Lab 4 - User role can be modified in user profile

Ahmed Khaled Saad Ali ID:1809799

Lab Progress & Screenshots:

Logging in as wiener  
Graphical user interface, application

Description automatically generated

We will turn Intercept ON, and enter an email and press “Update Email”

Graphical user interface, application

Description automatically generated

This POST request needs to be sent.

Graphical user interface, text, application, email

Description automatically generated

We will take it to the “Repeater” and turn Intercept OFF

Graphical user interface, text, application, email

Description automatically generated

When we send Request in “Repeater” we get a Response with “roleid” of the user

Graphical user interface, text, application, email

Description automatically generated

So, we can add in the Request “roleid:2” to access admin panel.

Graphical user interface, text, application, email

Description automatically generated

Sending request will result in a response with Admin roleid.

Graphical user interface, text, application, email

Description automatically generated

Back to website, by refreshing we find we have Admin panel

Graphical user interface, text, application, email

Description automatically generated

Deleting Carlos.

Graphical user interface, text, application, email

Description automatically generated

Carlos deleted; lab solved.

Graphical user interface

Description automatically generated with medium confidence

Lessons:

1) Hide identifiers like roleid even for normal users, because as soon as admin’s id is known normal users will be used as a vulnerability.

2) Check for buttons and features even if they appear not related to admin’s account