B2 - Binary Security

B-SEC-200

N.O.O.B

Noob-Oriented Operations on Binaries

2.0

To start the CTF, your **team leader** (from the intranet) must create an account on the NOOB interface, with his/her **Epitech email address** and the **name of the group** as defined on the intra.
Then, the rest of the project takes place on this interface.

Use **ONE** and **ONLY ONE** account to validate the challenges.
This account must be created **with the group leader's Epitech email address** and the name of the team must **match the one defined on the Intranet**.

Challenges are divided into three categories:

- easy
- intermediate
- hard.

The aim of each challenge is to find a flag hidden in a binary.
Exploit the program, find the flag, enter it on the plateform and… voilà!

Your main friends for debugging are GDB, ltrace, hexdump, objdump…
Some challenges also require you to script.

Each of these flags gives you points.
Your number of points will decrease over time, depending on the other teams' results: the more a challenge is validated, the less points it is worth.

Do not share the flags to other teams, unless you want your score to plummet (or unless you want to be flagged as a cheater…).

Have fun, hack fast!

All the attempts to exploit breaches must be carried out **manually**, or using scripts that you have developed by yourself.
Automated exploitation attempts and actions that can be classified as foul play, especially voluntary and/or repeated denial of service attacks, could, as backlash, cause your team to be **disqualified**.