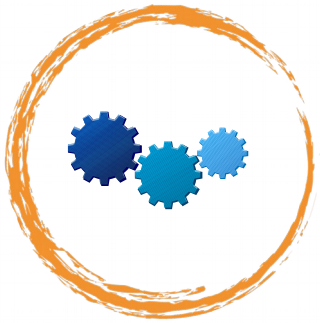
Detection of Security Bugs Using Static Code Analysis

David Formánek, supervised by RNDr. Andriy Stetsko, Ph. D.
Faculty of Informatics, Masaryk University, Brno

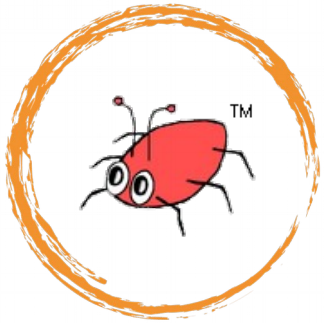
Many hidden security bugs in the code – automatic analysis needed



Implemented static taint analysis traces data flow of malicious inputs

Focus on most dangerous weaknesses and the most popular language (Java)

Added to an existing tool, presented at Black Hat, 1st place in SVOČ



Existing tools missed most of the problems or reported too many false positives

Detection accuracy improved from 53% to 95% (Juliet TS)