Lab 3 - User role controlled by request parameter

Ahmed Khaled Saad Ali ID:1809799

Screenshots:

Accessed My account page and login with wiener

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Re-clicking My account with intercept ON

Graphical user interface, text, application, email

Description automatically generated

We observe id value and Admin condition in Cookie, so we will try id=admin and of course change admin condition to true, and forward

Graphical user interface, text, application, email

Description automatically generated

We got another GET request with Admin condition, we will change it to true and forward.

Graphical user interface, text, application, email

Description automatically generated

Back to Site, we observe Admin Panel

Graphical user interface, application

Description automatically generated

But we found out a third GET request with Admin condition in Cookie below, we will change it to true and forward it.

Graphical user interface, text, application, email

Description automatically generated

Clicking Admin Panel sends the below GET request, editing Admin=true and forwarding.

Graphical user interface, text, application, email

Description automatically generated

Another one

Graphical user interface, text, application, email

Description automatically generated

Finally, Admin Panel opens

Graphical user interface, text, application, email

Description automatically generated

Clicking delete carlos opens below GET request, editing Admin=true and forwarding.

Text, email

Description automatically generated

Another one

Graphical user interface, text, application, email

Description automatically generated

Back to site, Carlos is deleted, lab completed

Bar chart

Description automatically generated

Learned Outcome:

1. You should keep intercept ON, to detect if the site has multiple checks on Admin access, because the site will redirect me to Normal access if you have intercept OFF
2. Avoid mentioning any admin credentials or checks in the GET/POST/PULL requests as it can be easily sniffed.