Praktikum Keamanan Jaringan

OWASP Juice Shop – Injection

Oleh:

Aldo Faiz Winarno (3122640039)

D4 LJ IT B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN 2023

Injection

Informasi Dasar

OWASP Top Ten adalah daftar risiko keamanan aplikasi web paling kritis yang diidentifikasi oleh Open Web Application Security Project (OWASP). Kerentanan injeksi terdaftar sebagai salah satu dari 10 risiko keamanan teratas dalam aplikasi web.

Serangan injeksi terjadi ketika input pengguna yang tidak dipercaya tidak divalidasi atau dibersihkan dengan benar, memungkinkan kode berbahaya disuntikkan ke dalam database aplikasi atau lingkungan eksekusi. Hal ini dapat menyebabkan berbagai pelanggaran keamanan yang serius, seperti akses tidak sah ke data sensitif, manipulasi data, dan eksekusi kode berbahaya.

Kategori OWASP Top 10 Injection mencakup berbagai jenis serangan injeksi, seperti injeksi SQL, injeksi LDAP, dan injeksi XML. Injeksi SQL adalah jenis serangan injeksi yang paling umum dan terkenal, di mana penyerang menyuntikkan pernyataan SQL berbahaya ke bidang masukan pengguna, mengeksploitasi kerentanan untuk mengambil, memodifikasi, atau menghapus data sensitif.

Skenario 1

String query = "SELECT * FROM accounts WHERE custID='" + request.getParameter("id") + " ' ";

Serangan injection yang mungkin terjadi pada kode ini adalah SQL Injection. Pada serangan ini, attacker dapat memanipulasi input parameter "id" untuk menyuntikkan kode SQL yang tidak sah ke dalam string query, seperti mengganti nilai "id" dengan "1' OR 1=1 --" yang akan mengubah string query menjadi "SELECT * FROM accounts WHERE custID='1' OR 1=1 --'", dan ini akan mengeksekusi perintah SQL yang tidak diinginkan.

Skenario 2

Query HQLQuery = session.createQuery("FROM accounts WHERE custID='" + request.getParameter("id") + " ' ");

Serangan injection yang mungkin terjadi pada kode ini adalah HQL Injection. Pada serangan ini, attacker dapat memanipulasi input parameter "id" untuk menyuntikkan kode HQL yang tidak sah ke dalam query, seperti mengganti nilai "id" dengan "1' OR 1=1 --" yang akan mengubah query menjadi "FROM accounts WHERE custID='1' OR 1=1 --'", dan ini akan mengeksekusi query HQL yang tidak diinginkan.

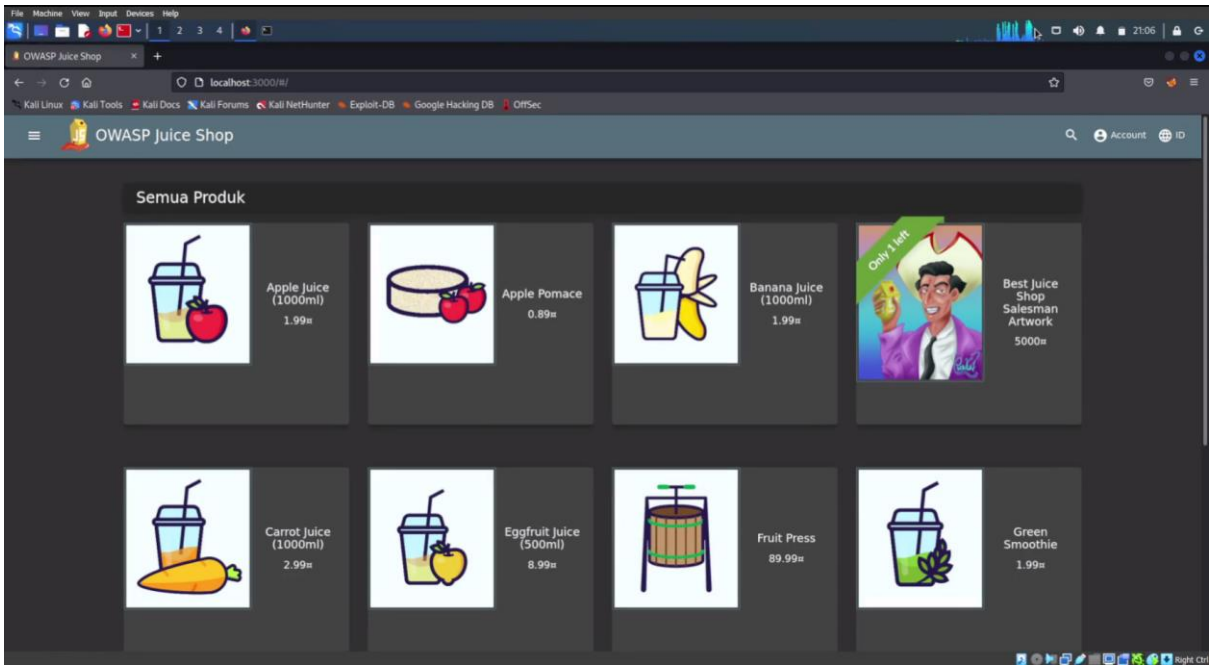
Dalam kedua skenario , penyerang mengubah nilai parameter 'id' di browser mereka untuk mengirim: **'UNION SLEEP(10);-- http://example.com/app/accountView?id=' UNION SELECT SLEEP(10);--** attacker mencoba melakukan serangan SQL Injection dengan memasukkan payload ' UNION SELECT SLEEP(10);-- ke dalam parameter "id". Payload ini akan menggabungkan query asli dengan query yang ditambahkan oleh attacker, yaitu SELECT SLEEP(10), yang akan menunda eksekusi query sebelumnya selama 10 detik. Tanda "--" digunakan untuk mengakhiri query asli dan mengabaikan karakter lain yang mungkin ada pada query. Ini mengubah arti dari kedua Query untuk mengembalikan semua rekaman dari tabel akun. Serangan yang lebih berbahaya dapat mengubah atau menghapus data atau bahkan menjalankan prosedur tersimpan.

Untuk mencegah serangan injeksi, pengembang harus menerapkan praktik pengkodean yang aman dan menggunakan kueri berparameter atau pernyataan yang disiapkan untuk memvalidasi dan membersihkan input pengguna. Selain itu, validasi masukan dan penyandian keluaran harus dilakukan untuk memastikan bahwa masukan pengguna diformat dan ditampilkan dengan benar untuk mencegah serangan skrip lintas situs (XSS). Juga disarankan untuk menggunakan alat seperti firewall aplikasi web (WAF) dan pemindai kerentanan untuk mengidentifikasi dan mengurangi potensi kerentanan injeksi.

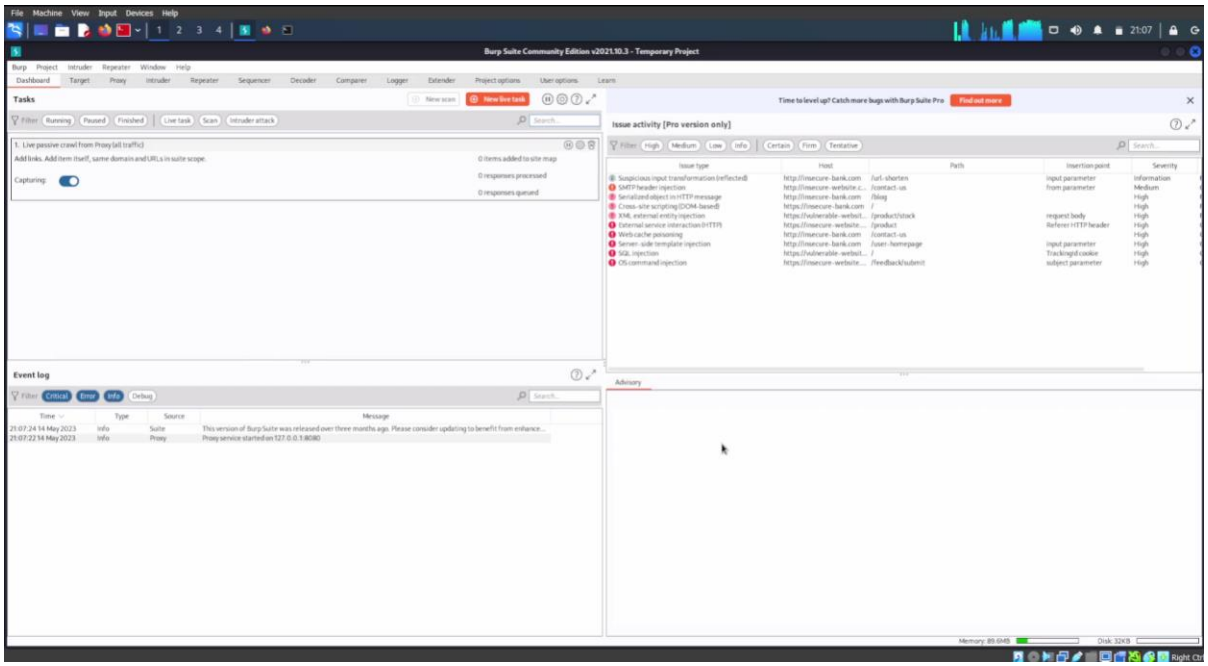
Percobaan

Pada percobaan ini akan masuk/login sebagai admin.

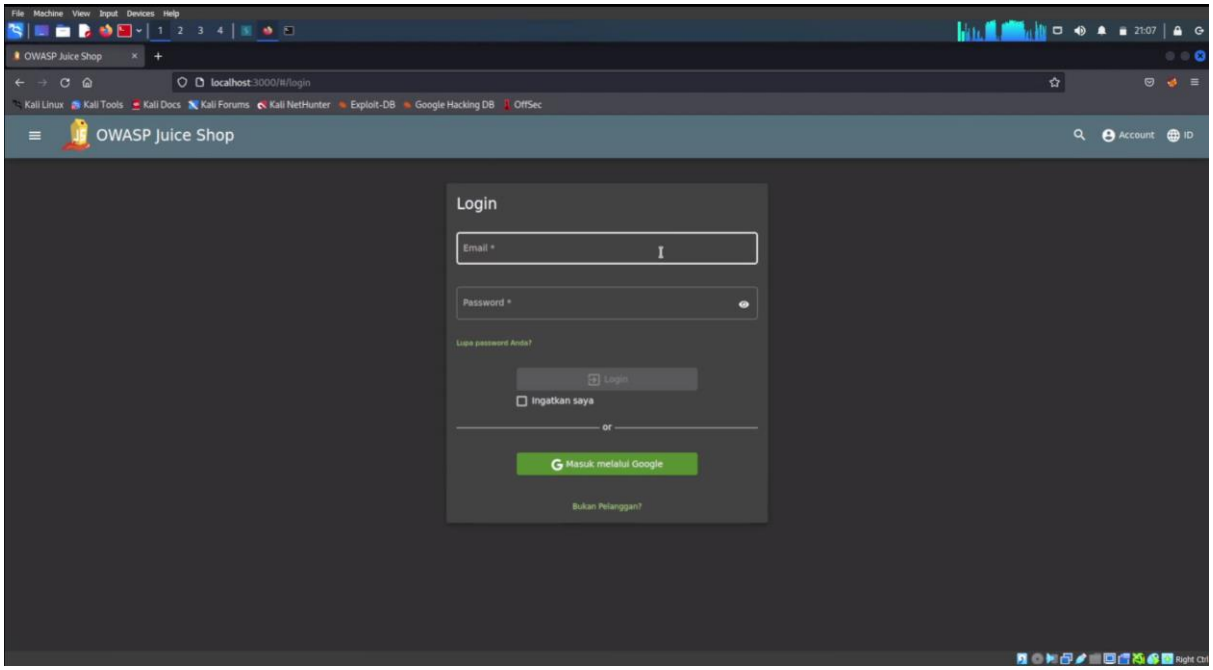
1. **Buka Aplikasi Juice Shop.**



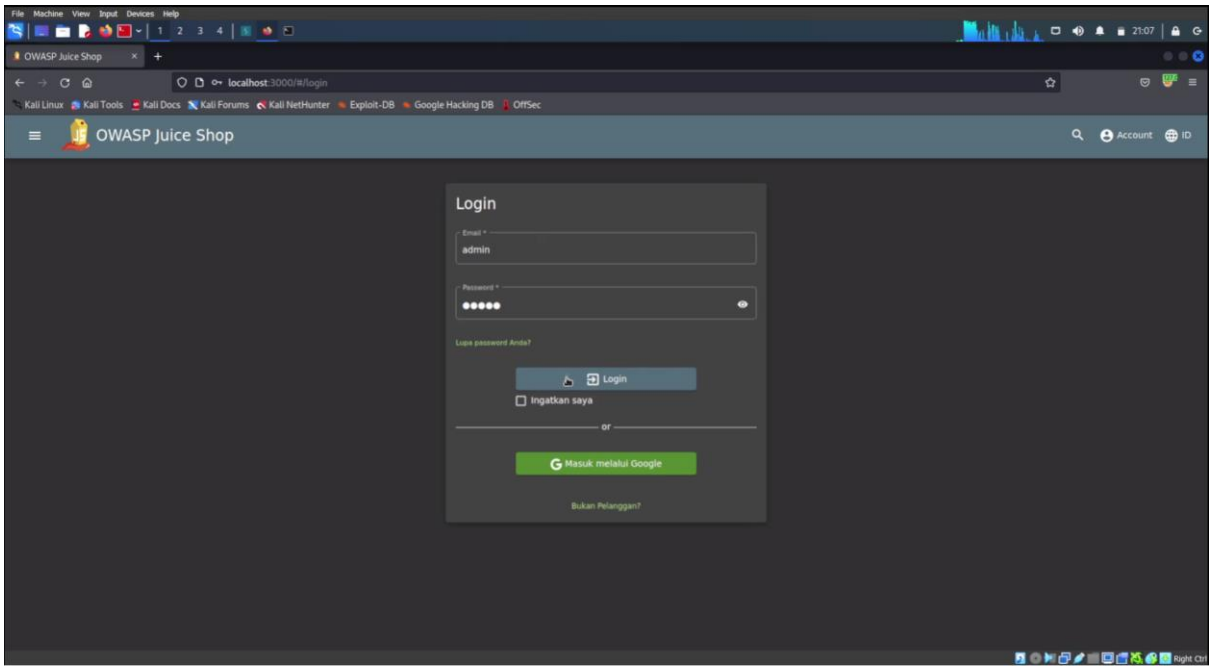
2. Buka Burpsuite.



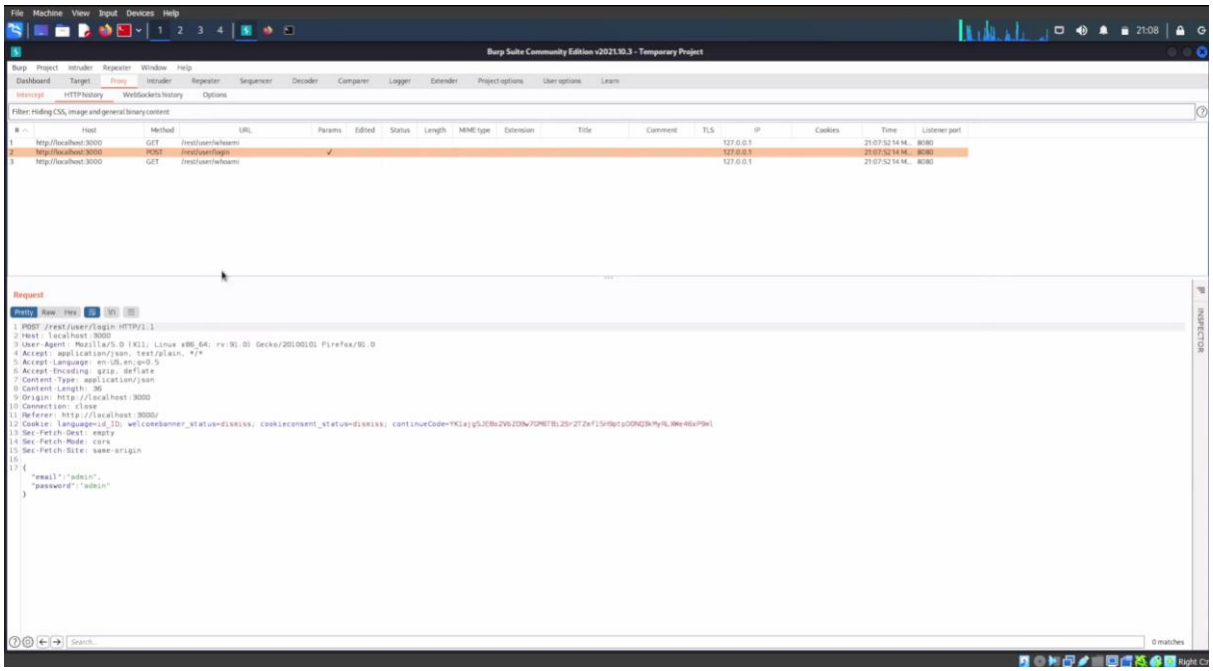
3. Masuk halaman login.



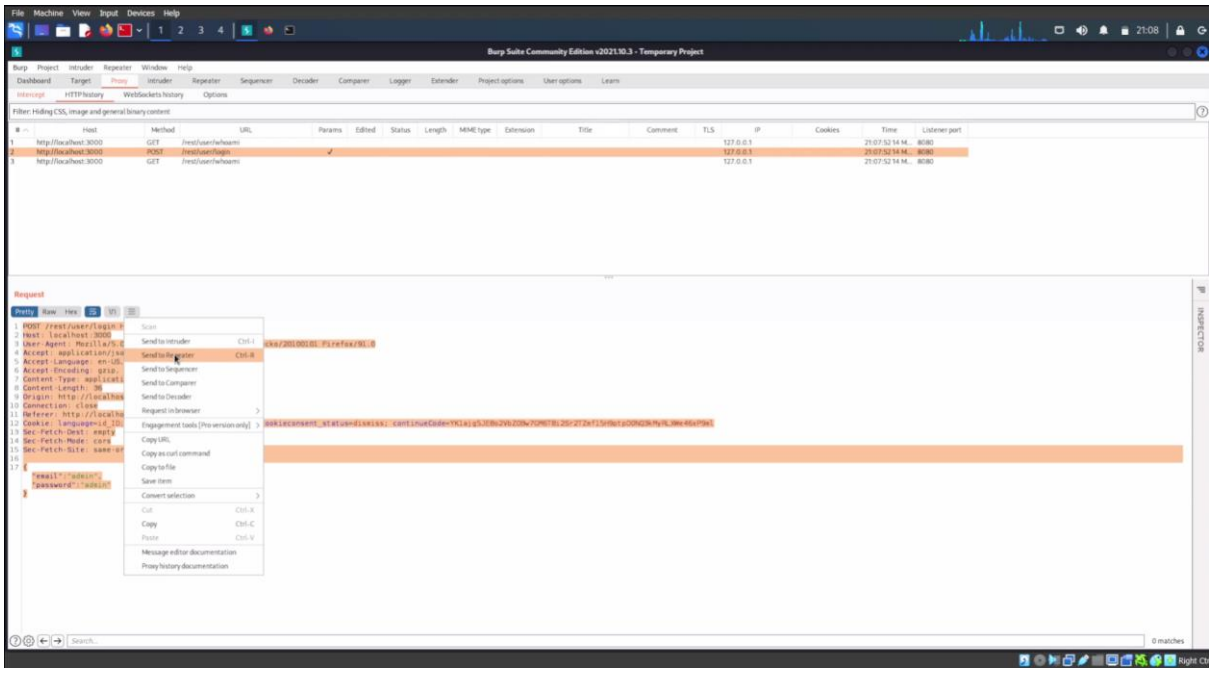
4. Masukkan email dan password, pastikan proxy menyala.



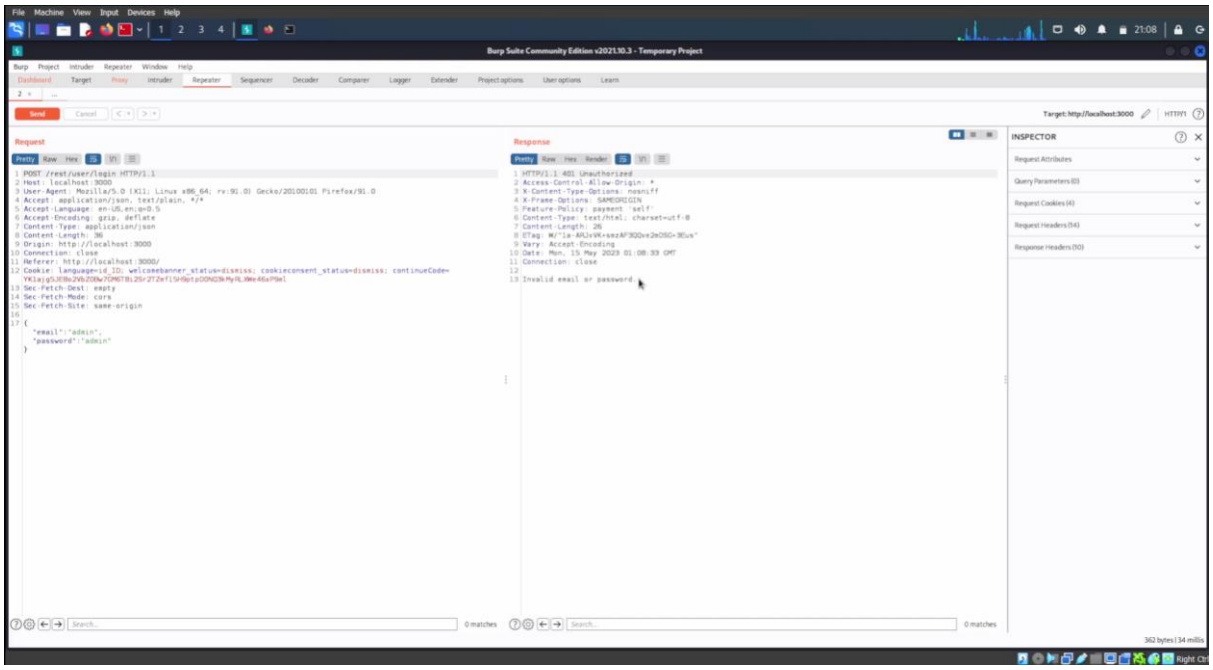
5. Pada burpsuite, pilih menu Proxy -> HTTP history dan pilih URL /rest/user/login.



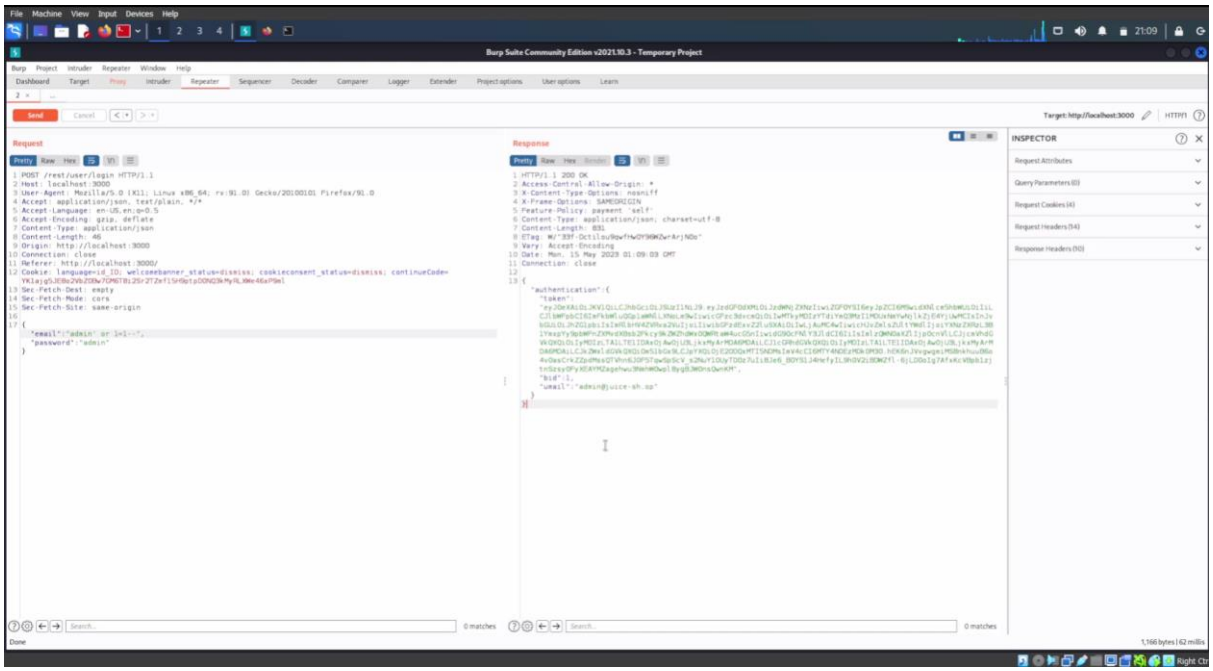
6. Lakukan Send to Repeater.



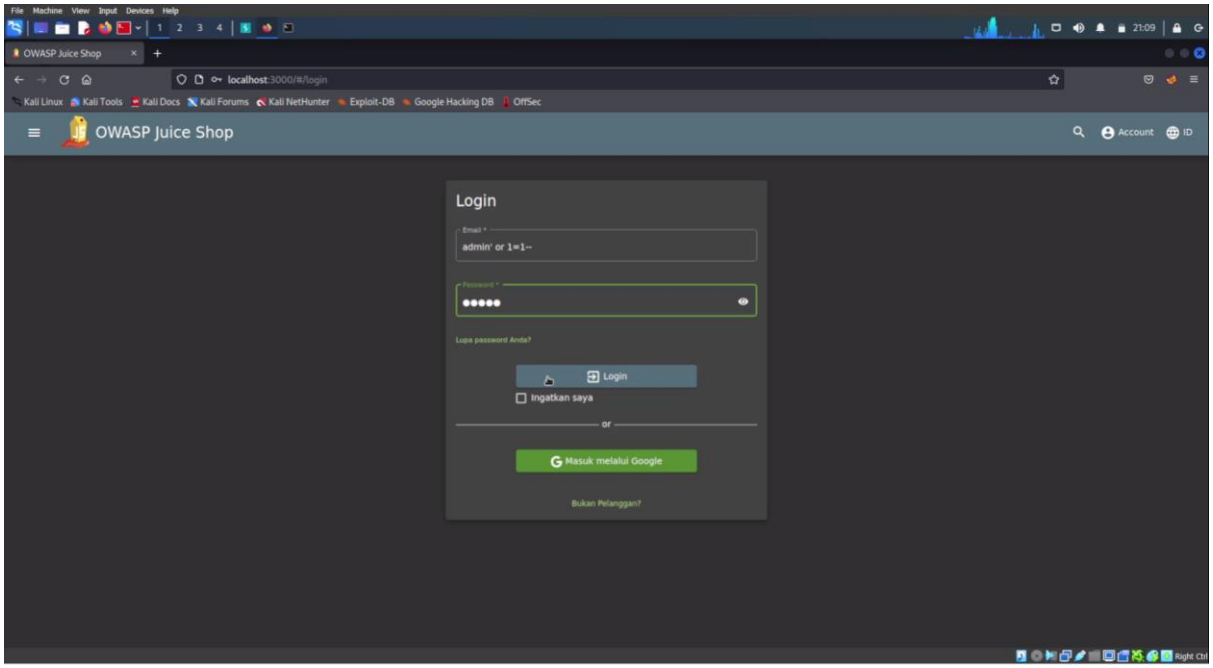
7. pilih menu Repeater, lakukan Send. (Terdapat keterangan Invalid)



8. Tambahkan ' or 1=1-- pada email. (Terdapat keterangan berhasil)



9. Masuk ke halaman login dan isi email dan password dengan tambahan sintax sebelumnya, pastikan proxy mati.



10. Dapat login sebagai admin.