LAPORAN RESMI
PRAKTIKUM KEAMANAN JARINGAN
A03 INJECTION

Oleh :

Tarisa Dinda Deliyanti 3122640037

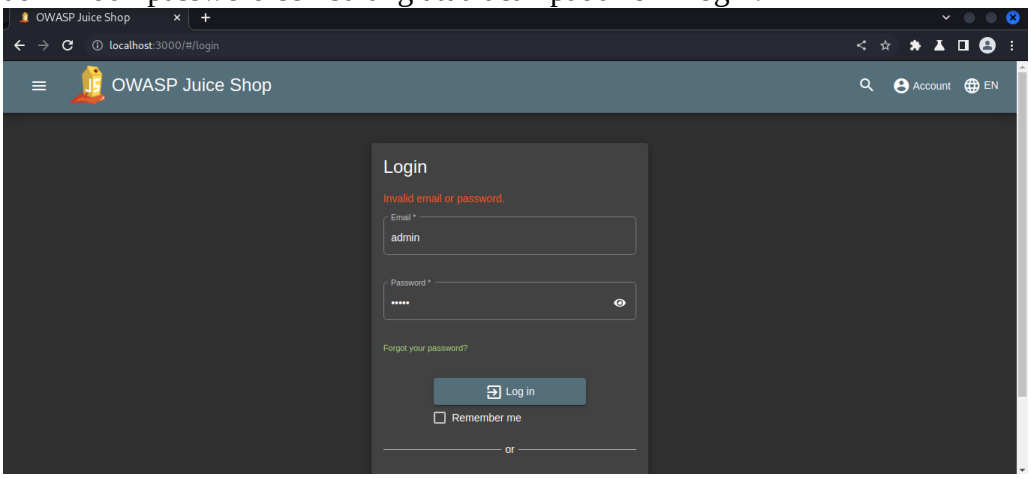
Fisabili Maghfirona Firdaus 3122640051

D4 LJ Teknik Informatika B

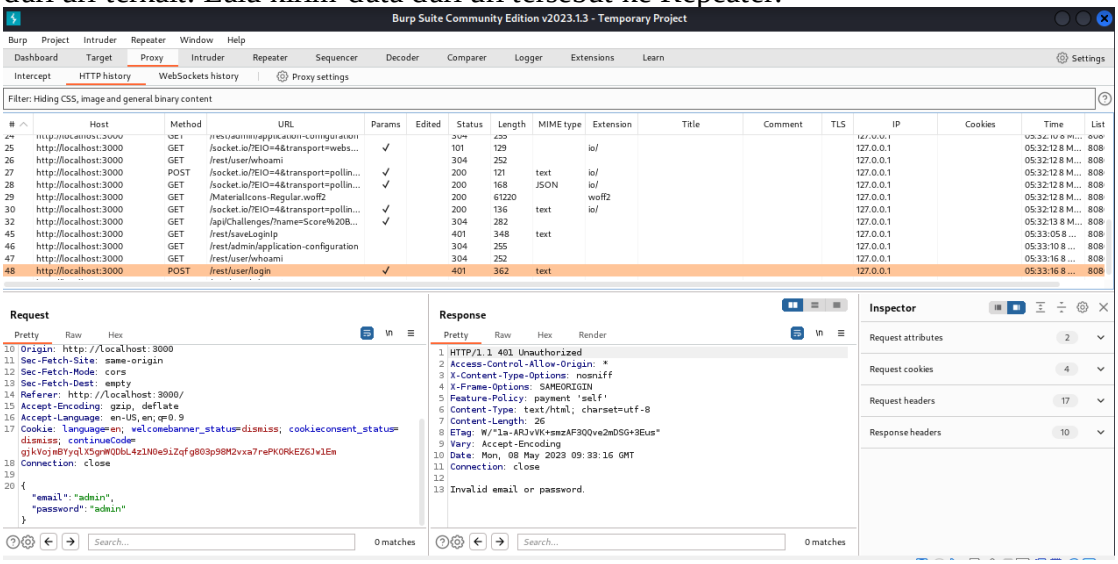
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
TAHUN AJARAN 2022/2023

Skenario 1 : Login dengan menggunakan karakter command

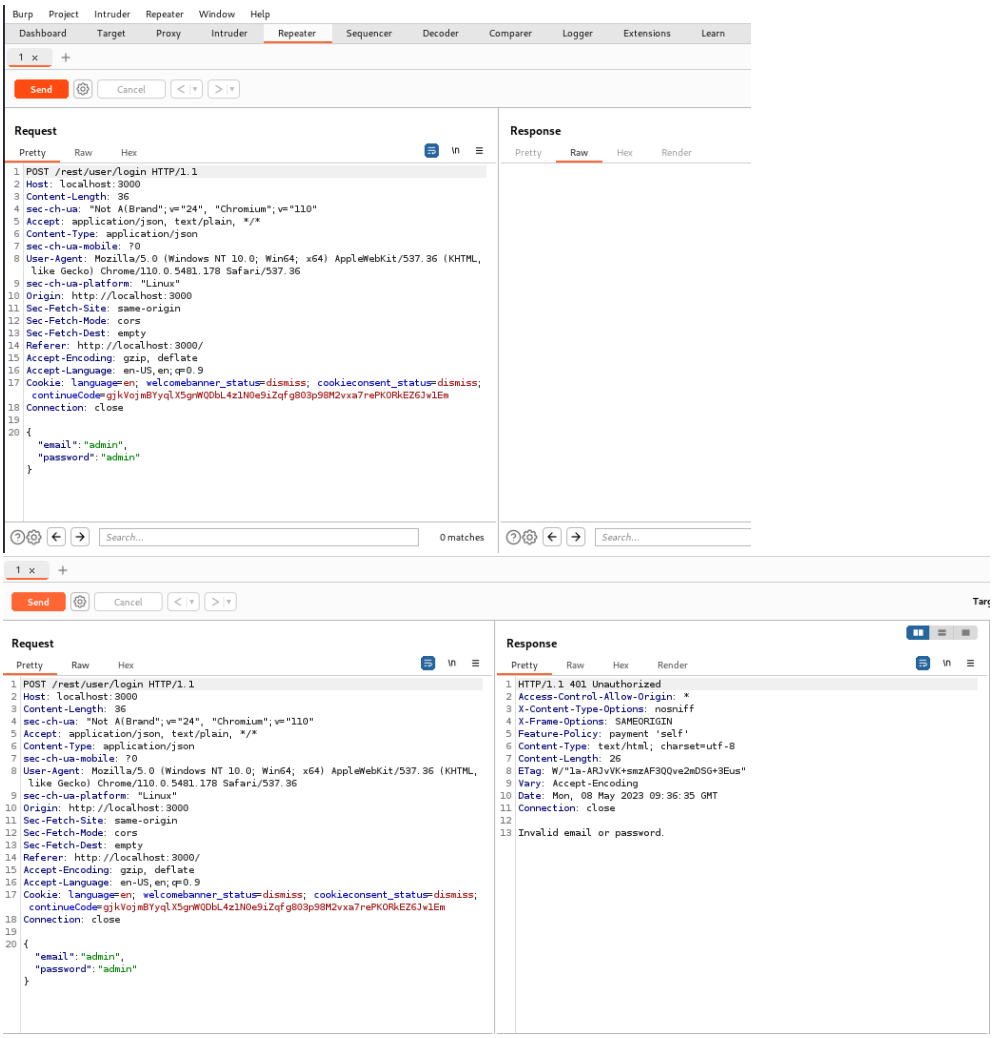
1. Percobaan login ini memanfaatkan sql injection dengan menginputkan akun email admin dan password sembarang atau acak pada form login.



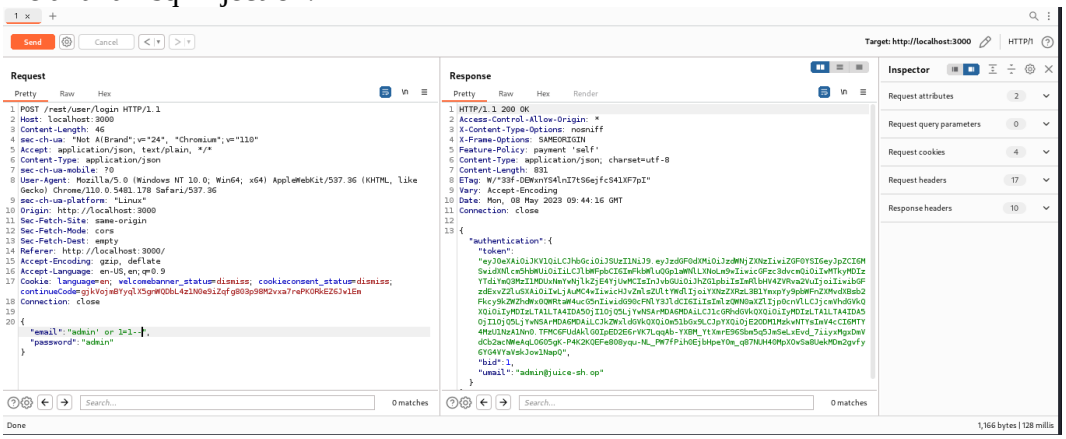
2. Proses login pada gambar di atas akan terdeteksi di Burp Suite pada menu Proxy bagian HTTP history. Kemudian cari url /rest/user/login untuk melihat request dan response dari url terkait. Lalu kirim data dari url tersebut ke Repeater.



3. Tampilan di bawah ini merupakan data request pada Repeater, lalu klik tombol Send untuk mendapatkan data response.



4. Menambahkan 'or 1=1--' pada email di bagian request Repeater. Kemudian klik tombol Send lagi untuk melihat response. Jika sudah mendapatkan token berarti berhasil melakukan sql injection.

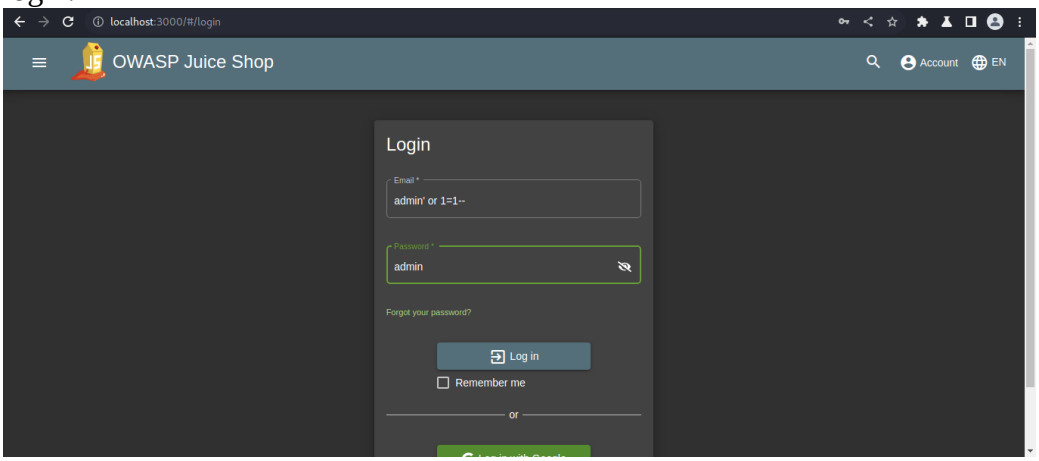


Note:

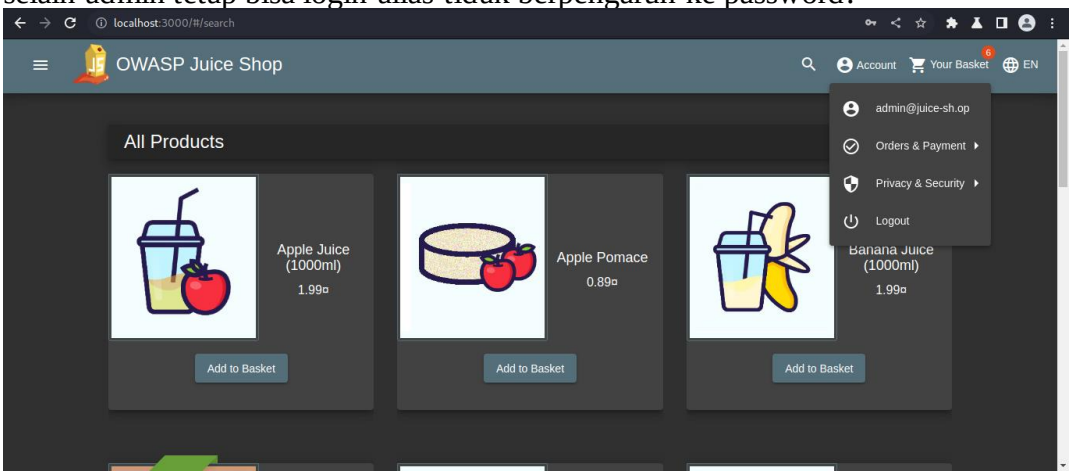
Terdapat tanda -- sebagai command dan ada tanda (‘) setelah kata admin adalah untuk *mentrigger* atau membuka proses injeksinya, jika tidak terdapat tanda (‘) akan tetap menjadi teks biasa. Jika terdapat kata dengan tanda (‘) yang bersamaan dengan tanda (‘) untuk *mentrigger* proses injeksi, harus ditambahkan tanda (\) atau *input sanitation*

agar jika ada teks dengan tanda (‘) seperti Raf’a tetap bisa terbaca nanti penulisannya menjadi Raf\’a.

5. Menginputkan email admin’ or 1=1-- pada form login dan password admin dan berhasil login.



Pada percobaan ini yang diinjeksi adalah emailnya sehingga ketika password diisi selain admin tetap bisa login alias tidak berpengaruh ke password.



Note:

Percobaan sql injection tidak akan terjadi eror pada database. Untuk mengatasi agar tidak terjadi sql injection, harus membuat secure form sehingga untuk membuat coding nya harus terdapat filter atau pengkondisian yang detail seperti hanya boleh ada angka, huruf, dan tidak boleh symbol, serta menerapkan input injection.