doi: 10.1631/FITEE.1500379

题目：基于改进规则检查静态分析技术的高效脆弱性检测方法

概要：静态分析是保障软件开发质量的一种重要方法。通过与软件开发过程集成并进行交互式应用可进一步提升静态分析工具的作用优势。然而，静态分析工具的交互式应用具有高性能和快速响应等要求。为此，本文以基于规则检查技术的静态分析工具作为研究对象，提出一种改进的规则检查算法，旨在提升静态分析工具的性能。该方法首先采用一种领域描述语言构造脆弱性规则的特征对象表达式，然后基于特征对象表达式的运算结果，对脆弱性规则进行过滤。由于一个代码文件通常只包含与部分脆弱性规则相关的错误，通过规则过滤可有效提高规则检查算法的效率，进而提升静态分析的性能。为了对方法可行性及有效性进行评估，方法实现过程被集成到开源静态分析工具 PMD 中并基于扩展后的 PMD 进行了实验分析。实验结果表明提出的方法可在不损失静态分析检测能力和精度的情况下获得平均 28.7%的性能提升。

关键词：基于规则的静态分析技术；软件质量；软件验证；性能改进