

# B2 - Web Security

B-SEC-400

## SHODAN

Security & Hacking Oriented Data Access Network





Welcome to South Park, where the Chinpokomon spree has no limits!

You'll need to buy them all to become Chinpoko-master!

But, unfortunately, you're as poor as Kenny, and you can't afford them (except for Shoe, maybe...) Hence, you'll have to use devious means to get them.

Well, actually, you're not exactly going to get Chinpokomon, but flags (sha512 hashes to be precise). In order to find them, you'll have to detect and take advantage of any Web page breach.



The more a task is validated, the less points it is granted.

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

To start the quest, your team leader must create an account on the [SHODAN interface](#), with his/her Epitech email address and create a team. Then you can create an account too and join the team.

The rest of the project will take 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.**



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.