Lab 11 - Multi-step process with no access control on one step

Ahmed Khaled Saad Ali ID:1809799

Lab Progress & Screenshots:

Logged in as Administrator and accessed admin panel to observe requests sent by administrator account.

Graphical user interface, text, application, chat or text message

Description automatically generated

We would notice when we Upgrade user we get the below request with Intercept ON, so we will send it to “Repeater”

Graphical user interface, text, application, email

Description automatically generated

Then we press Yes to confirm operation, we get request below and send it to “Repeater”

Graphical user interface, text, application, email

Description automatically generated

We want to get Cookie session for wiener and replace it with admin’s cookie session, so we will login as wiener, have Intercept ON and refresh My account page.

Graphical user interface, text, application, email

Description automatically generated

We copy Cookie session of wiener, put in /admin-roles request in the repeater and change username below to wiener then send request.

Graphical user interface, text, application, email

Description automatically generated

It gave “Unauthorized” in response.

Graphical user interface, text, application, email

Description automatically generated

So, we will try the confirmation of upgrade request, do some edits and then send request.

Graphical user interface, text, application, email

Description automatically generated

We get no errors or Unauthorized access in the response, so we refresh wiener page and we find that page has an Admin Panel now, with that the lab is solved.

Bar chart

Description automatically generated with low confidence

Lessons:

1) With minimal JavaScript & HTML knowledge we deduced how to manipulate HTML request

2) Don’t have your admin account be vulnerable with /admin-roles or /administrator-roles or whatever that can be then sent as a request from admin with data in the request manipulated for attackers needs.