

Pré CQI 2023 - Reverse Engineering - 10 pts

Context

Security is an essential aspect to all public facing programs. A company that takes security seriously will test their systems against attacks. This challenge will evaluate your capacities to test the security of such a system. You will have to exploit an executable in order to extract a flag with the given format: `flag-012345678901`. You will be provided a portion of the code that makes up the executable.

Required Software

- The given executable is for linux, therefore, you will need a computer with linux or a virtual machine with linux.
- We strongly suggest to use a reverse engineering tool such as the following:
 - Radare2
 - Binary Ninja
 - IDA
 - Ghidra

Delivery

You will have to deliver the flag and a bash script demonstrating your exploit.

Instructions

You will have to exploit the `binary-with-flag` executable by giving it a specially crafted username and password.