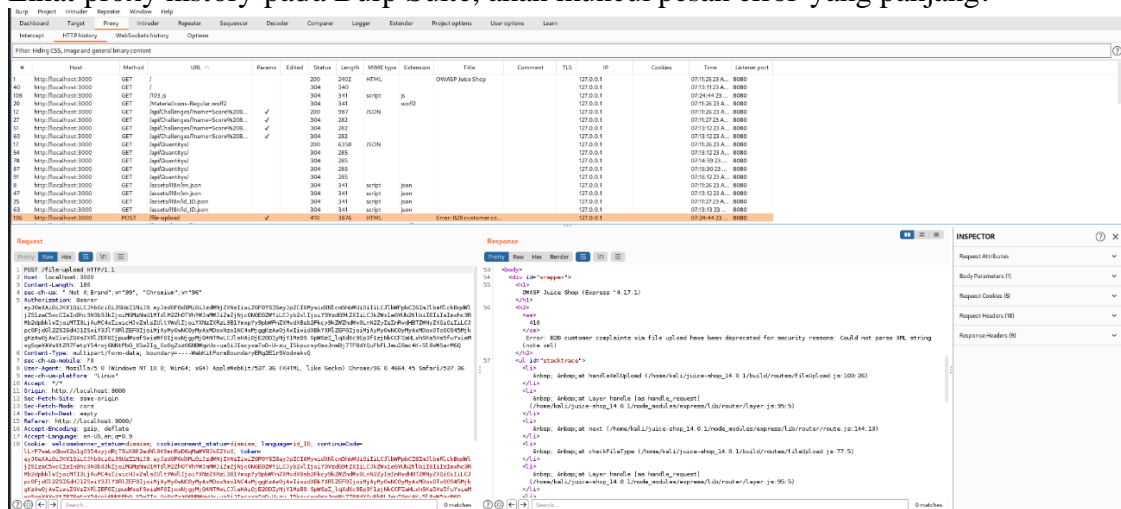
1. Buka halaman Login pada aplikasi OWASP Juice Shop. Masukkan email dan password seperti pada tampilan di bawah ini.

The screenshot shows the Login page of the OWASP Juice Shop application. The email field is filled with `admin@juice-sh.op` and the password field is filled with `admin123`. There is a "Log in" button and a "Remember me" checkbox.

2. Buat file berisi terserah dan unggah ke dalam form complaint. Tambahkan customer, message, dan unggah file tes1.xml lalu klik Submit.



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



Note:

Repeater adalah salah satu bentuk injeksi dalam melakukan suatu request. Fungsi burpsuite adalah untuk mengintercept.