The Flavour of Real-World Vulnerability Detection and Intelligent Configuration

Cristina Cifuentes

Oracle Labs

Abstract. The Parfait static code analysis tool focuses on detecting vulnerabilities that matter in C, C++, Java and Python languages. Its focus has been on key items expected out of a commercial tool that lives in a commercial organisation, namely, precision of results (i.e., high true positive rate), scalability (i.e., being able to run quickly over millions of lines of code), incremental analysis (i.e., being able to run over deltas of the code quickly), and usability (i.e., ease of integration into standard build processes, reporting of traces to the vulnerable location, etc). Today, Parfait is used by thousands of developers at Oracle worldwide on a day-to-day basis.

In this presentation, we'll sample a flavour of Parfait — we explore some real world challenges faced in the creation of a robust vulnerability detection tool, look into two examples of vulnerabilities that severely affected the Java platform in 2012/2013 and most machines since 2017, and conclude by recounting what matters to developers for integration into today's continuous integration and continuous delivery (CI/CD) pipelines. Key to deployment of static code analysis tools is configuration of the tool itself - we present our experiences with use of machine learning to automatically configure the tool, providing users with a better out-of-the-box experience.