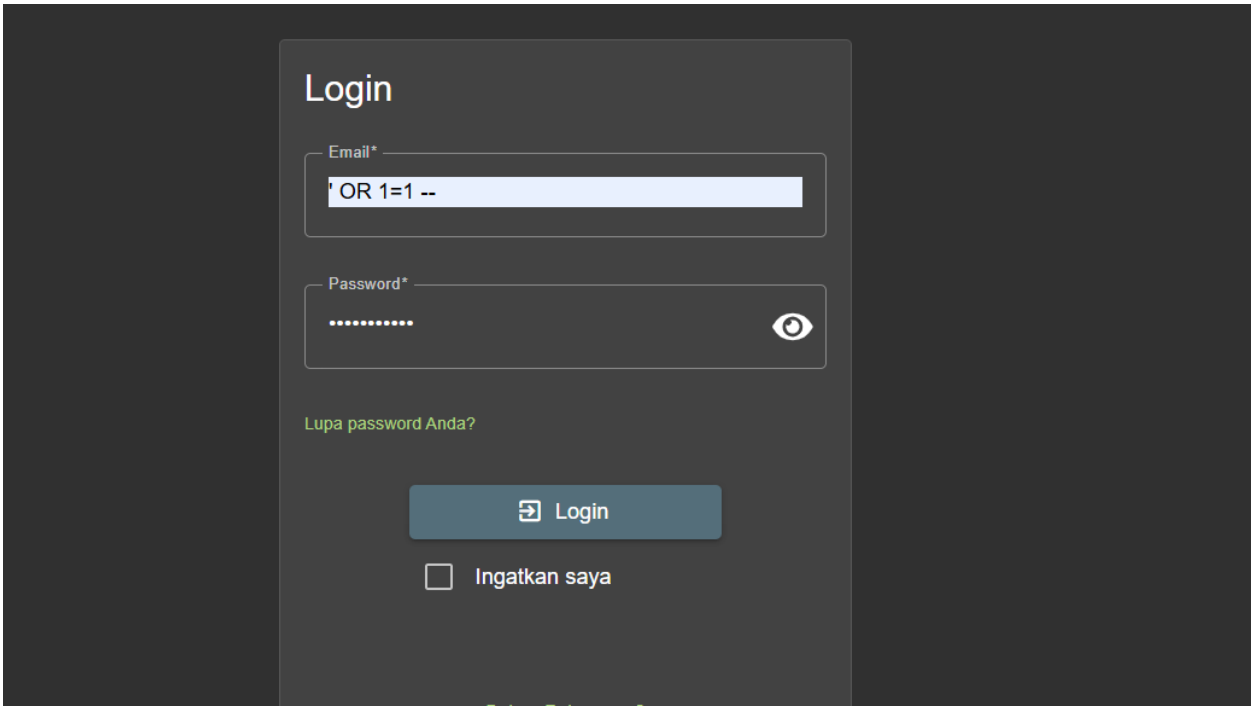
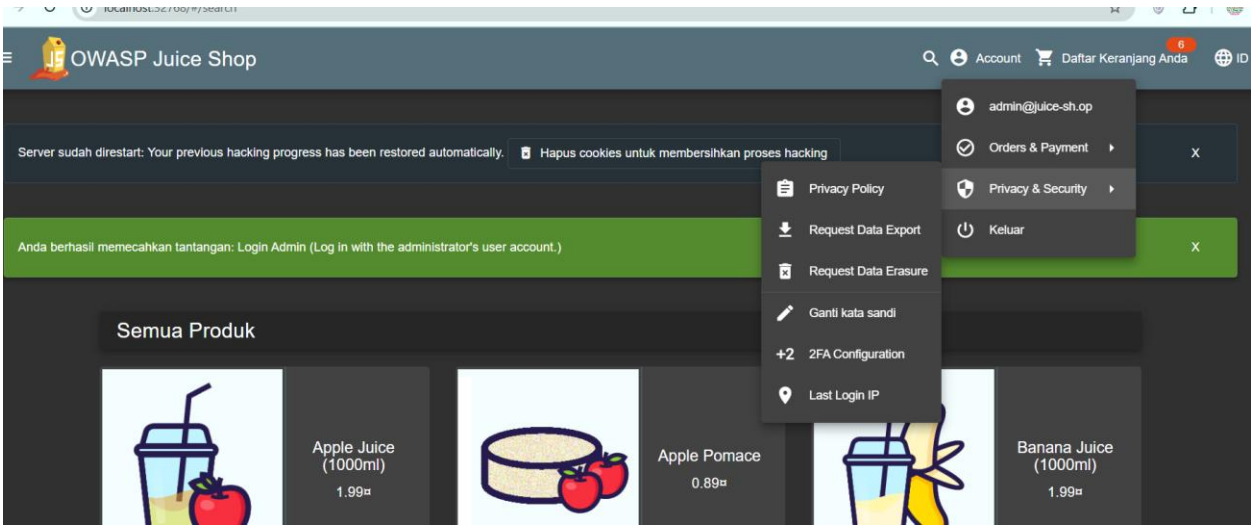
Temuan SQLi

1. Sql Injection





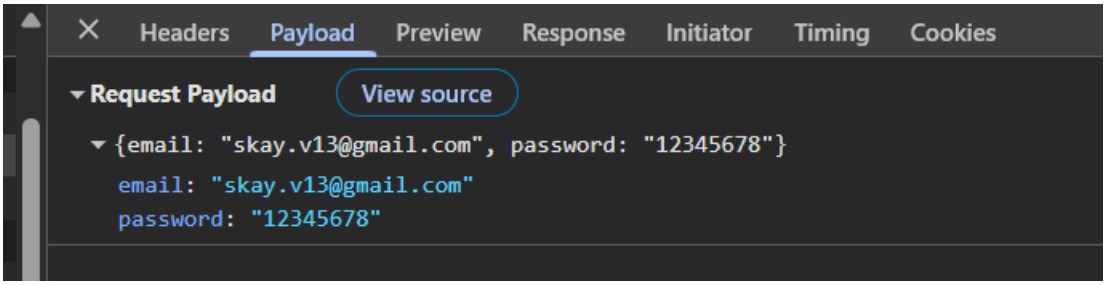
Penyebab

Pada halaman login, bisa dilakukan SQL Injection di form username dan passwordnya, hal ini dikarenakan string concatenation.

Rekomendasi

Untuk pencegahannya bisa menggunakan Parameterize query

2. Password ga dienkript



Ketika login Email dan Passwordnya tidak di enkript

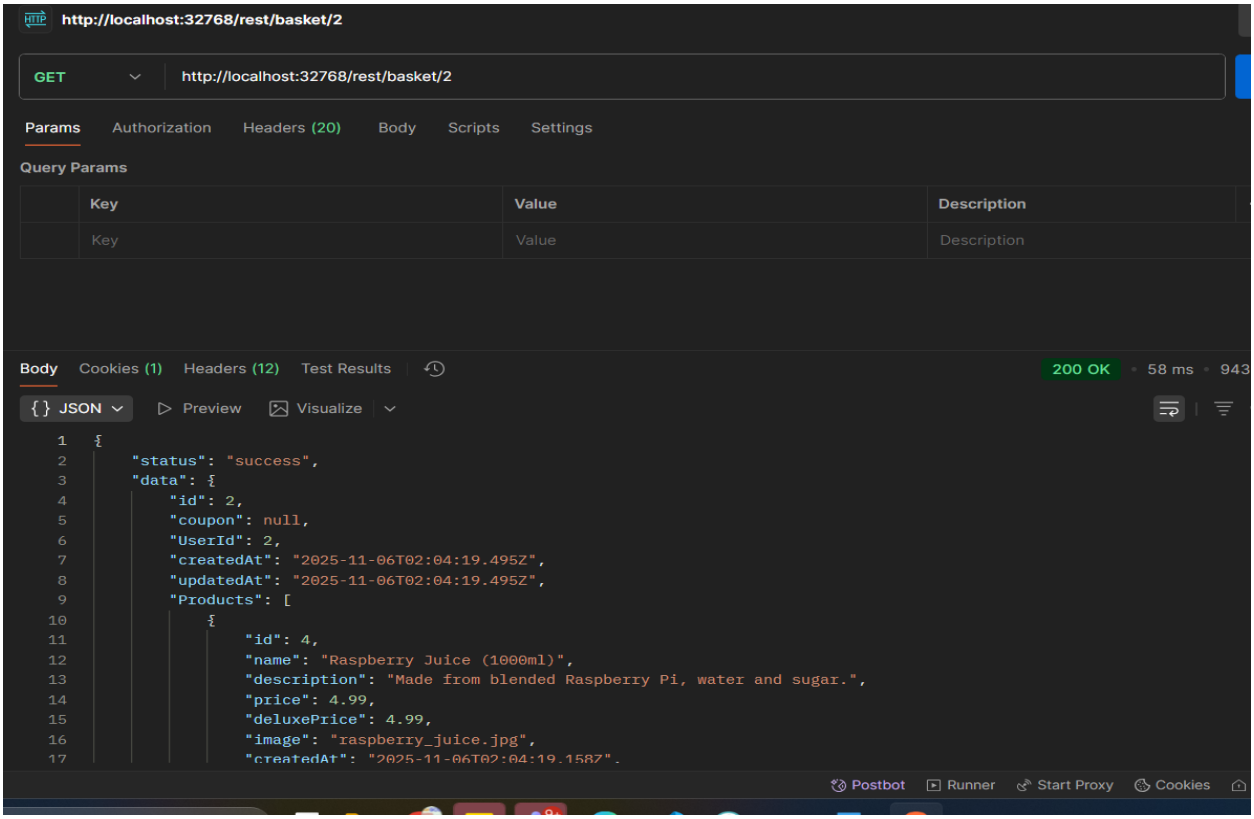
Penyebab

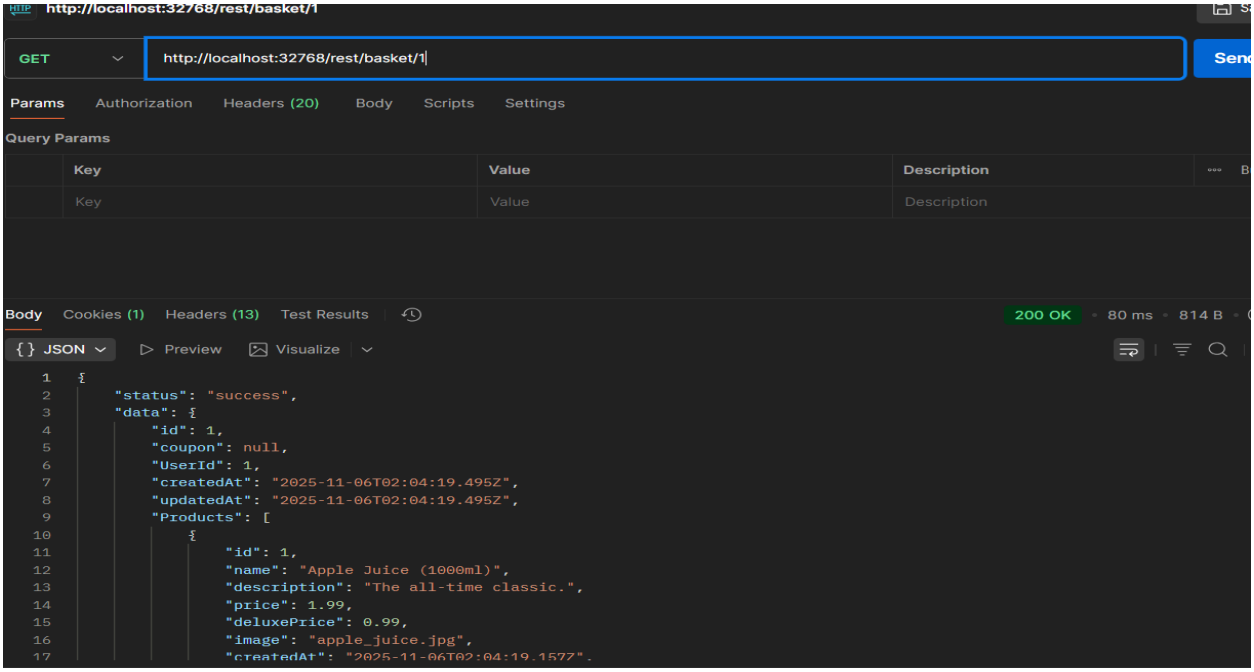
Password tidak di enkript

Rekomendasi

Password di enkript

3. Broken Access Control (BAC)



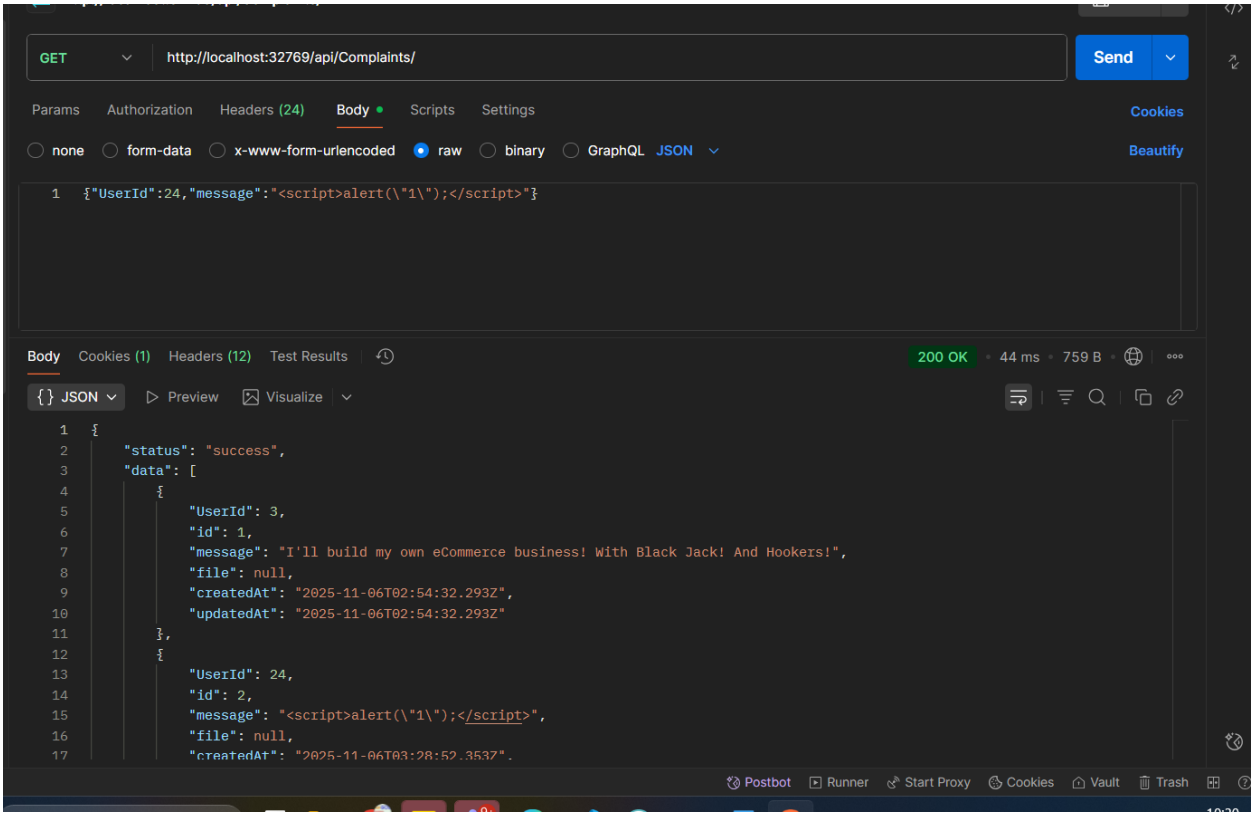


Penyebab

Dengan memakai token yang sama, bisa memanggil keranjang milik orang lain, karena tidak ada validasi akses kontrolnya

Rekomendasi

Sistem harus memvalidasi terhadap keranjang dari requesternya



Pada menu complaints Ketika mensubmit complain yg method POST, saya ubah method nya menjadi GET. Saya bisa melihat complain dari semua user

Penyebab

Tidak ada validasi pada Method GET Complaint

Rekomendasi

Methodnya harus divalidasi bahwa hanya admin saja yg boleh lihat