Lab 9 - User ID controlled by request parameter with password disclosure.

Ahmed Khaled Saad Ali ID:1809799

Lab Progress & Screenshots:

Logged in as wiener.

Graphical user interface, text, application

Description automatically generated

We find this request, with an identifier to the user of the logged in account.

Graphical user interface, text, application, email

Description automatically generated

We will take the request to the “Repeater” and change its “id” field to “administrator” and send request. We should get in the password in the response because it is displayed on the account page and as we know in HTML for input type password, its value is just right there in “value” field. We copy the password’s value.

Graphical user interface, text, application, email

Description automatically generated

We login with administrator’s password.

Graphical user interface, text, application

Description automatically generated

Administrator’s account page accessed.

Graphical user interface, text, application

Description automatically generated

Admin panel accessed.

Graphical user interface, text, application, email

Description automatically generated

Carlos is deleted, Lab solved.

Chart, bar chart

Description automatically generated

Lessons:

1) Don’t simply include identifiers of a user in when he sends a request.

2) With minimal HTML knowledge, password’s value was deduced from response.