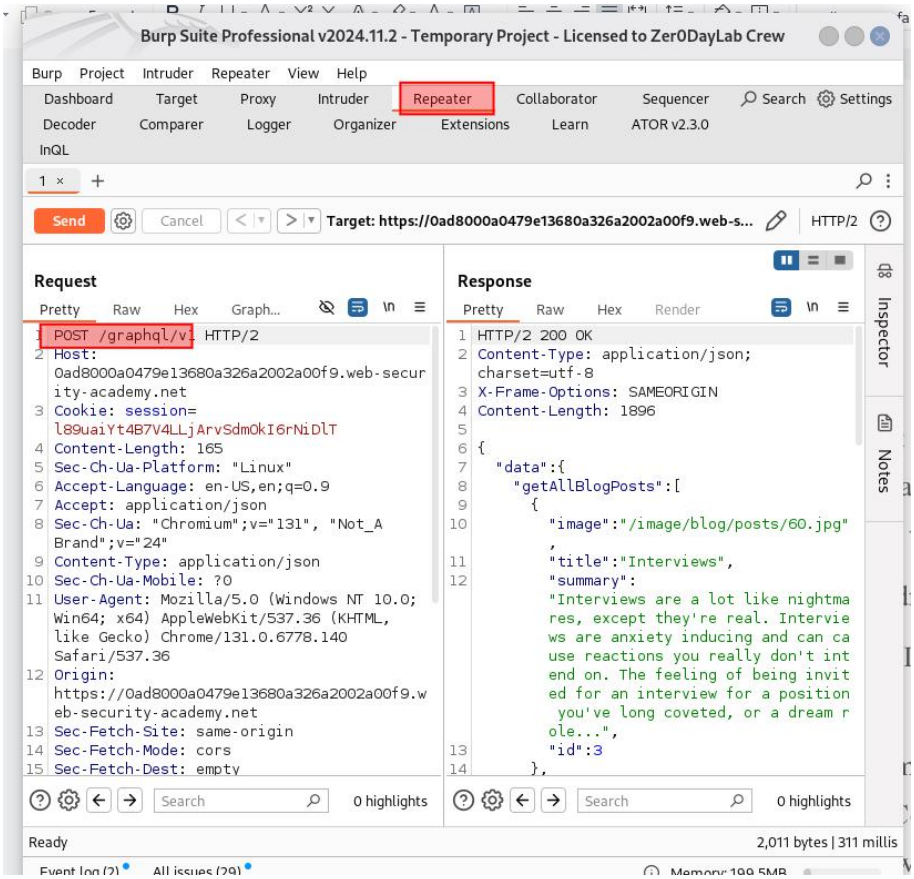
Lab-2: Accidental exposure of private GraphQL fields

Description:The user management functions for this lab are powered by a GraphQL endpoint. The lab contains an access control vulnerability whereby you can induce the API to reveal user credential fields.

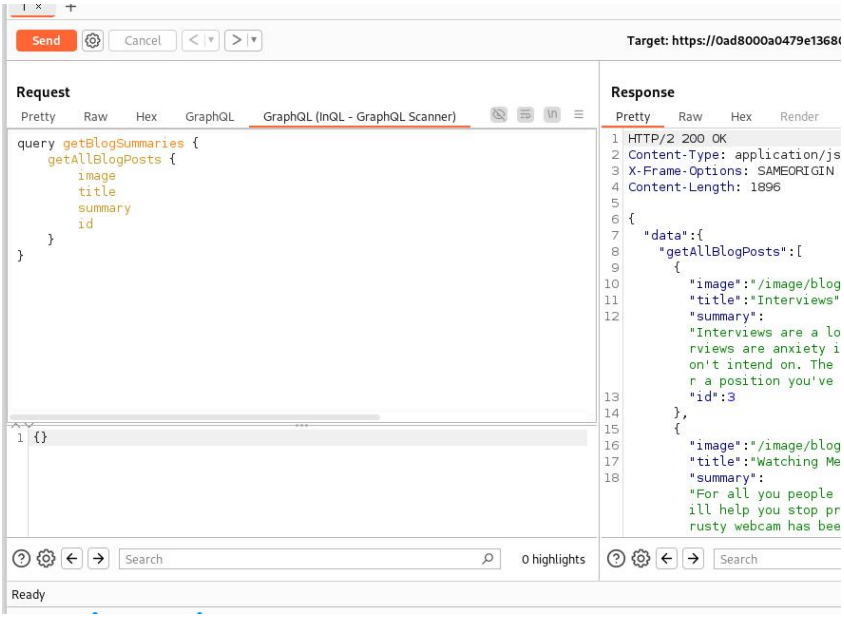
To solve the lab, sign in as the administrator and delete the username carlos

Solution:Like the previous lab1 I also use here Inql extension here to solve the lab.

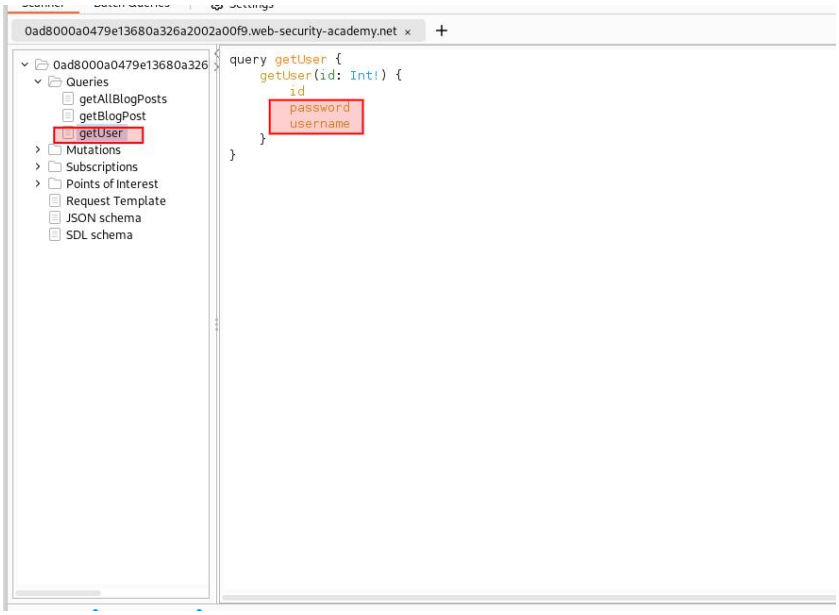
Access the lab.This is the simple website like the previous one with additional login functionality.Copy the lab link and paste it in burb chromium browser.Visit everything in the website.In burb proxy history we find POST /graphql/v1 request just send it to repeater.



Now If we visit GraphQL and GraphQL(InQL-GraphQL Scanner) tab we will see some parameters like the previous lab.



Now let's see if we can find any hidden parameter for that.Right click the copy url, paste the url into Inql extensions.



Under getUser we will notice there password and username paramter. Now copy all the query and paste it into GraphQL(InQL -GraphQL Scanner tab under repeater tab and change the int! with 1.Now in response we will

notice administrator user with password.Now login with these credentials and delete carlos to solve the lab.