

# Security in Software Applications - Project 1

A.A. 2024/2025

Download and install flawfinder (<http://www.dwheeler.com/flawfinder>)

Use this tool to statically analyze the code fragment in the file `project1_SSA24.c`.

Your report (ONE file in pdf format called LastName\_Matricola.pdf) should contain:

- up to 3 lines stating the major strengths and weaknesses of the tool;
- a screenshot of the output of the tool for the fragment;
- an analysis of each warning (max 3 lines each);
- vulnerabilities, if any, not flagged by the tool;
- a corrected version of the fragment where all the vulnerabilities found have been removed, with a screenshot showing that the tool “has no complains”.

This project counts for 10% of the final grade, i.e. 3pts.

0.5 extra points are assigned if the project is submitted within 2 weeks (29th of October).

**Maximum length** of the report: 2 pages.

Other clarifications:

- Flawfinder is a lexical analyzer. It works with non-compilable code. If you find typos, you may report and fix them as well.
- A proper analysis of a warning requires a human inspection to see whether the alert is a True Positive or a False Positive. A simple description of the vulnerability does not suffice.