Lab 5 - Method-based access control can be circumvented

Ahmed Khaled Saad Ali ID:1809799

Lab Progress & Screenshots:

Logging in as Administrator, to search for vulnerabilities

Graphical user interface, application

Description automatically generated

Trying out Upgrading carlos to ADMIN in the Admin Panel with Intercept ON, we will have a POST request appear, with critical information: /admin-roles & Cookie session, username & action below. We will send it to the “Repeater”.

Graphical user interface, text, application, email

Description automatically generated

We will logout from Admin and log in as wiener.

Graphical user interface, text, application

Description automatically generated

With Intercept ON, we refresh wiener page to have request from wiener to get his Cookie session & send request to “Repeater”

Text

Description automatically generated with low confidence

We will copy wiener’s Cookie Session & paste instead of Cookie session in Admin Request in the “Repeater”, also we will change request method to GET.

Graphical user interface, text, application, email

Description automatically generated

Username field appears, lets try entering wiener in place of carlos, Send request and then refresh wieners page.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, website

Description automatically generated

Failed tries:

System had protection for Cookie session copying from user wiener to admin’s request in “Repeater”. It gives “Unautherized” in Response.

Graphical user interface, text, application, email

Description automatically generated

We tried changing carlos to wiener in username field, but it gave “Unautherized” in Response as well.

Graphical user interface, text, application, email

Description automatically generated

So, we deduced that POST request is heavily protected, so we try with another request method and it worked.

Lessons:

Make sure to cover up protection and clear vulnerabilities of all HTTP request methods.