Static Analysis for Security

Brian Chess
Fortify

All software projects are guaranteed to have one artifact in common—source code. Together with architectural risk analysis,[1] code review for security ranks very high on the list of software security best practices (see Figure 1).[2] Here, we'll look at how to automate source-code security analysis with static analysis tools.

The promise of static analysis is to the same security-related mistakes. tool without being aware of the finer points of security bugs.

Testing for security vulnerabilities is complicated by the fact that they often exist in hard-to-reach states or crop up in unusual circumstances. Static analysis tools can peer into more of a program's dark corners with less fuss than dynamic analysis, which requires actually running the code. Static analysis also has the potential to be applied before a