# Improving software security with Infer Quandary via confusion matrix perturbation analysis

ICT Risk Assessment final project

Giovanni Bartolomeo and Laura Bussi

# 1 Introduction

When dealing with security issues, we are provided a pletora of tools for the analysis of possible vulnerabilities in software. Many of them analyse the behaviour of the software at run time, but static analysis can also be performed: several tools can analyse source code and find possible flaws before the program is running.
Of course, both this kind of approaches cannot be 100% accurate. Most likely they will provide as result a set of possible vulnerabilities which intersect the set of the actual ones, i.e. for each pointed out vulnerability we will have four possible cases:

- **True Positive** Tool correctly identifies a real vulnerability
- **False Negative** Tool fails to identify a real vulnerability
- **True Negative** Tool correctly ignores a false alarm
- **False Positive** Tool fails to ignore a false alarm

From this classification, we obtain a $2 \times 2$ matrix, namely a confusion matrix. Confusion matrix can be a useful tool to benchmark a security analysis tool capabilities.

## 1.1 OWASP Benchmark

# 2 Project structure

Prova

# 3 Benchmark results

Prova

# 4 Conclusions

Prova