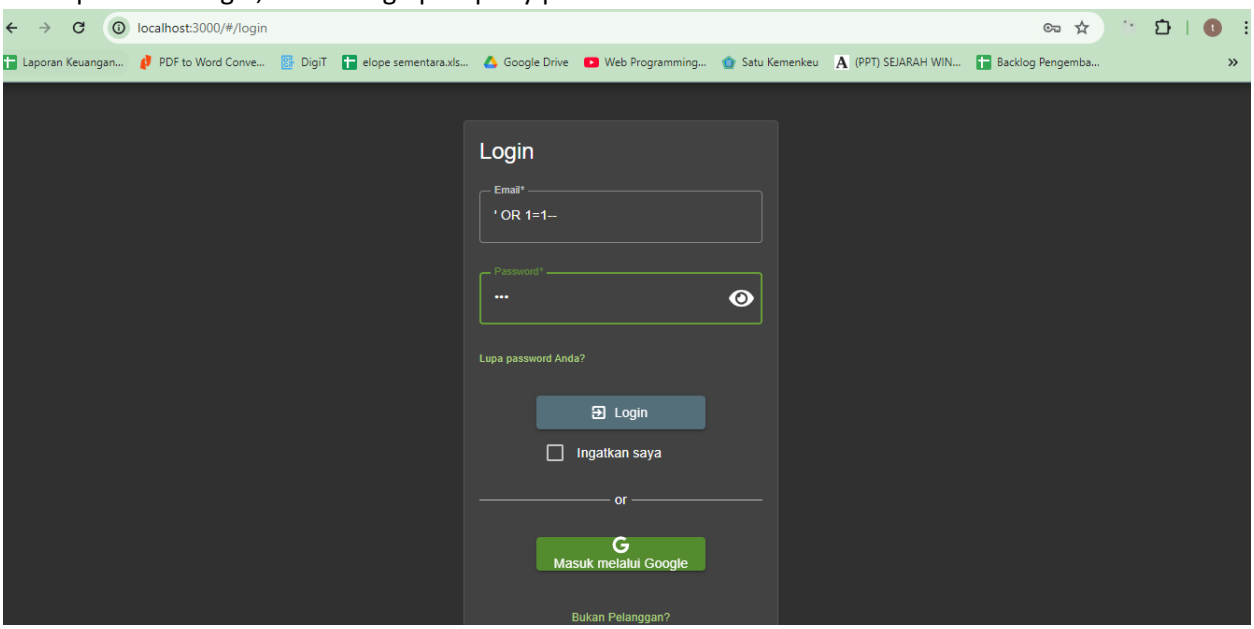
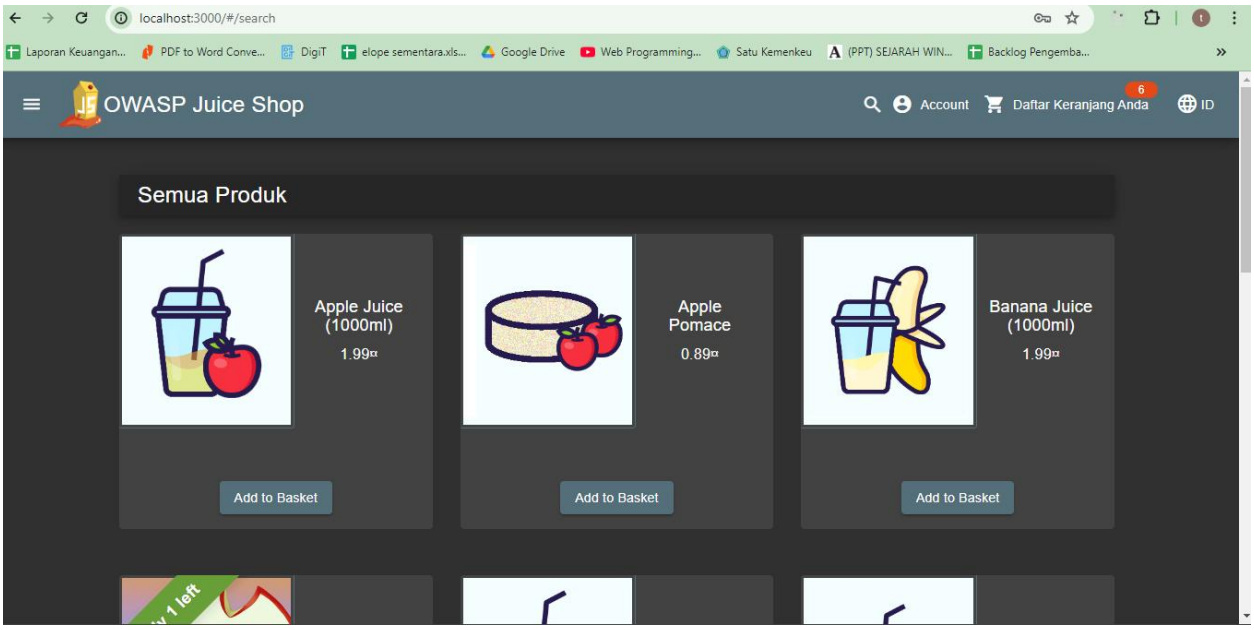
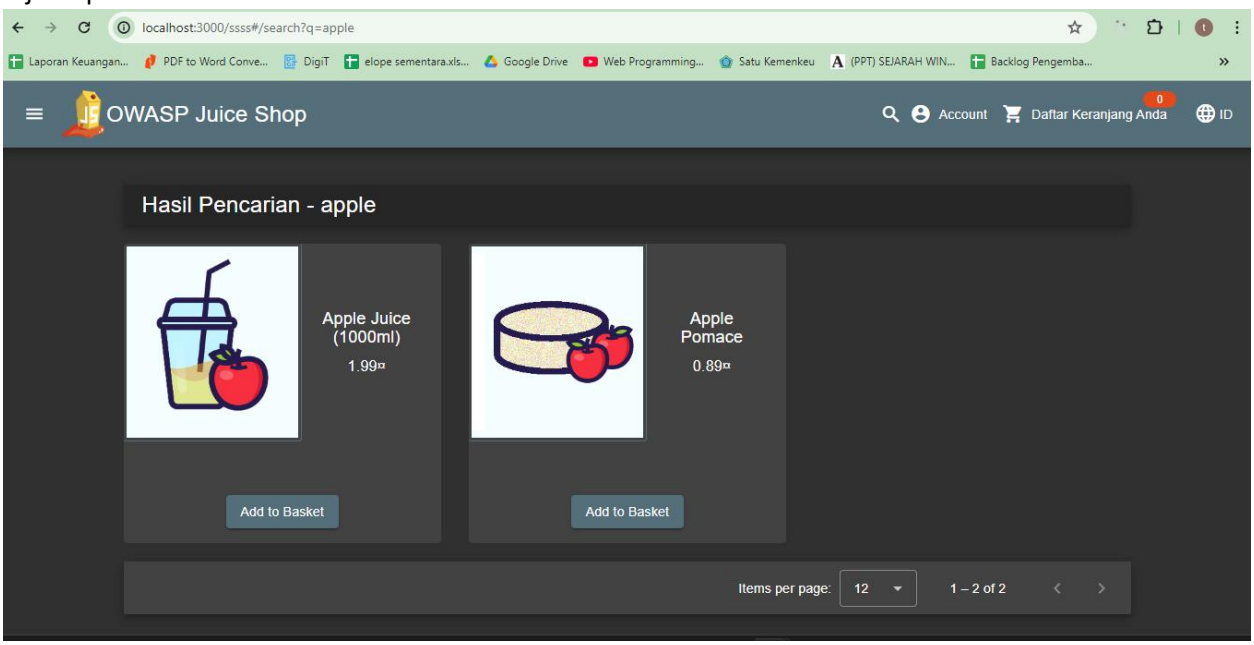
1. Celah pada saat login, user menginput query pada field email ‘ OR 1=1—u

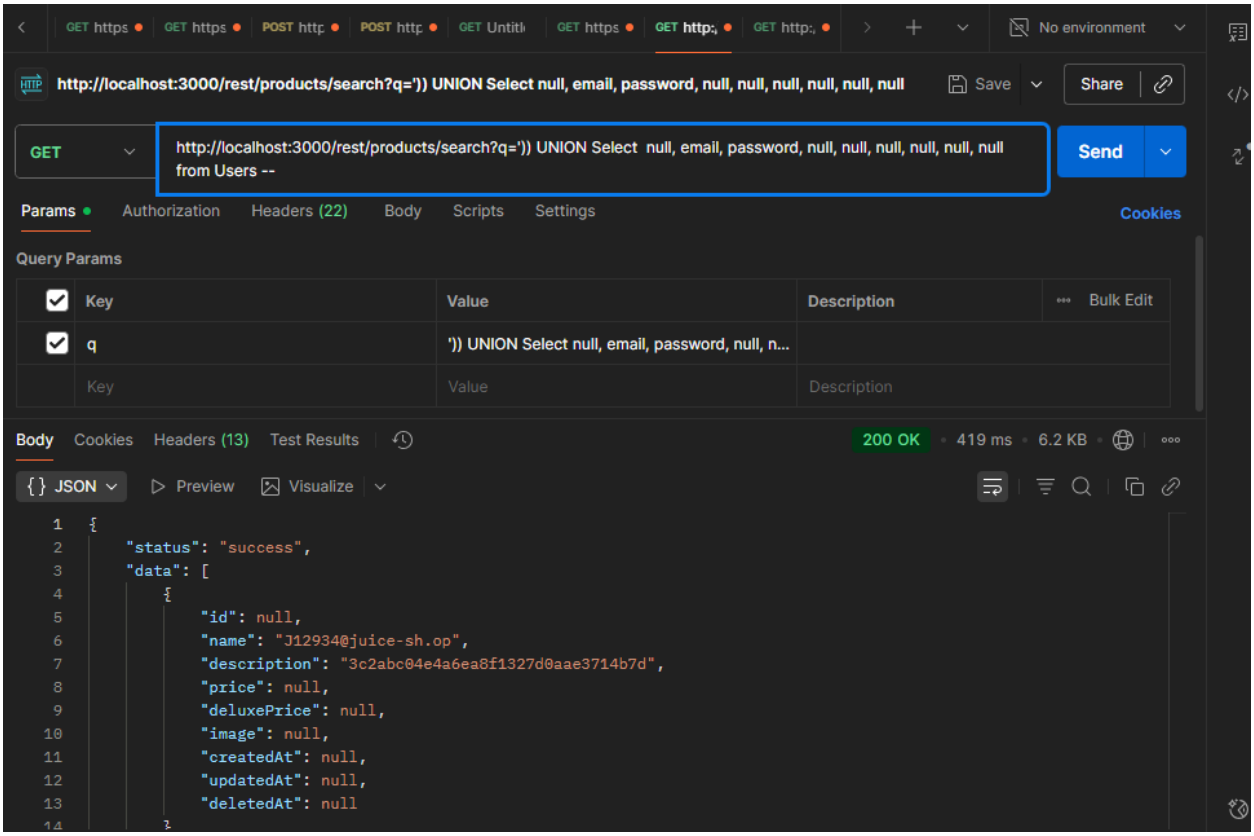




1. Root Cause Anaysis dan rekomendasi:
   Injeksi berhasil dikarenakan belum dipasang sanitasi karakter atas inputan
2. Rekomendasi:
   - Batasi karakter yang boleh diinput (whitelist), terutama untuk field yang tidak boleh mengandung tanda kutip, operator logika, atau komentar SQL
   - Gunakan Parametrized query /prepared statement
3. Verification Scenario
   Hasil yang diharapkan adalah pada saat user menginput payload yang berisi script, system akan melempar error dan tidak dapat memproses

2. Injeksi pada field search





1. Root Cause analysis
   a. **Query dibangun dengan menggabungkan (concatenation) input user langsung ke SQL** — mis. `... WHERE name = ' + q + '` atau `... WHERE (...)` sehingga input `')) UNION Select ... --` memutus konteks dan menyisipkan SQL baru.

b. **Jumlah kolom & tipe cocok** — `UNION SELECT` berhasil hanya jika jumlah kolom dan tipe yang dipilih cocok dengan query asli (attacker menyesuaikannya).
c. **Hasil query dikembalikan ke client tanpa filtering** — aplikasi menampilkan hasil query langsung ke user, sehingga data dari `Users` muncul di keluaran.

2. Rekomendasi
   a. Perbaiki code: **Jangan** pernah concatenation input user ke string SQL — gunakan *parameterized queries* / prepared statements
   b. Validasi & whitelist input
   c. Batasi hak akses database (principle of least privilege)
   d. Hindari menggabungkan banyak tabel sensitif dalam endpoint publik
3. Verification scenario
   a. Input user selalu diperlakukan sebagai data, bukan kode SQL.
   b. String injeksi seperti ')) UNION Select ... -- tidak memodifikasi struktur query — dianggap sebagai kata pencarian literal.
   c. Endpoint tidak mengembalikan data dari tabel lain (mis. Users). Hasil hanya berasal dari tabel products.
   d. Response selalu ter-encode/terstruktur (JSON), tidak ada stack trace atau query SQL di body.
   e. Query dibatasi (LIMIT), dan panjang input dibatasi.
   f. Jika terjadi error internal, client menerima pesan generik (500) saja; detail error hanya di log server.
   g. DB user untuk service hanya punya privilege yang diperlukan (least privilege).