Lab 8 - User ID controlled by request parameter with data leakage in redirect.

Ahmed Khaled Saad Ali ID:1809799

Lab Progress & Screenshots:

Logged in as wiener.

Graphical user interface, text, application, email

Description automatically generated

We see this GET request with “id” field, we send to the “Repeater”

Graphical user interface, text, application, email

Description automatically generated

When we send request with “id=wiener”, we get his API key in the response.

Graphical user interface, text, application, email

Description automatically generated

So, we will change “id” field to carlos, and we copy his API Key from response.

Graphical user interface, text, application, email

Description automatically generated

Submit API Key.

Graphical user interface, application

Description automatically generated

Lab Solved.

Chart

Description automatically generated with medium confidence

Lessons:

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