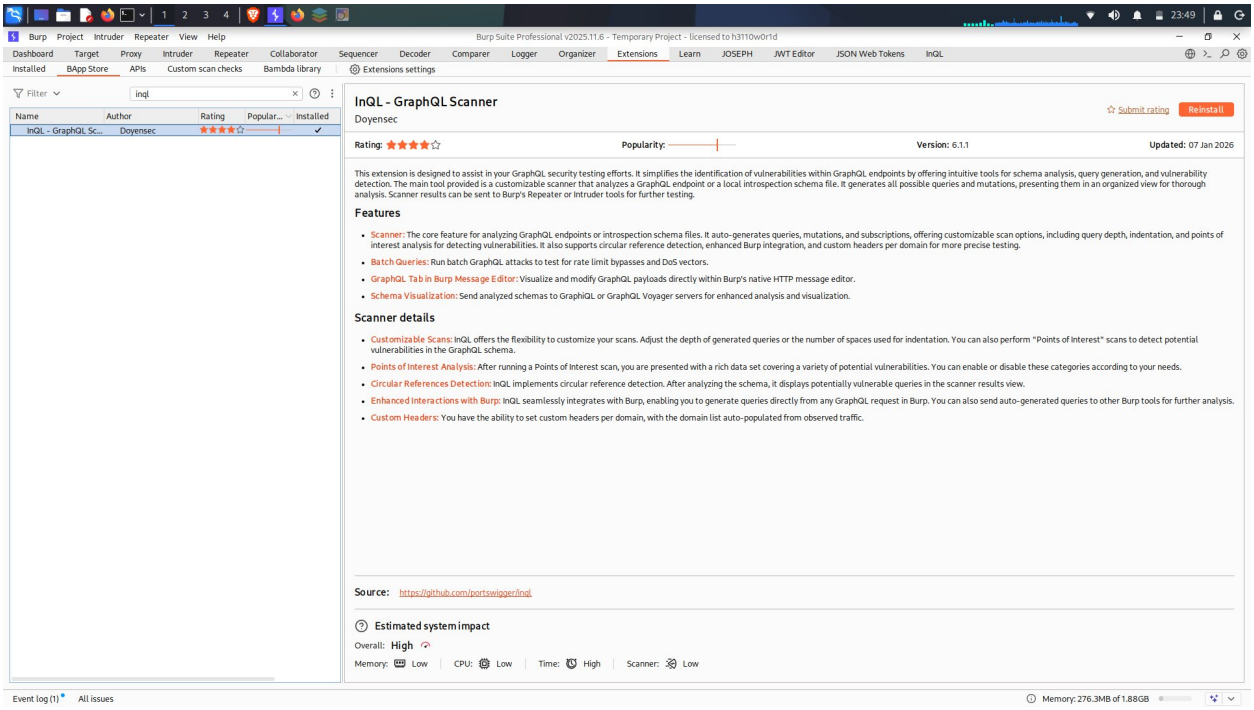
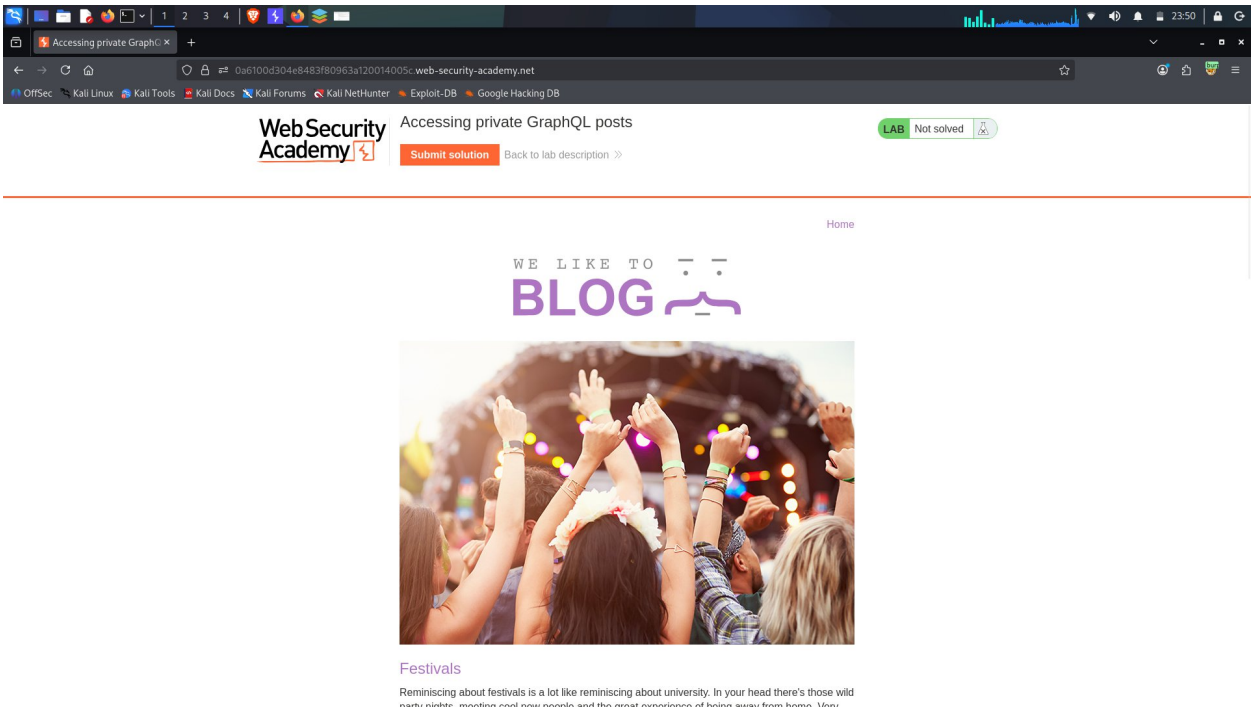
Accessing private GraphQL posts

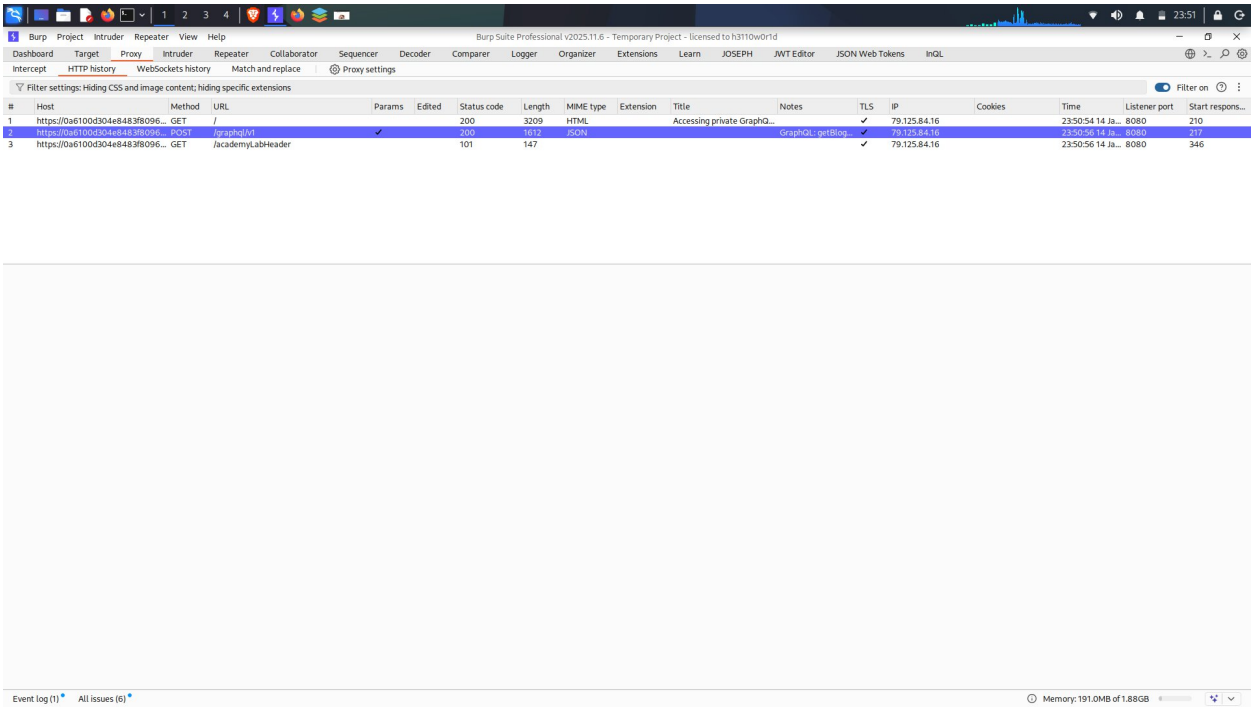
Langkah pertama download ekstensi tools seperti di gambar



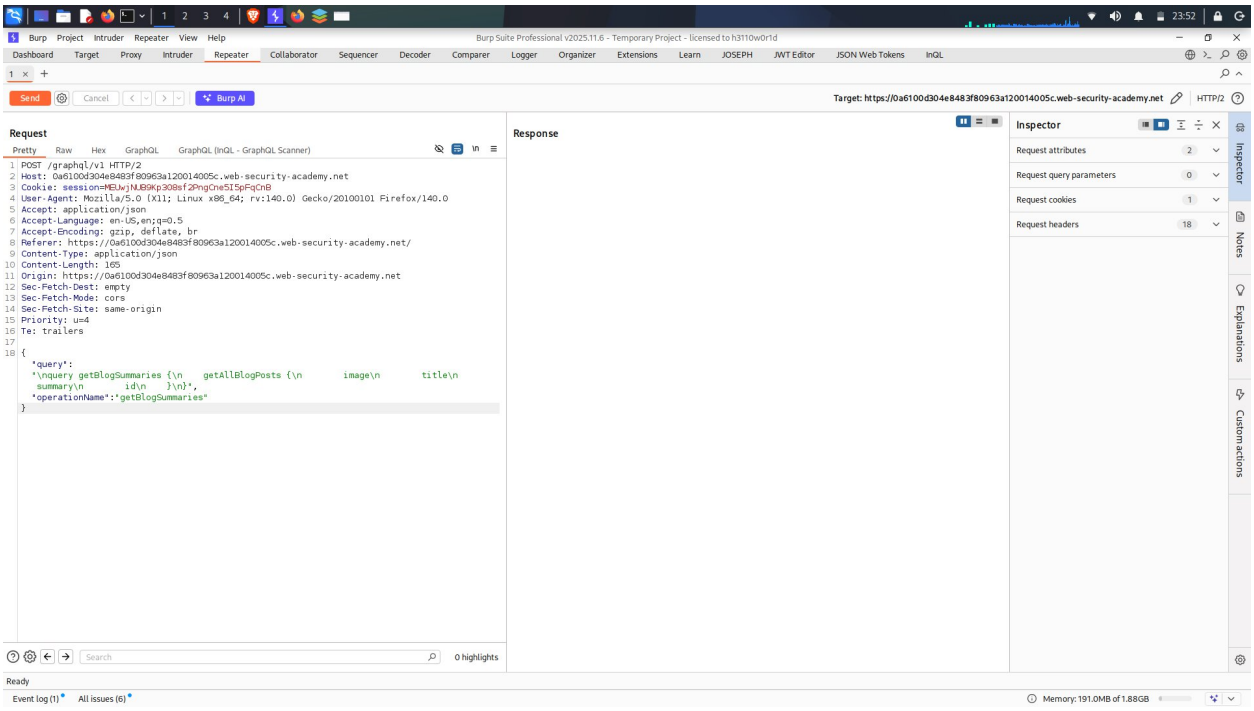
Lalu buka lab nya dan nyalakan foxyproxy,buka burpsuite jangang di intercept



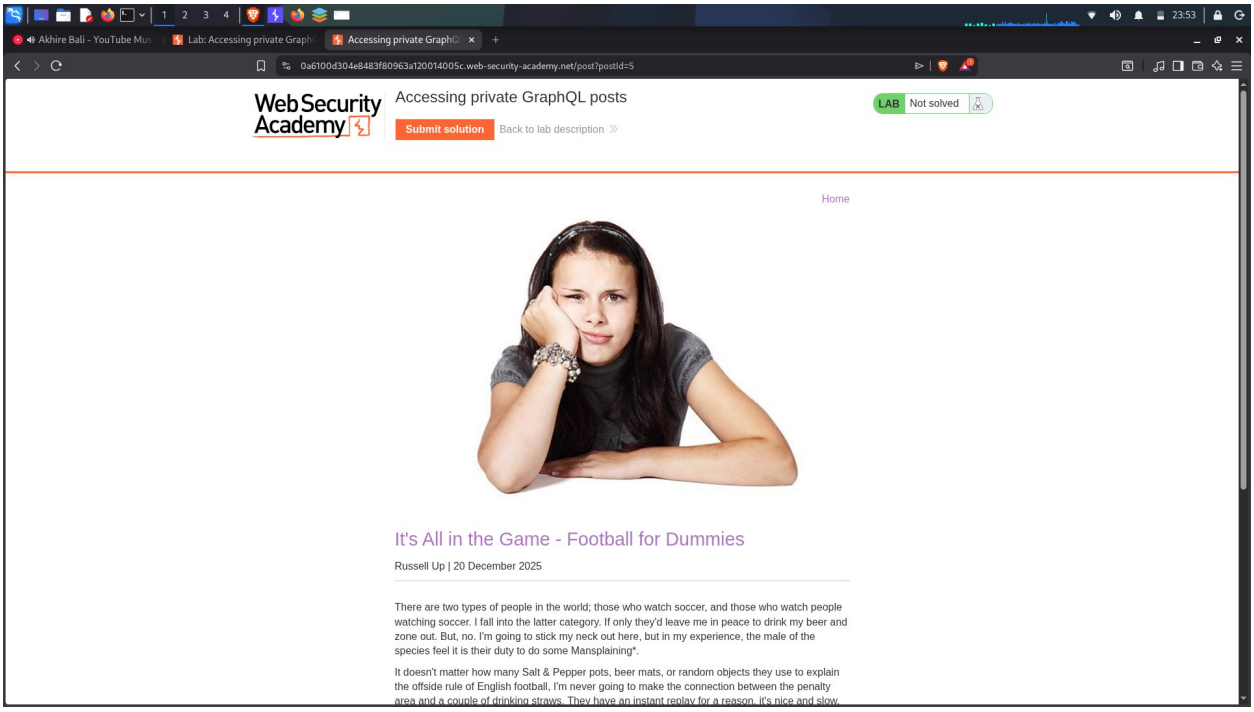
Dan ini burpsuite nya



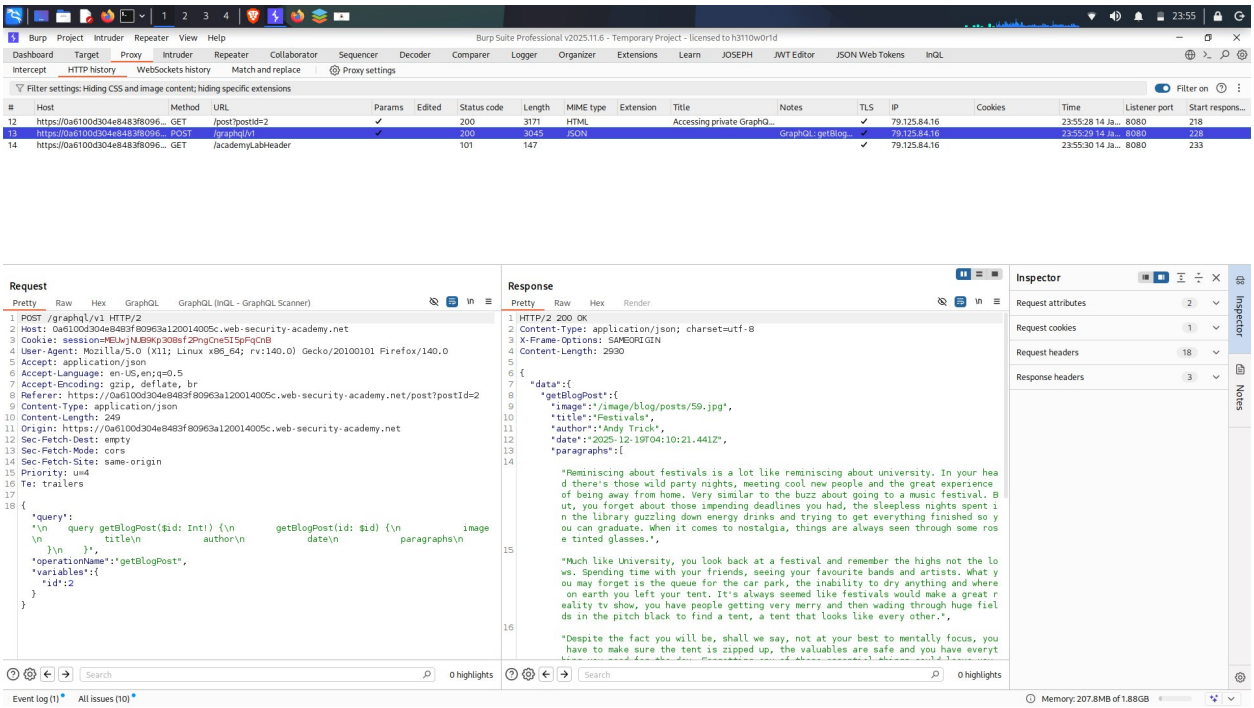
Lalu send to repeater yang ke dua



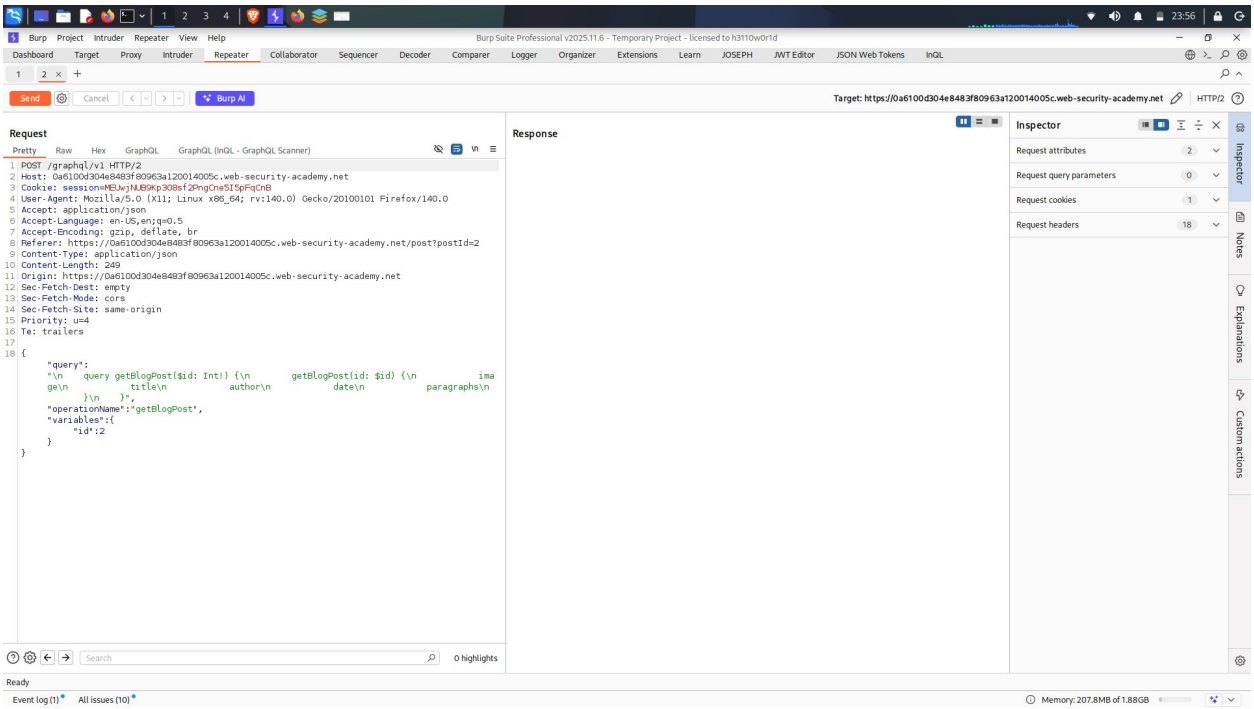
Lalu kemudian buka web lab nya dan klik viewpost



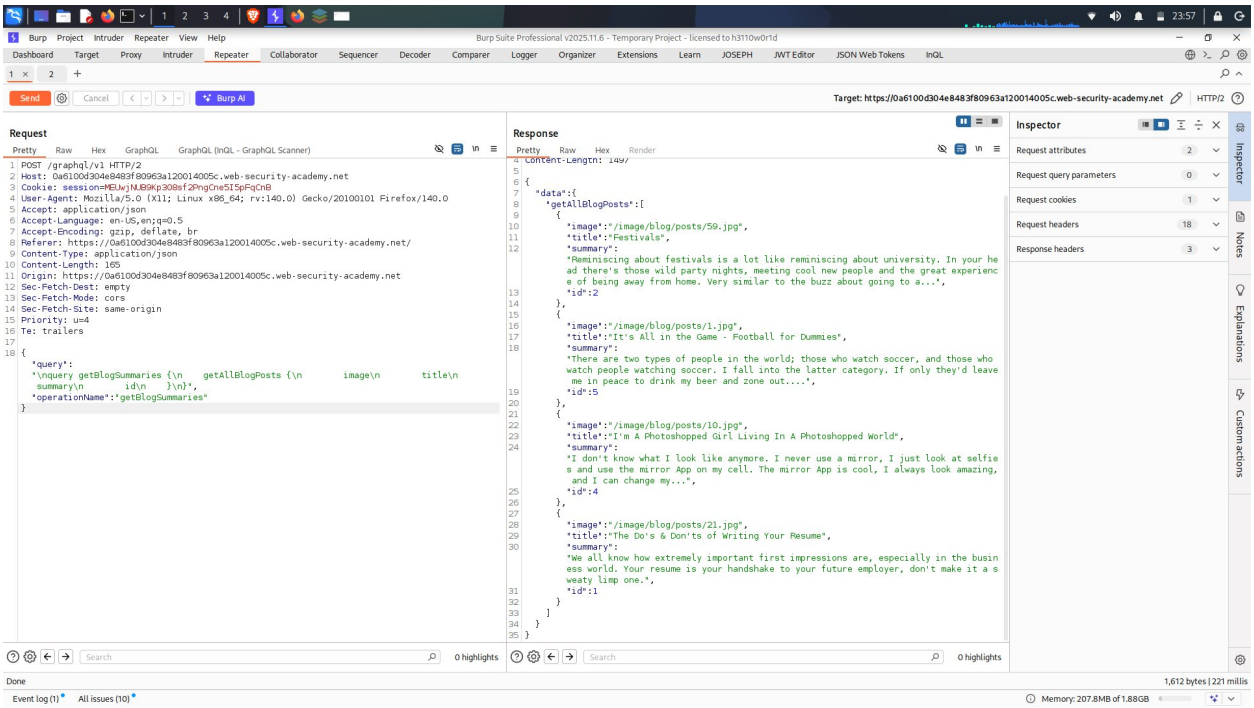
Lalu buka kembali burpsuite nya



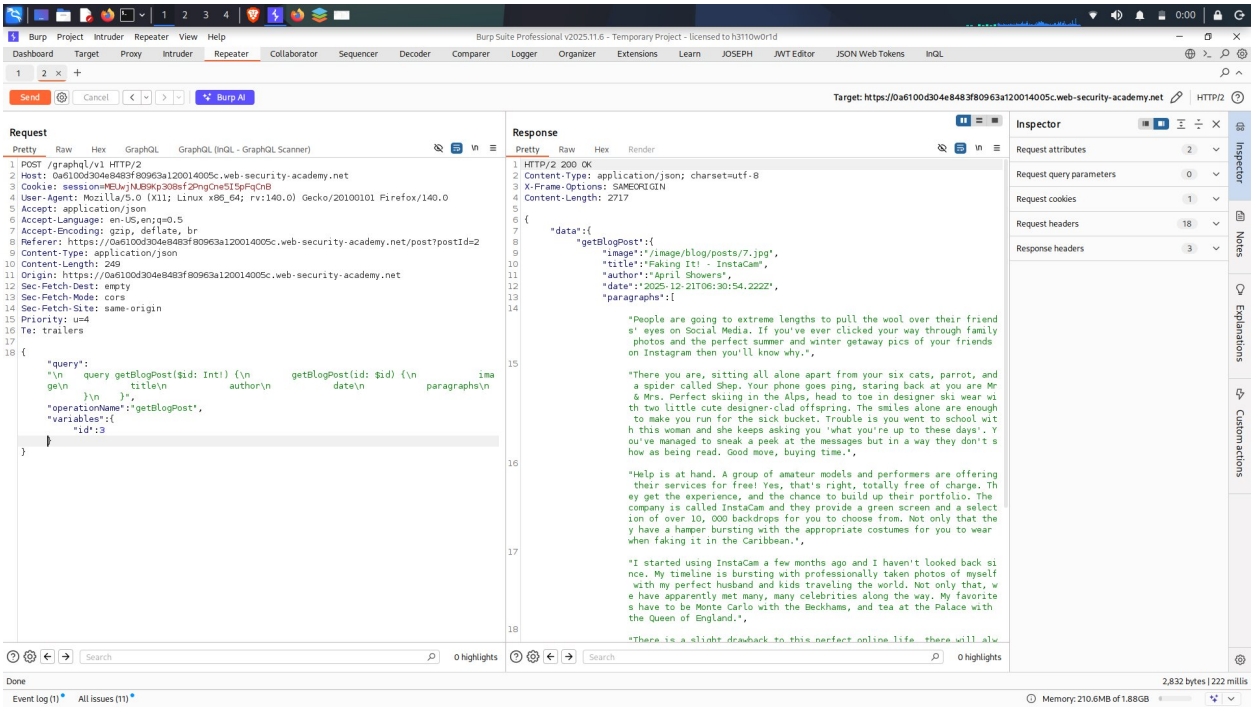
Pilih nomor 2 dan send to repeater sebelum nya clear history dulu sebelum membuka view post



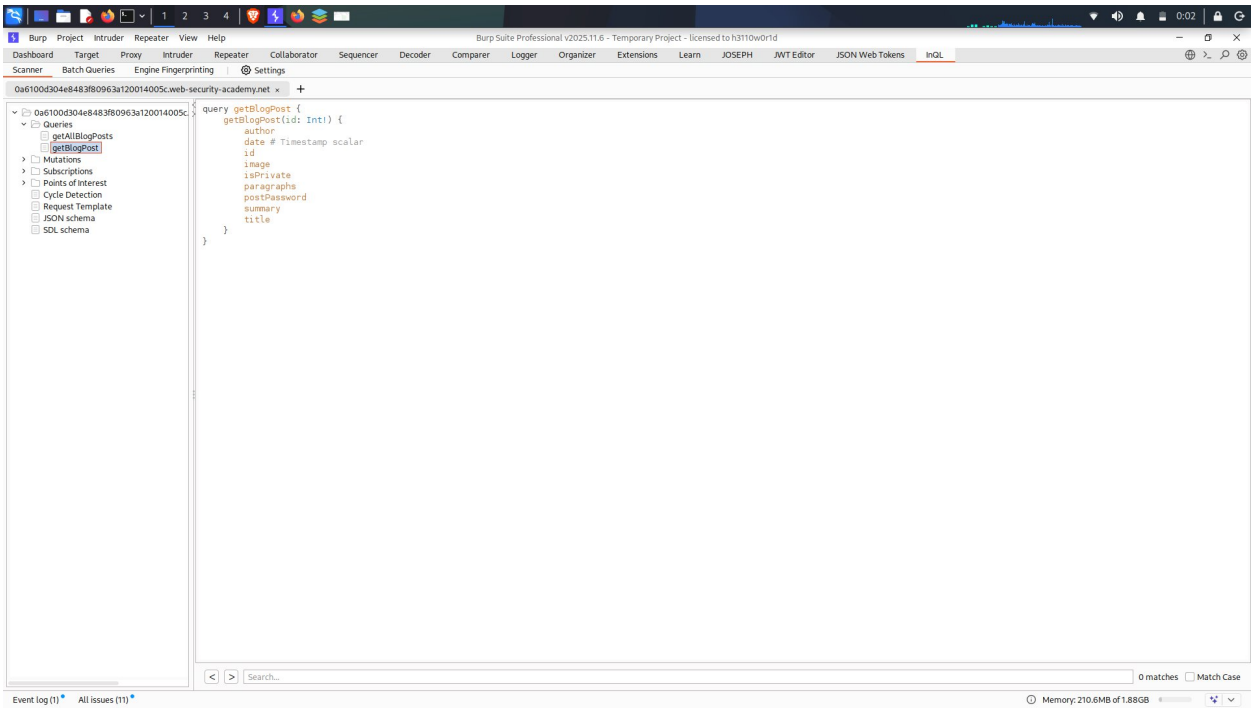
Lalu kemudian klik send blog utama atau pertama yang



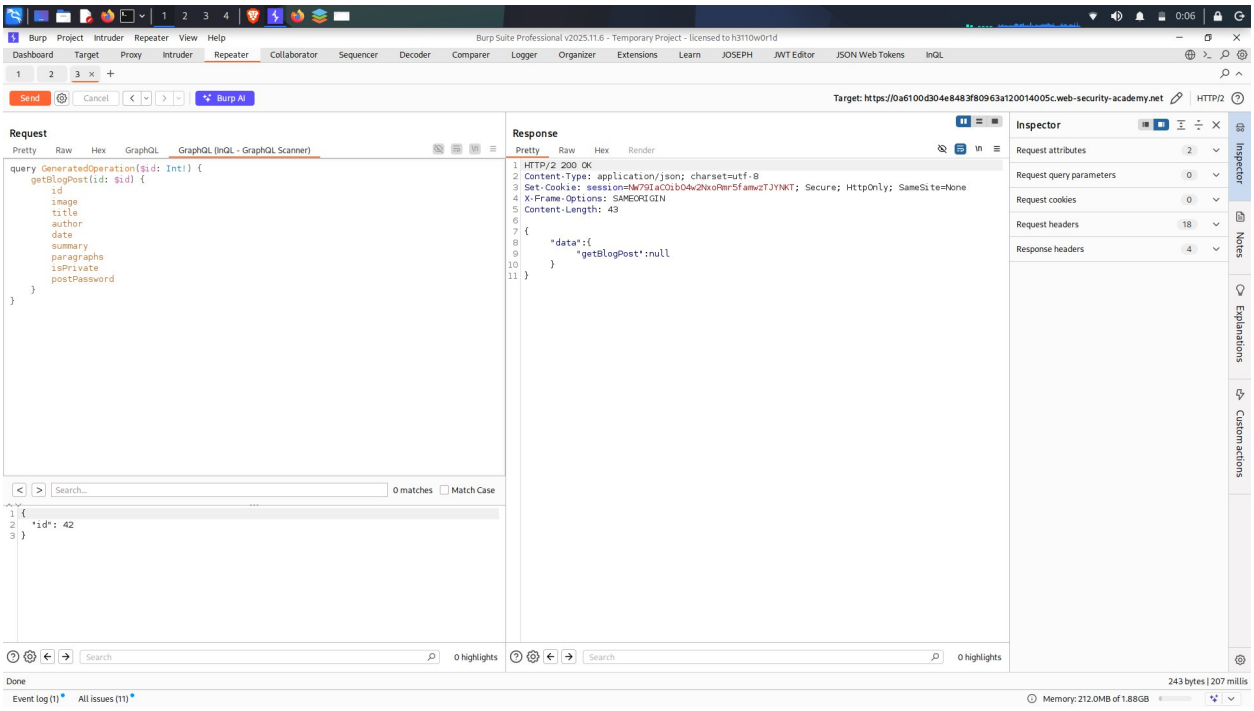
Saat blog utama di send terdapat anomali yaitu "id": 3 di sembunyikan lalu coba rubah “id”:2 menjadi 3 di repeater kedua atau viewpost tadi



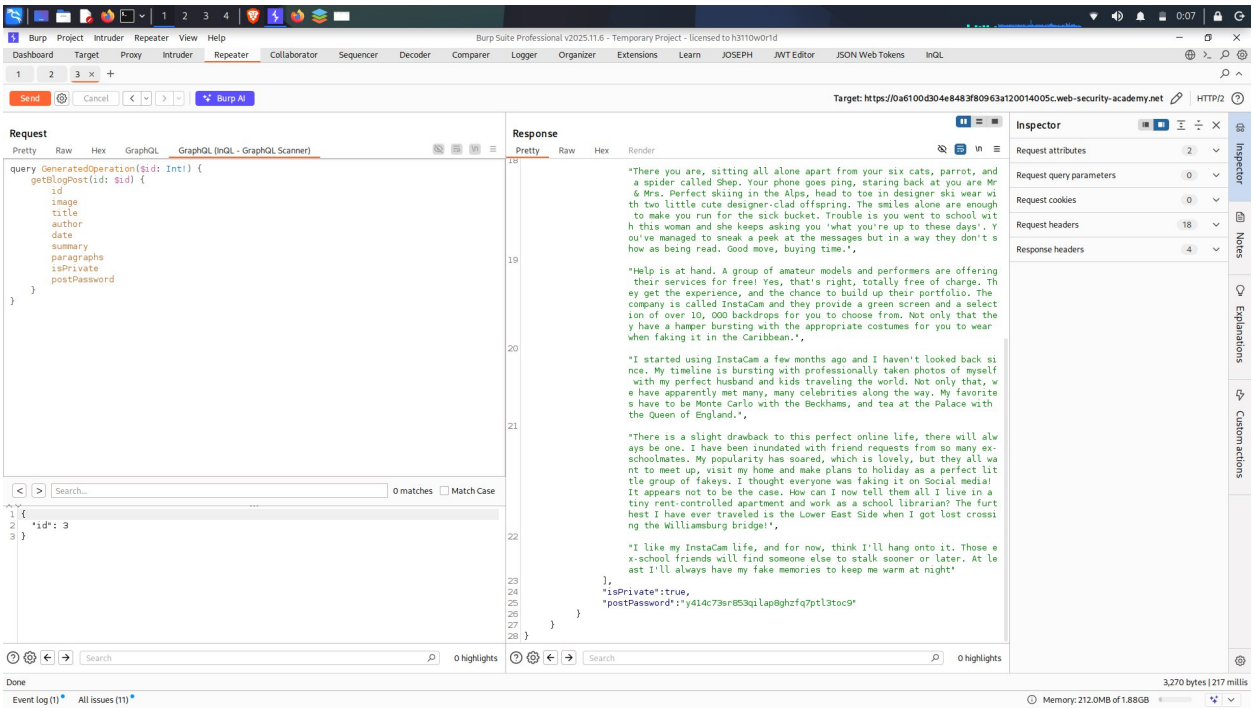
Dan ternyata ada.memang id 3 di sembunyikan lalu copyurl yang repeater pertama atau blog utama kemudian paste di INQL kemudian pastekan dan klik analyze dan amati



Saat di analyze di INQL terdapat PostPassword saat mengklik queries>getblogposts kemudian coba send to repeater getblogposts tadi kemudian klik Graphql atau inql Graphql dan send

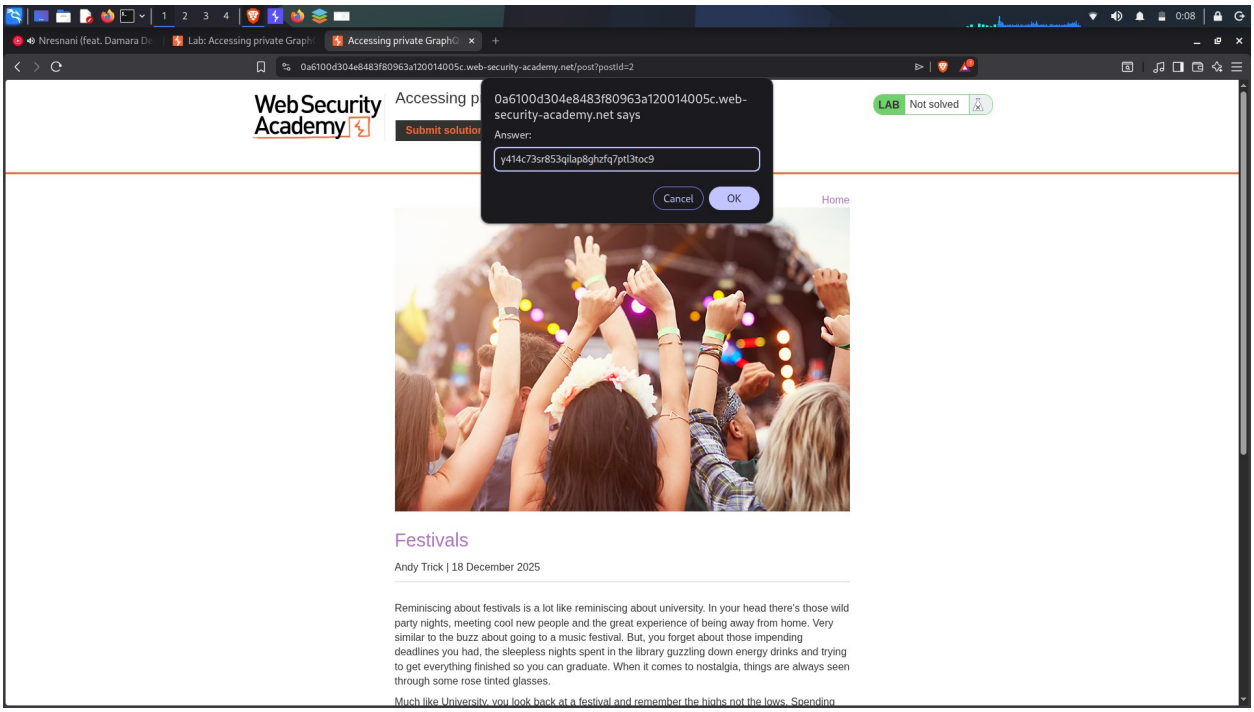


Lalu ubah nilai id tadi menjadi 3 karena id tadi di sembunyikan di post utama



Dan ternyata saat id tadi di rubah menjadi 3 ditemukan password yaitu y414c73sr853qilap8ghzfq7ptl3toc9

Lalu klik submit solution dan masukan password tadi



Dan lab pun tersolved