

Static Code Analysis



Dario Campagna

Head of Research

Static Code Analysis

Static code (or program) analysis is the analysis of computer software that is performed without actually executing programs.

- Identification of coding errors
- Individuation of duplicated code
- Computation of software metrics
- Formal methods (e.g., Hoare logic, Model Checking)



Automated Tools

Automated tools that perform static code analysis can identify issues that reduce code readability, maintainability, quality.

- IDE code analysis functionalities (e.g., IntelliJ inspections)
- SonarQube



Using automated tools for static-code analysis

- Check/select/configure the inspection rules in default profiles/configuration
  - Too restrictive/permissive rules
  - Rules that you prefer to ignore
  - Rules you want to check and are not included

- Review the rule documentation to confirm it checks for the expected conditions

- Use inspection results as a way to uncover information about your code

- Do not fix violations just because they are reported by the tool, take informed decisions

- Maintain the inspection rules

