Lab 10 - Insecure direct object references

Ahmed Khaled Saad Ali ID:1809799

Lab Progress & Screenshots:

Opening Live Chat Page.

Graphical user interface, text, application, email

Description automatically generated

We try View transcript button to see if we can obtain old chat logs with Intercept ON. We forward request.

Graphical user interface, text, application, email

Description automatically generated

We find specified txt file to be downloaded of current chat log, we change it to 1.txt to download oldest chat log and forward request.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

It pops up again so we do the same.

Graphical user interface, text, application, email

Description automatically generated

We observe in this downloaded chat log the password.

Text

Description automatically generated

We login as Carlos using the password copied from chat log.

Graphical user interface, application

Description automatically generated

Carlos account page accessed, lab solved.

Bar chart

Description automatically generated with medium confidence

Lessons:

1) Be aware of Social Engineering attackers, don’t trust giving anyone your password.

2) Don’t save chat logs or any file on system incrementally, because changing one number gives access to all chat logs or files by attackers/sniffers.