



B2 - Binary Security

B-SEC-200

N.O.O.B

Noob-Oriented Operations on Binaries



3.0



To start the CTF, your **team leader** (from the intranet) must log-in on the **NOOB interface** using the Office365 authentication and create a team on it.

Then the team leader can invite his/her teammates into the team on the platform.

The rest of the project takes place on this interface.



It is still mandatory to register your group on the intranet.
The team leader on both platform must be the same.

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 platform and... voilà!



Your main friends for debugging are GDB, ltrace, hexdump, objdump...
Some challenges also require you to create some kind of scripts.

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**.

It is strictly forbidden to:

- attack or simply try to connect to a port on the machine that is not the main platform or a challenge
- perform any kind of penetration testing on the main platform
- use the server as an attack vector to infect other users or launch further attacks!
- simply enough, perform any other action that is not intended.

It is worth mentioning that the server is constantly monitoring for such behaviours.



EPITECH SECURITY DISCORD

Thus it is totally optionnal, if you're interested by the field of security (and if not, what are you doing here?), we encourage you to join our Discord server to be able to chat with other people from Epitech (and some outsiders) about it, share news, etc.

The discord also have a dedicated channel about this project were you'll be able to find help from other students and pedagogical members.



Beware, the following invitation link will automatically give you a role indicating that you're a Tech1 student. Don't share it! Other students will have other ways to join.

To join the server click on the following link: [Epitech Security](#).