

Pwn Challenge (16 points)

The frobnicate server allows clients to run a set of operations on its stored files. Most of them are standard, but the eponymous frobnicate operation has been developed in-house.

The source code is available here: <https://lettieri.iet.unipi.it/hacking/2022-02-03.tar.gz>

You can request two hints on the solution:

- Hint #1: Analysis of the main bug in server.c. Cost: -3 points.
- Hint #2: Analysis of the bug in frobnicate.c. Cost: -2 points.

Web Challenge (14 points)

TinyCVE is a website hosting a database of the favorite CVE entries of the webmaster. The website seems to magically understand what is the client's platform, and it shows vulnerabilities correlated to such a platform in addition to those searched with a search string. The candidate must steal a flag that is hidden somewhere in the application.

You can request two hints on the solution:

- Hint #1. Nature of the vulnerability and which input to leverage. Cost: -3 points.
- Hint #2. PHP code of the website. Cost: -2 points.