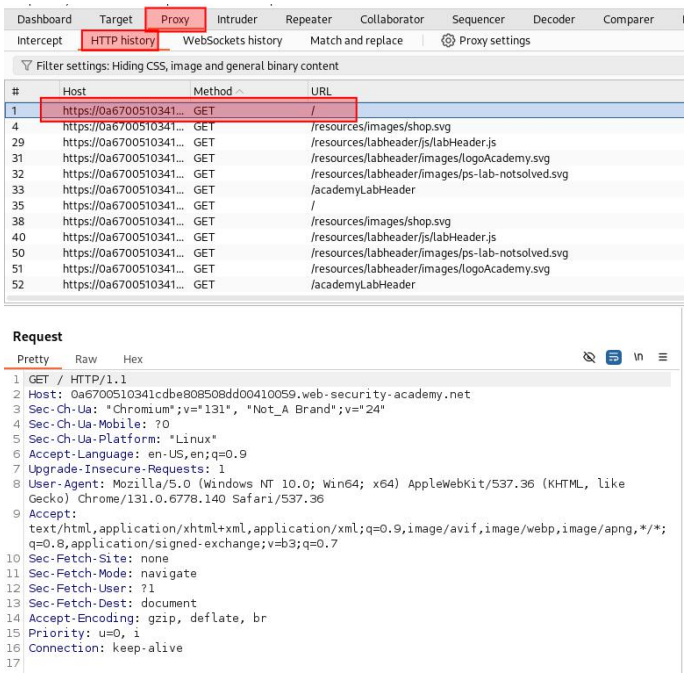
Lab: Finding a hidden GraphQL endpoint

Description:The user management functions for this lab are powered by a hidden GraphQL endpoint. You won't be able to find this endpoint by simply clicking pages in the site. The endpoint also has some defenses against introspection

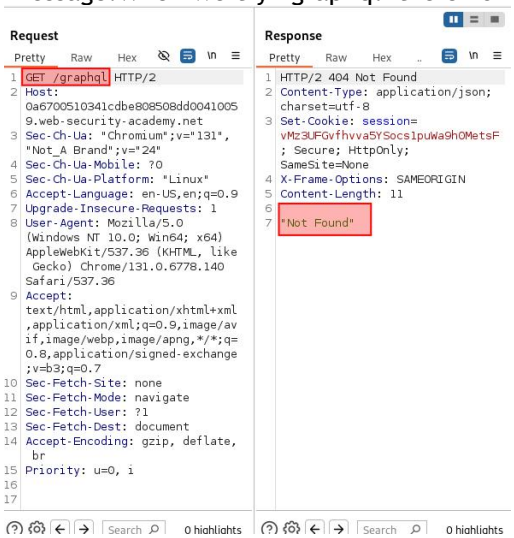
To solve the lab, find the hidden endpoint and delete carlos

Solution

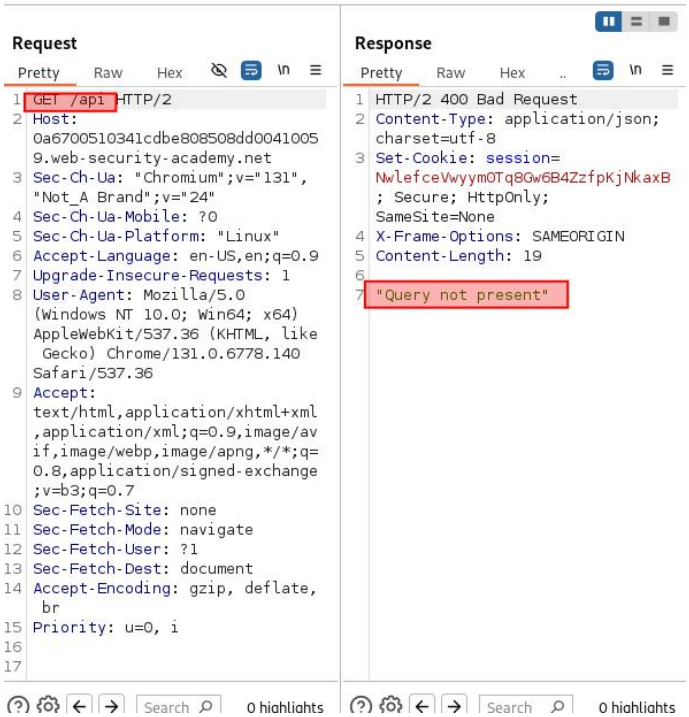
Access the lab through the burb chromium browser.Visits every functionality and focus for burb proxy history to find any endpoints.Unluckily there is no endpoint which also mentions in the description.Now let's try to find hidden endpoints.From burb proxy history send the root get request to burb repeater.



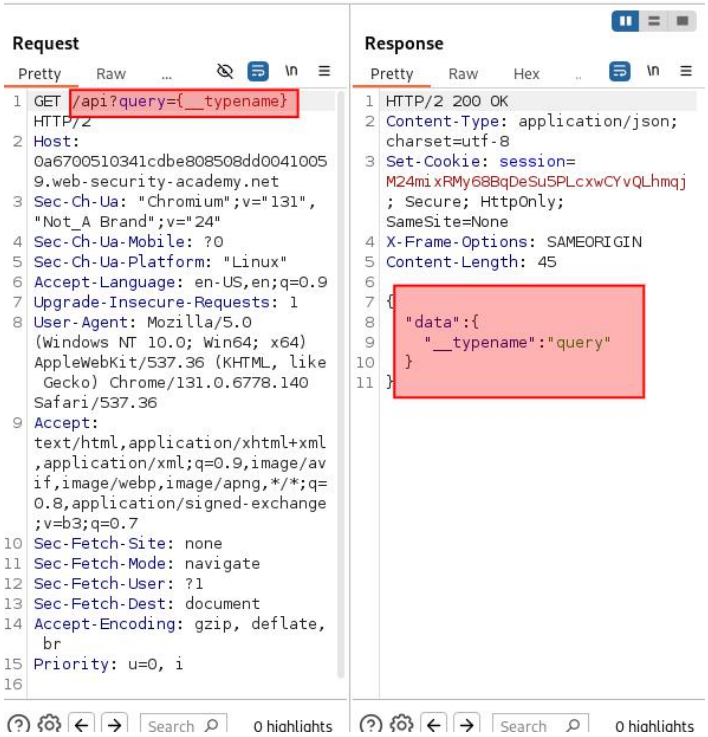
Now in burb repeater try traverse every endpoints like /graphql,/api/graphqi,/v1/graphql etc and focus or the error message.When we try /graphql the error message is "Not Found".



Now let’s try /api endpoints,where we see “Query not present” which indicate that the endpoint is different from the others.

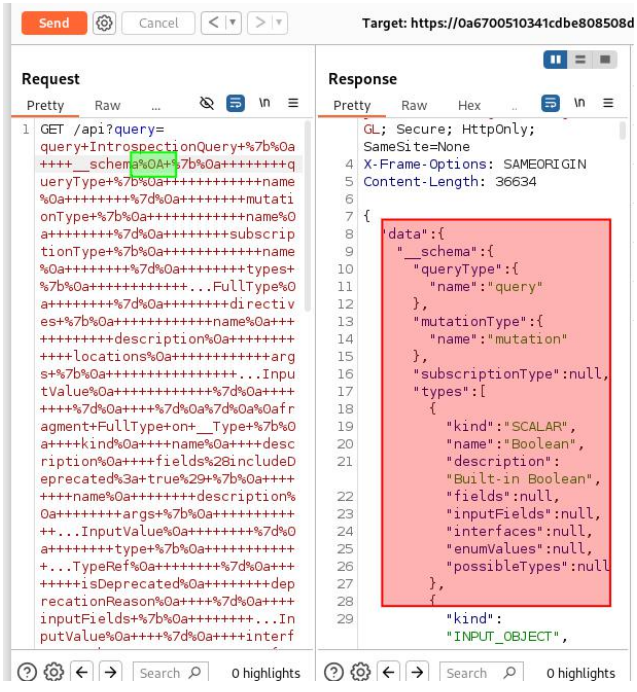


Now let’s try univeral query query={__typename} for validation the endpoint. As it is get request, we have to write the query in url,response confirms that the endpoint is valid.

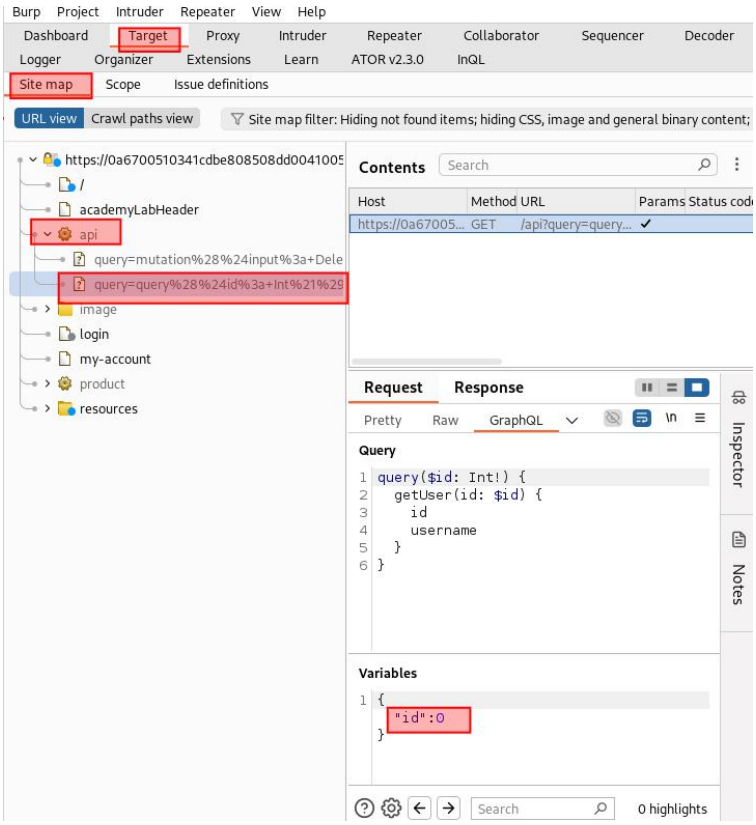


Now it’s time to introspec the query.So right click the request and GraphQL->Set introspection query.Respone indicate that schema is ok but introspection is resticted.

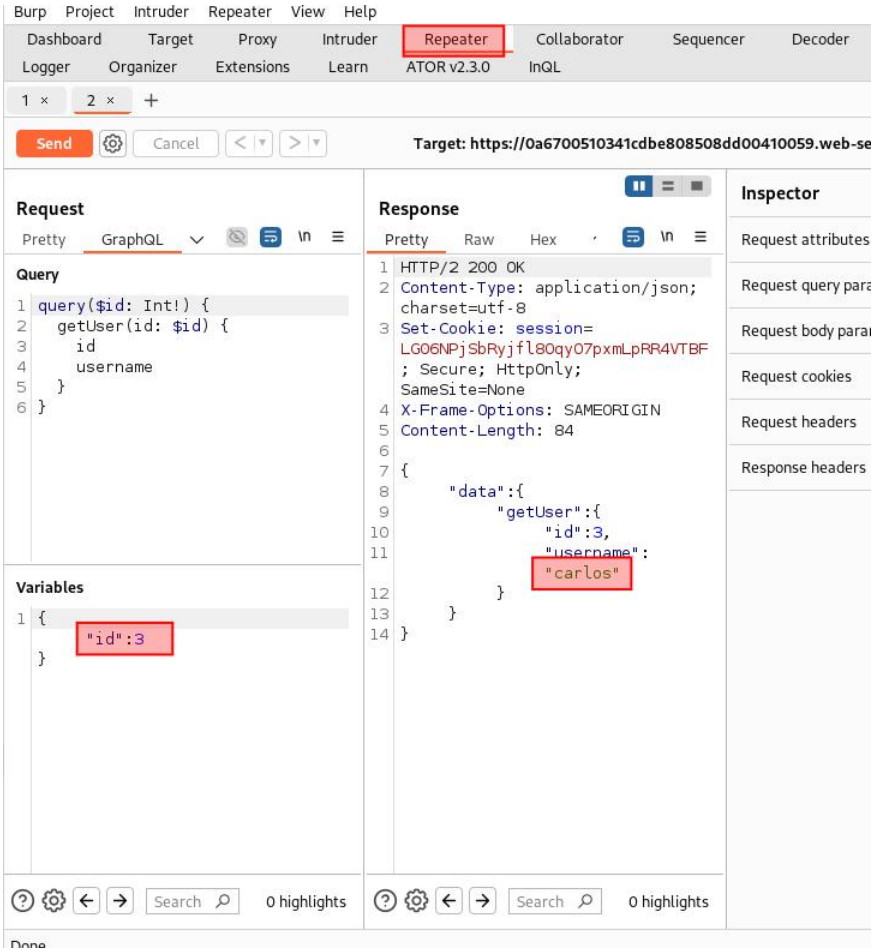
So we need to bypass the resticition.Let's try a url endcoded new line(%0A) after the __schema.Which returns positive news for us.



Now we need to find user data.So right click GraphQL->Save GraphQL queries to site map.



Here we see id parameter let's modify the id parameter value and see the respone in repeater.For id value 3 we will see the id for carlos.So we can confirm we need to delete the id 3 value.



Now again go to the site map in the api find the DeleteOrganizationalUserInput request send the request to burb repeater change the id parameter to 3 which for carlos and send the request to server to solve the lab.