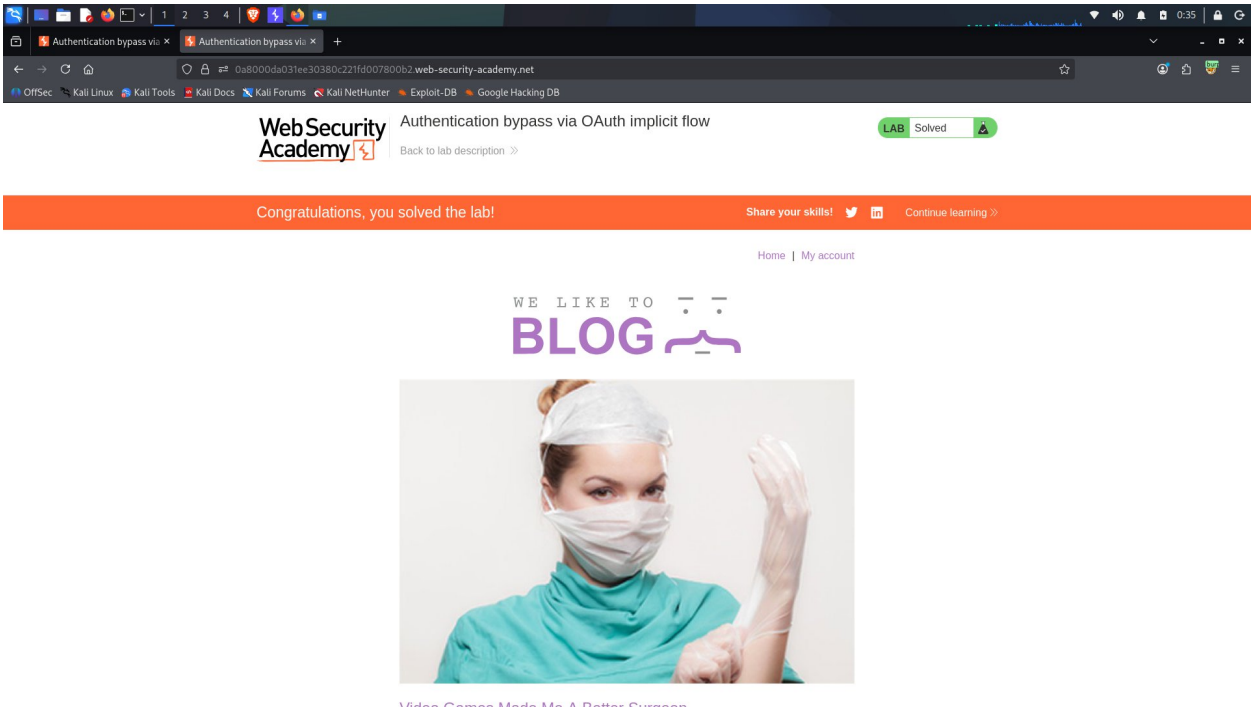
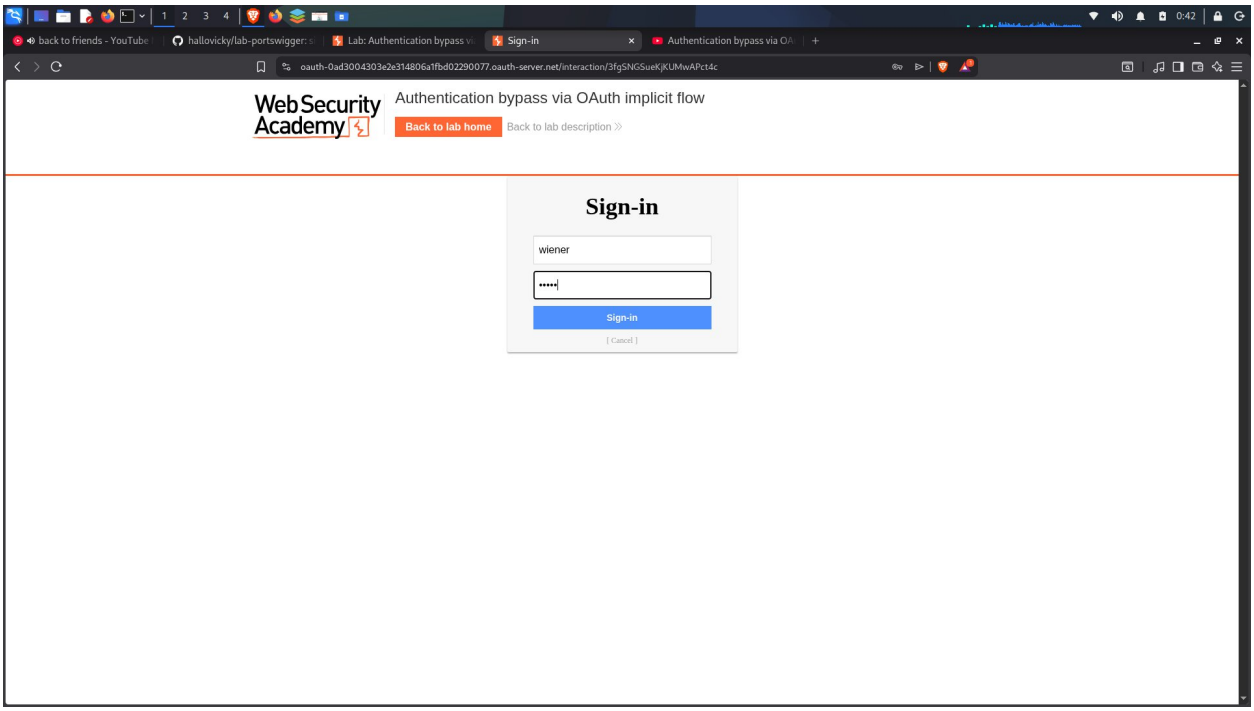
Lab: Authentication bypass via OAuth implicit flow

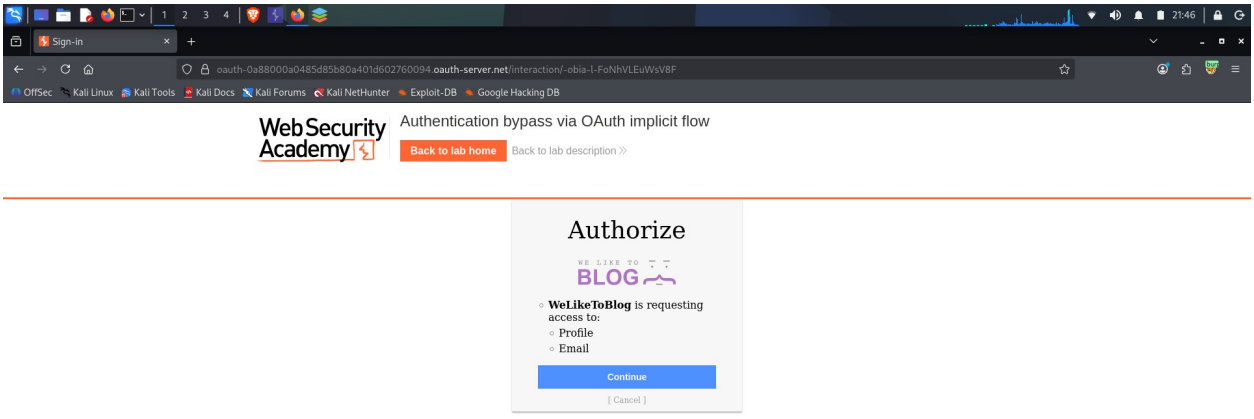
Langkah pertama buka lab kemudian klik my account



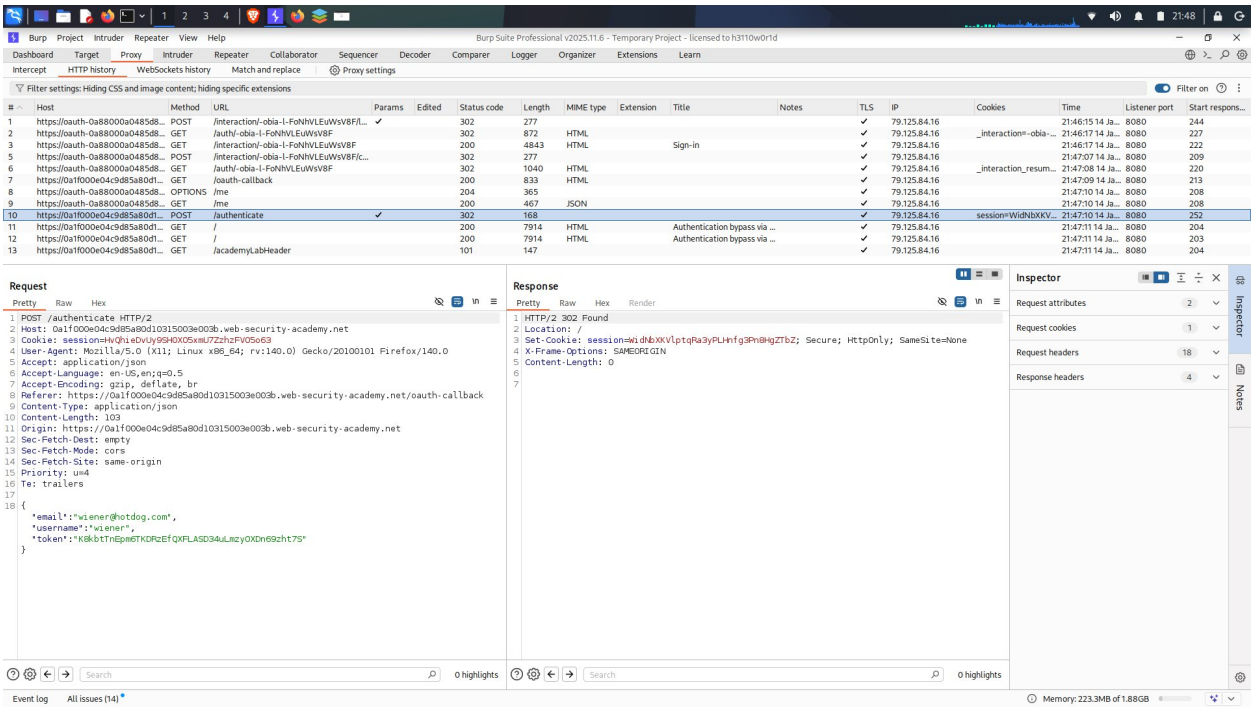
lalu sign in dengan username wiener dan password pieter dan jangan lupa nyalakan burpsuite nya



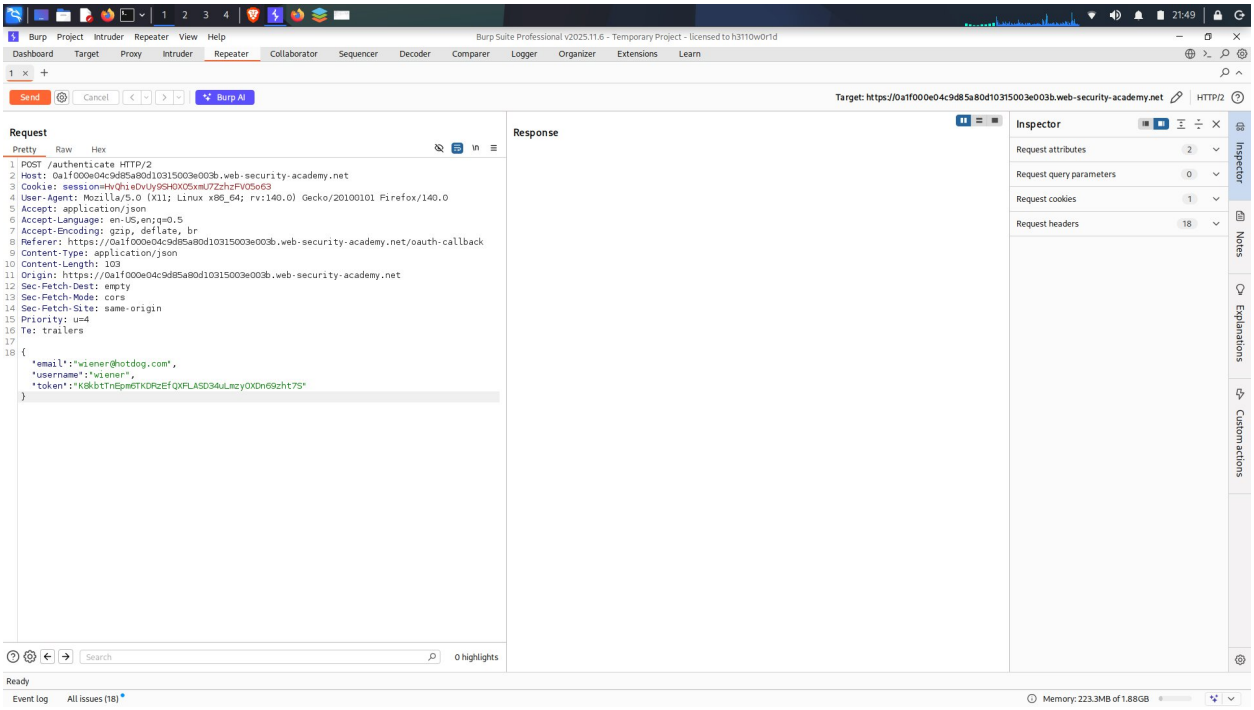
Lalu klik sign in kemudian klik continue bersamaan juga dengan burpsuite diaktifkan di foxyproxy nya akan tetatpi intercept nya jangan di nyalakan



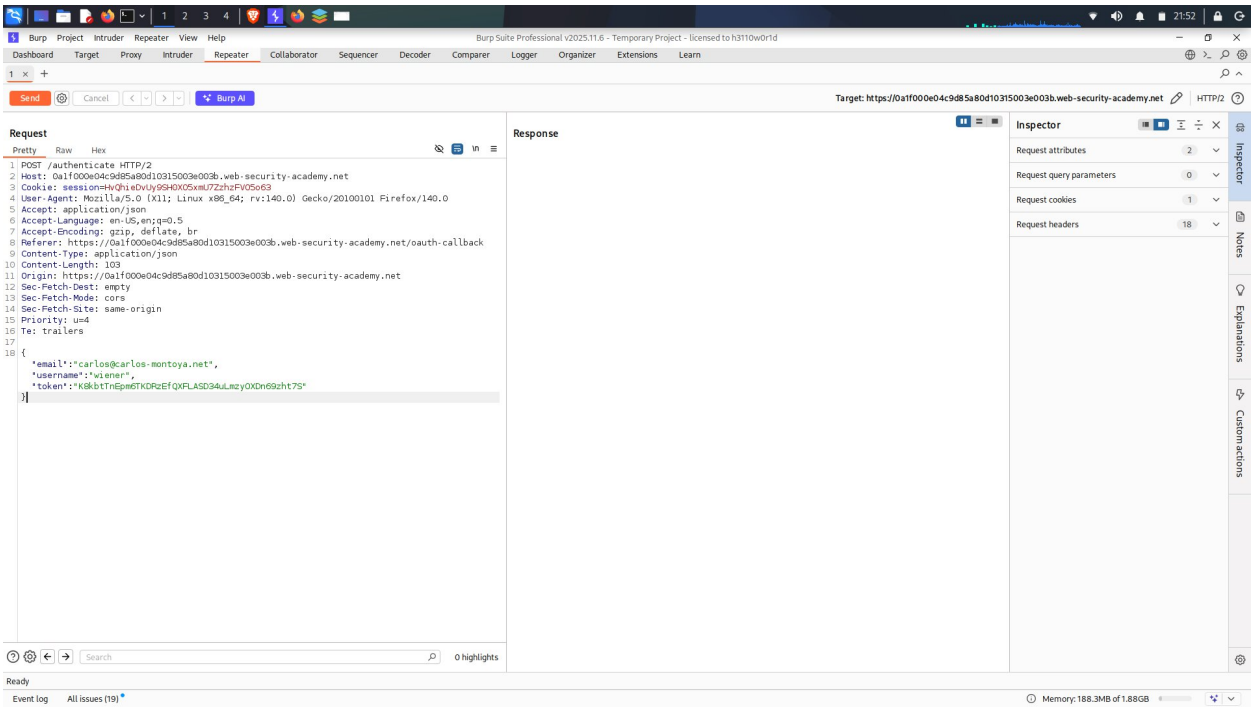
Dan ini adalah burpsuite nya



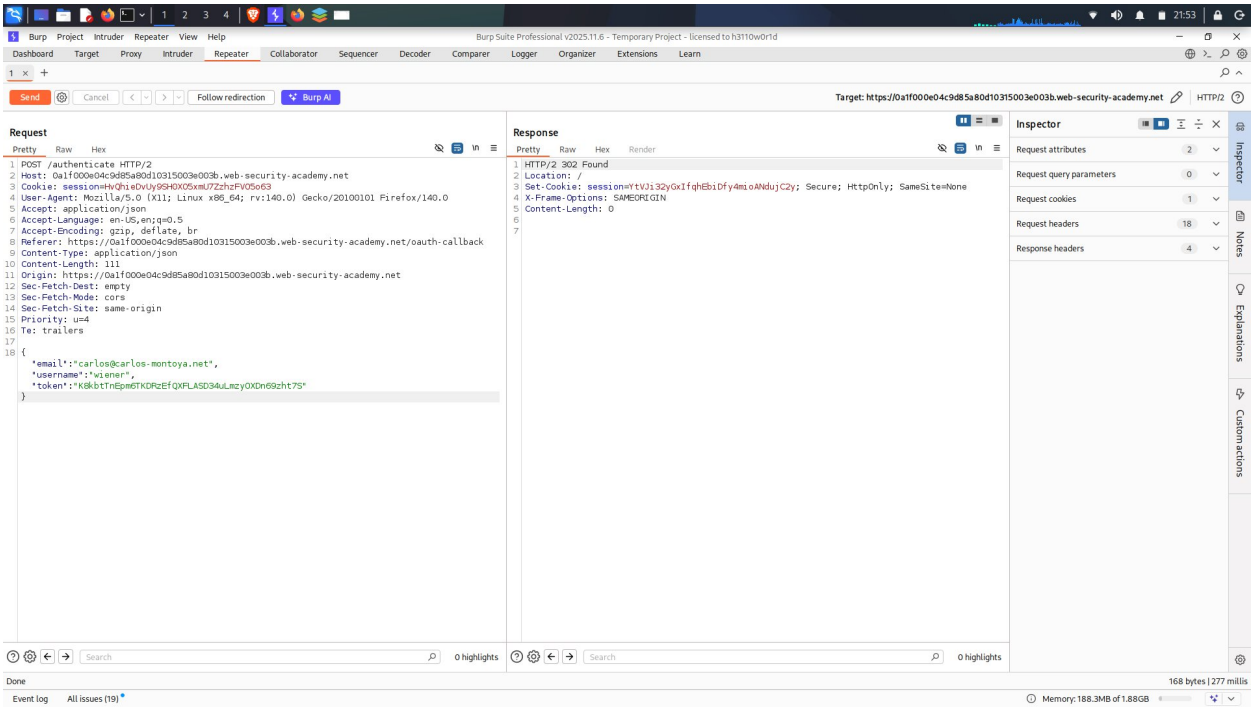
Lalu kemudian send to repeater



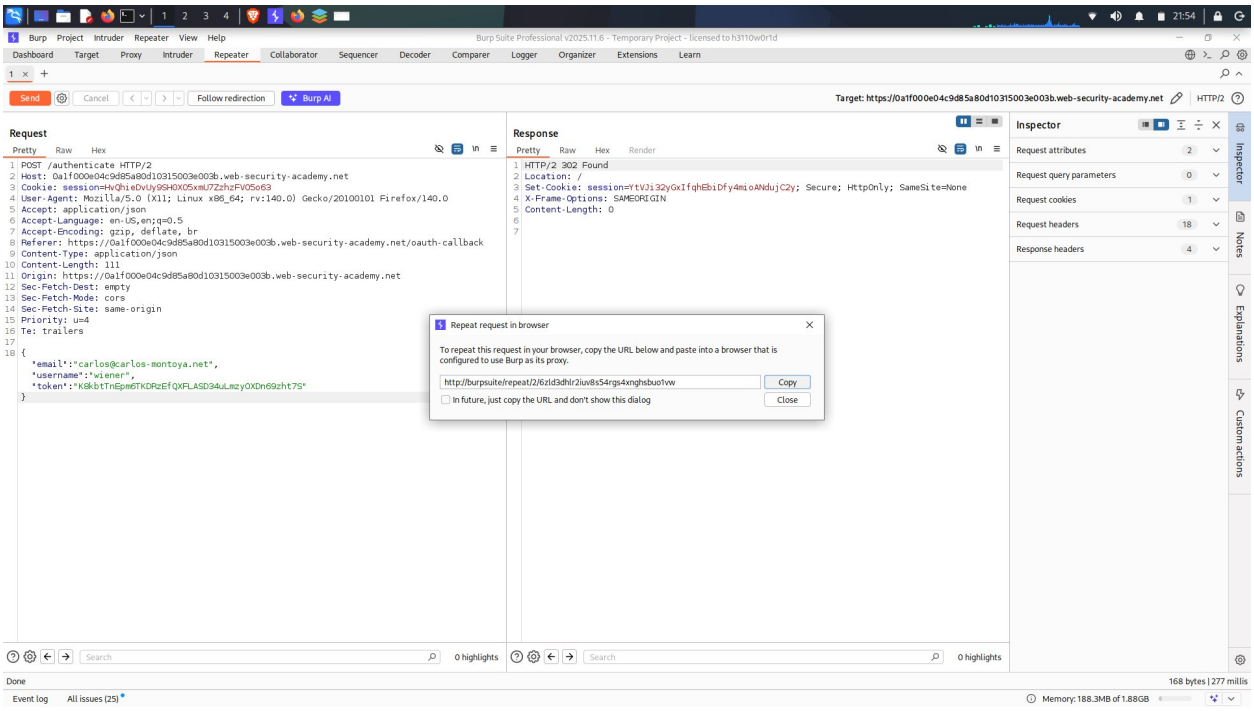
Lalu kemudian rubah email yang semula "email":"wiener@hotdog.com", menjadi carlos@carlos-montoya.net



Lalu coba send dahulu



Dan found lalu kemudian klik kanan dan klik request in browser lalu pilih in original sesion



Kemudian klik copy dan buka di browser

Dan lab pun solved