# PRAKTIKUM A03

# INJECTION (OWASP 10 JUICE SHOP)


**DI SUSUN OLEH :**

Nadya Indah Trisnawati (3122640034)

Mochammad Jauhar Ulul Albab (3122640044)

LJ D4 IT B

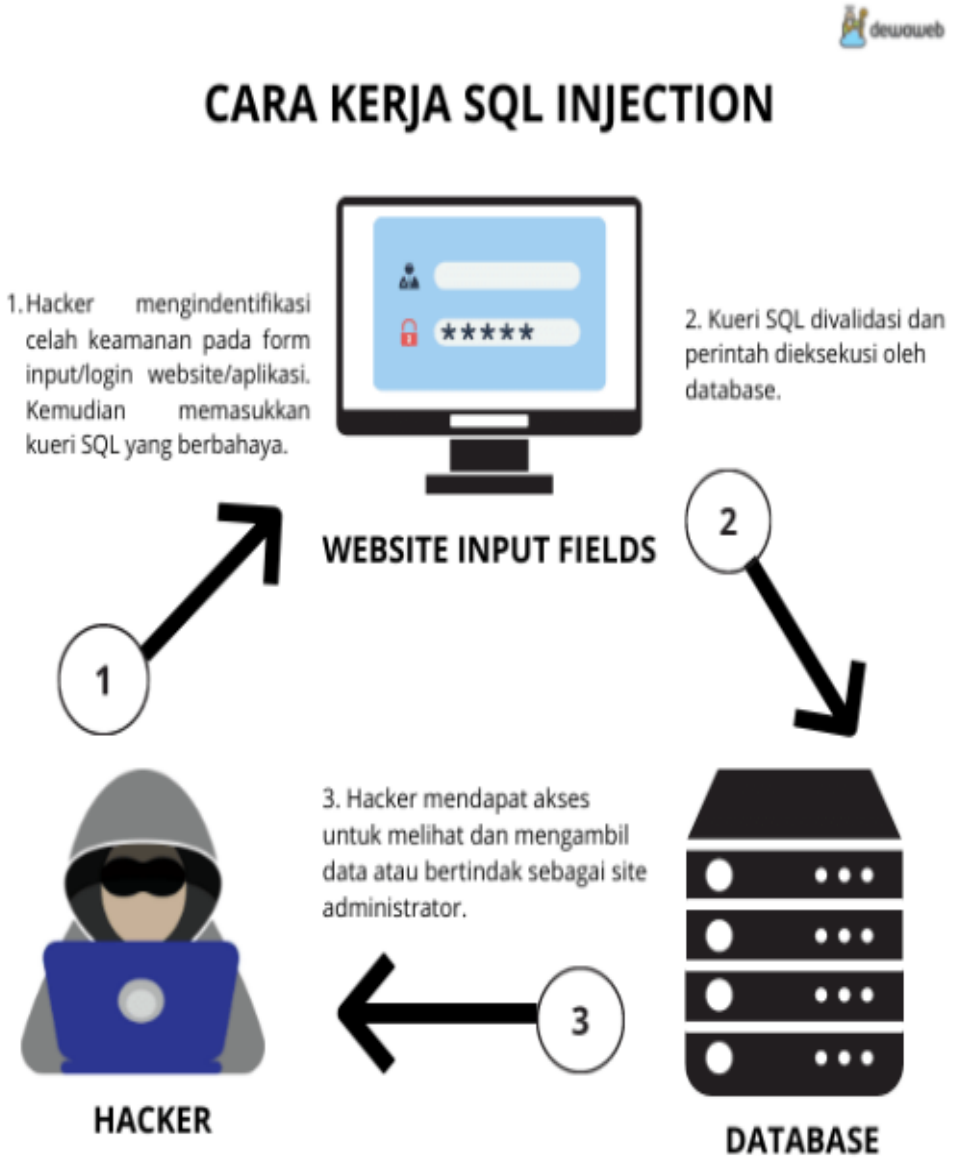
**PROGRAM STUDI TEKNIK INFORMATIKA**

**DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER**

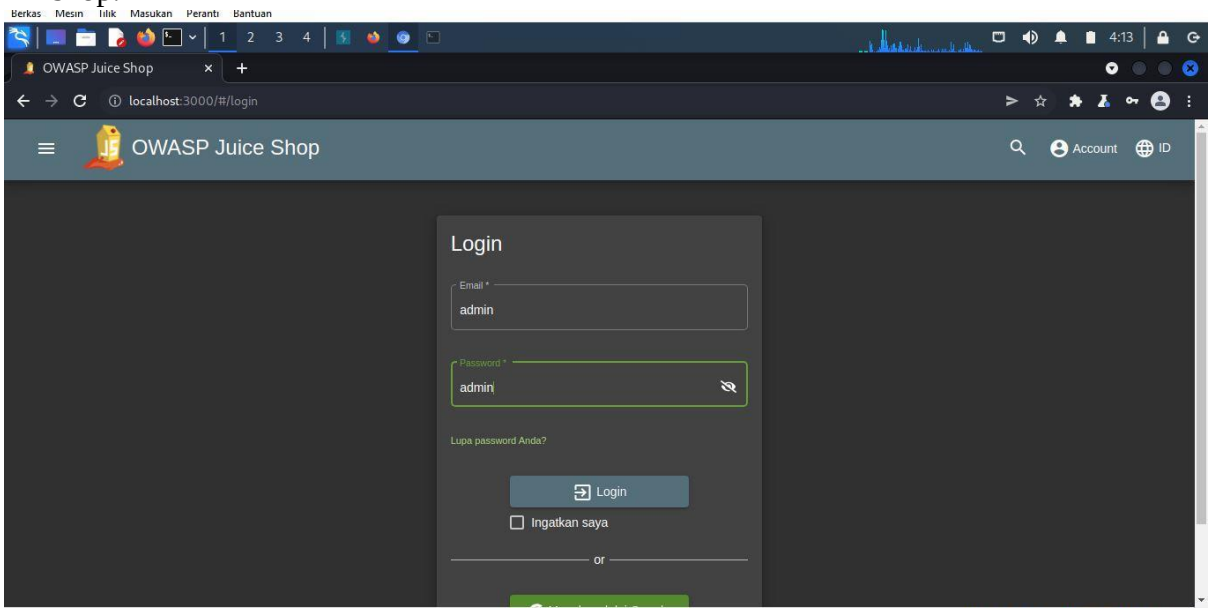
**POLITEKNIK ELEKTRONIKA NEGERI SURABAYA**

1. **Injection**

Injection adalah sebuah serangan keamanan pada aplikasi web yang memanfaatkan celah pada input yang diterima oleh aplikasi tersebut. Serangan ini dilakukan dengan memasukkan kode-kode yang tidak semestinya pada input, sehingga membuat aplikasi tersebut mengalami kerentanan dan dapat digunakan untuk melakukan serangan. Pada OWASP Juice Shop, tantangan Injection memiliki beberapa level yang semakin sulit. Tantangan tersebut meliputi SQL Injection, NoSQL Injection, dan Command Injection. Setiap level tantangan memiliki instruksi yang jelas dan disertai dengan petunjuk serta hint yang dapat membantu para pengembang aplikasi dan pengujian keamanan dalam menyelesaikan tantangan tersebut.

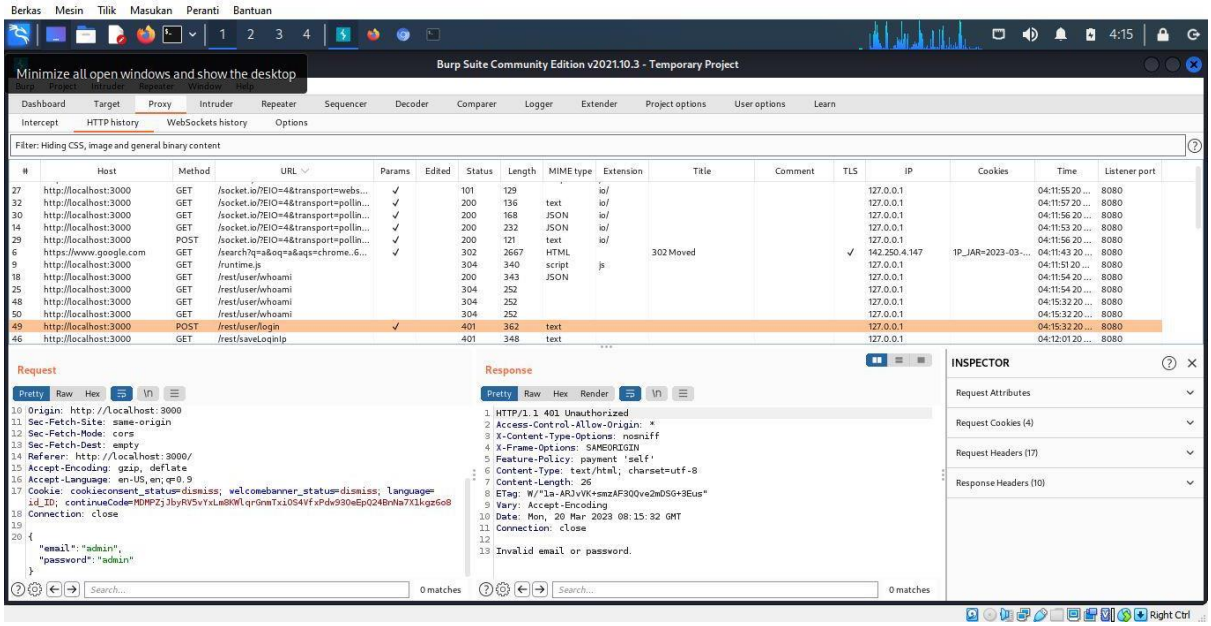


2. Percobaan 1 : Login Admin
   - Memasukkan email dan password secara dummy di login admin pada owasp juice shop.



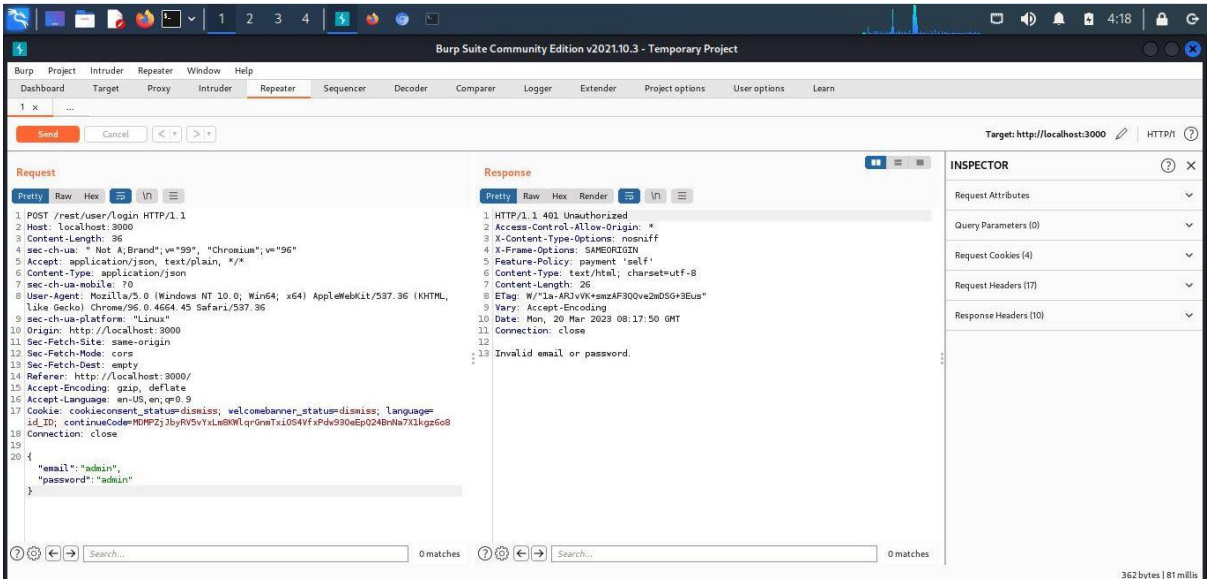

Analisa : Melakukan login dengan mengisi email dan password admin tanpa di ikuti dengan nama domain email dibelakangnya. Hal ini dilakukan untuk membuktikan apakah dapat login dengan email dan password yang random.

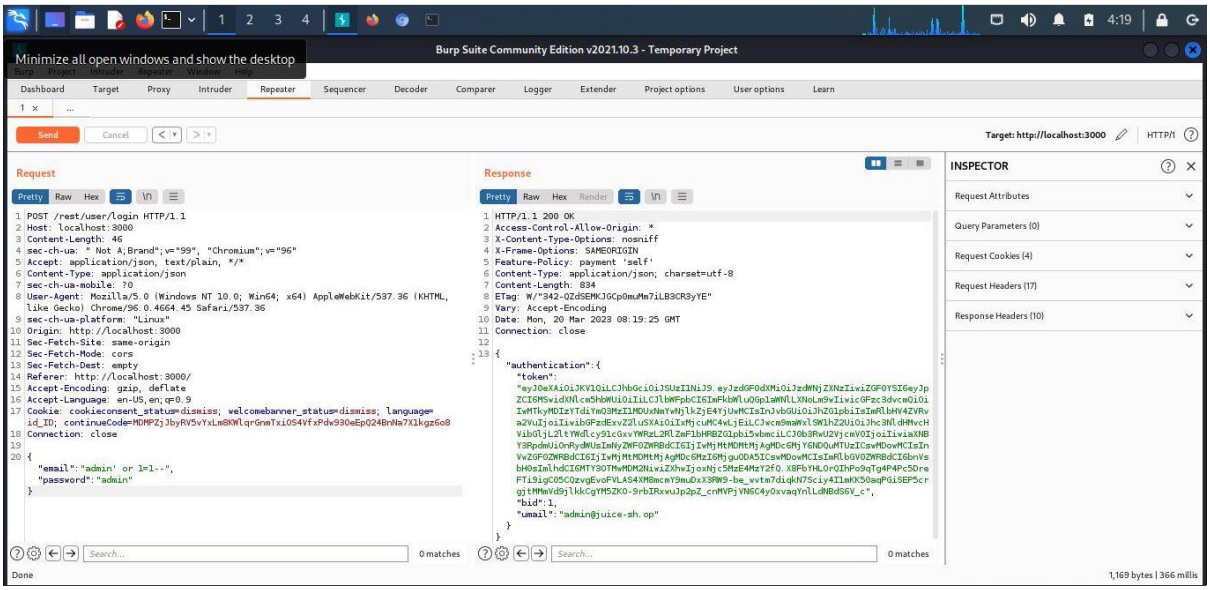
   - Melakukan pengecekan menu proxy http_request




Analisa : Dengan melakukan pengecekan HTTP req didalam menu proxy, yang dimaksudkan untuk mencari alamat url/rest/user/login untuk melihat request dan respon yang diberikan. Namun hasilnya belum bisa masuk ke akun admin dikarenakan belum terautentifikasi data email dan juga password.

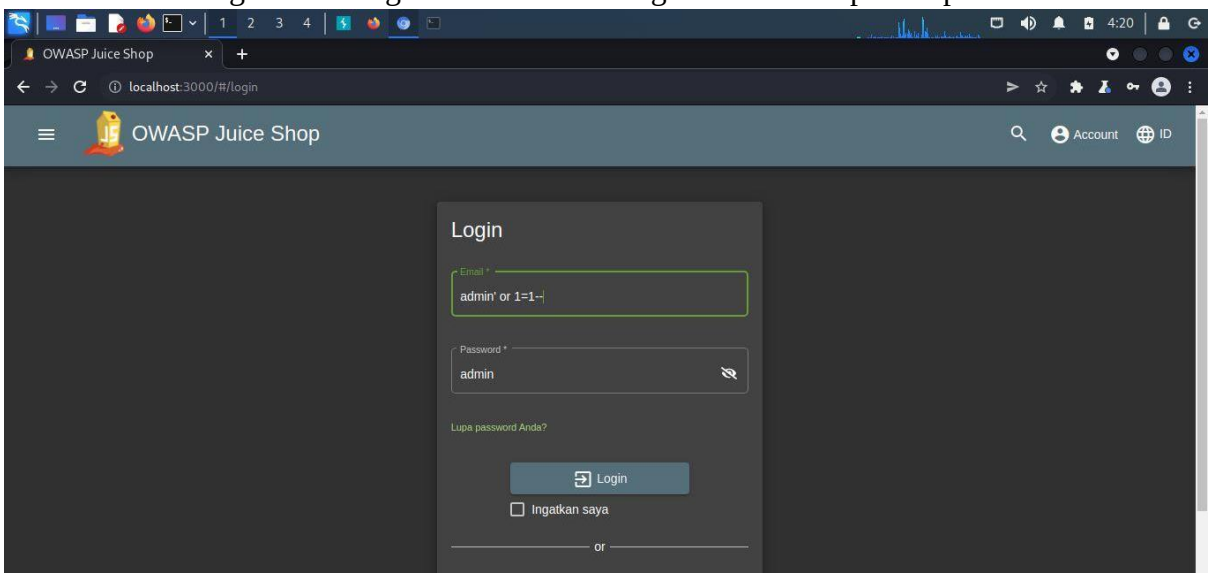
- Memindahkan request ke repeater untuk dapat dimodifikasi isi requestnya.

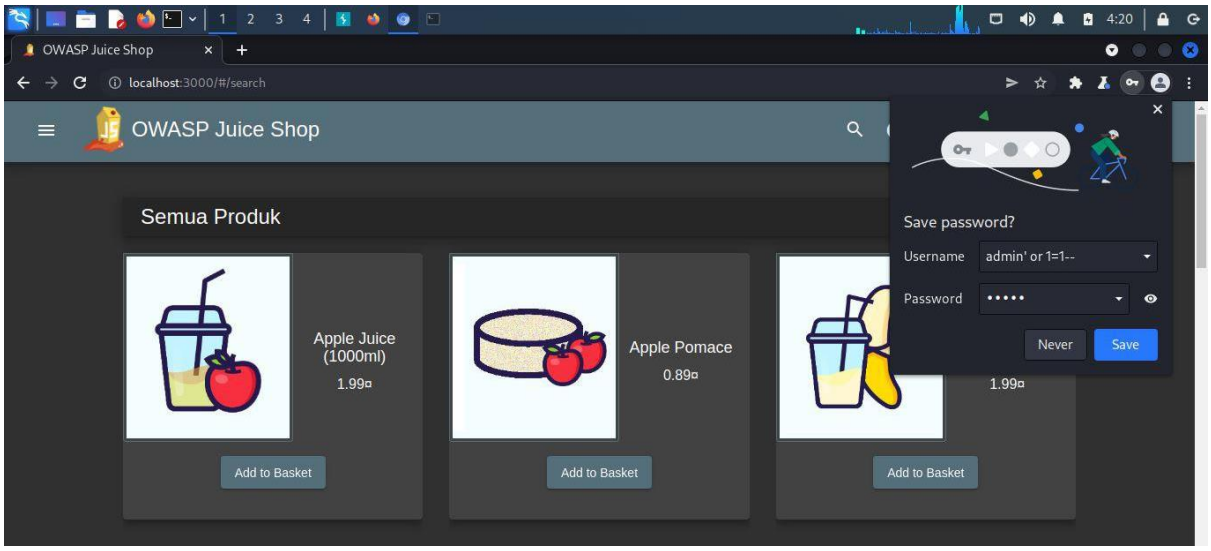



Analisa : Mencoba melihat kembali saat dilakukan penyalinan request apakah respon yang diberikan sama seperti sebelum dimodifikasi. Pada gambar kedua mencoba untuk memodifikasi email dengan injection sesuai dengan arahan modul dengan memberikan tanda ‘or 1=1 -- untuk dapat melakukan generate response yang sesuai dan mendapatkan token authenthication serta kode pesan 200. Pada gambar tersebut berhasil mendapatkan pesan sukses yang berarti injeksi sudah berhasil.

- Melakukan login user dengan email sesuai dengan modifikasi pada repeater




Analisa : Setelah memasukkan kode injection yang telah dilakukan diawal tadi, maka halaman dashboard telah berhasil di akses dan masuk sebagai user admin.

3. Ketika sebuah injeksi SQL diinputkan ke dalam database, maka query SQL yang dihasilkan akan berbeda dari yang seharusnya. Injeksi SQL dapat dimanipulasi untuk memodifikasi atau menampilkan data yang tidak seharusnya bisa diakses atau dimodifikasi oleh pengguna yang tidak berhak.
4. Perbedaan utama antara injection dan SQL injection adalah target dari serangan tersebut. Injection adalah serangan yang lebih umum dan dapat terjadi pada berbagai jenis aplikasi web yang terhubung dengan database atau tidak. Sementara itu, SQL injection secara khusus ditujukan untuk memanipulasi database melalui query SQL yang dihasilkan oleh aplikasi web. Baik injection maupun SQL injection dapat mengakibatkan kerusakan pada aplikasi web dan kebocoran data sensitif, oleh karena itu sangat penting untuk melakukan pengujian keamanan dan menerapkan praktik keamanan seperti validasi input dan penggunaan parameterized query untuk menghindari serangan injeksi pada aplikasi web.