T7 - MSc Pool

T-POO-700

Risk factor

Project

1.1

{EPITECH.}

Risk factor

delivery method: Github
language: anything that gets the job done

- The totality of your source files, except all useless files (binary, temp files, obj files,...), must be included in your delivery.

Check your application robustness!
Find and patch as many security gaps as possible.

You must check several attack vectors and ask yourself the following questions:

- are they injectable (XSS, Script, HTML, …)?
- are they vulnerable to sql injections, nosql?
- are there accessible configuration files?
- are password hashes difficult to break?
- are routes accessible by unauthorized users?
- are endpoints accessible by unauthorized users?
- is it possible to fill the database and cause a denial of service when rendering the page?
- are JWT tokens http-only? If not, how to recover these tokens?
- are the passwords sent in clear? If so how do you recover them?
- is the application available only in https? if not, how could a malicious user intercept a client's requests to your server?

This list is not exhaustive and you should be able to find other vectors of attacks.

Remember to exchange with your classmates, you probably have different ways to approach the same project and can give each other new ideas and different suggestions!

And how about the mobile app?