Lab 7 - User ID controlled by request parameter, with unpredictable user IDs

Ahmed Khaled Saad Ali ID:1809799

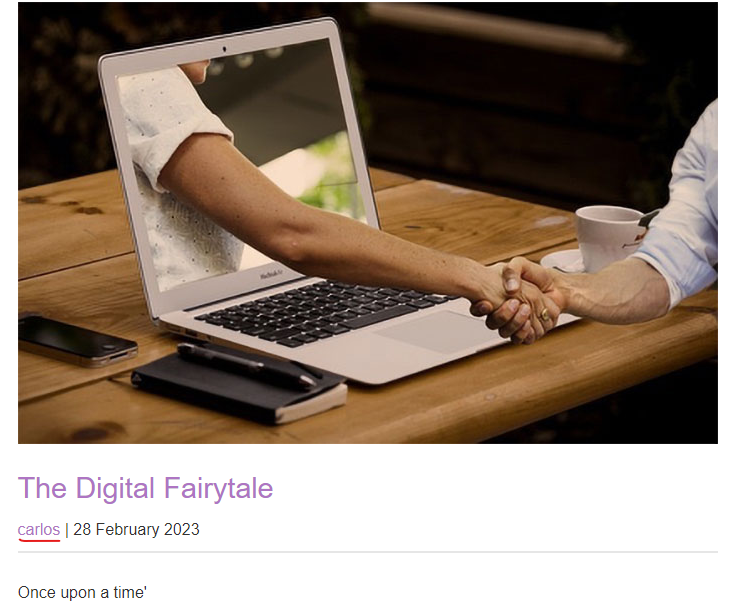
Lab Progress & Screenshots:

Logged in as wiener.

Graphical user interface, text, application, email

Description automatically generated

We found out carlos has written a blog, so we turn Intercept ON and see what we get in request.



We find carlos’s userId.

Graphical user interface, text, application, email

Description automatically generated

so we copy it and go to wiener’s account page to replace it with wiener’s userId.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Carlos’s account page accessed, API Key copied, lab solved.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application, website

Description automatically generated

Lessons:

1) Make sure that when a user clicks to view another user they don’t send identifiers to that user in requests.

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