Using Static Analysis

Dr. Jared DeMott
SECURITY RESEARCHER AND ENGINEER

@jareddemott www.vdalabs.com

Overview

Introduce Automated Analysis

Pros vs. Cons

Review Cycle

Basic Usage of Tools

Check Code Automatically

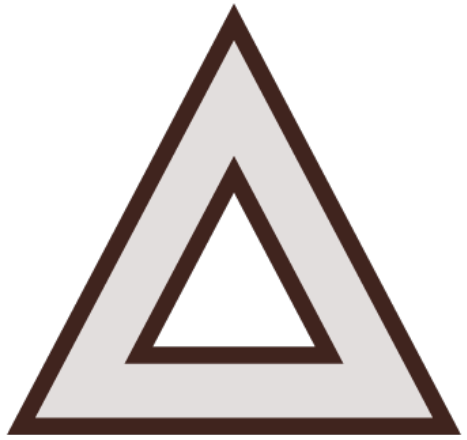
- Development tools
- Security tools

Pros of Static Analysis Tools

- Runs across all code
- Extensible to find new bugs

Cons of Static Analysis Tools

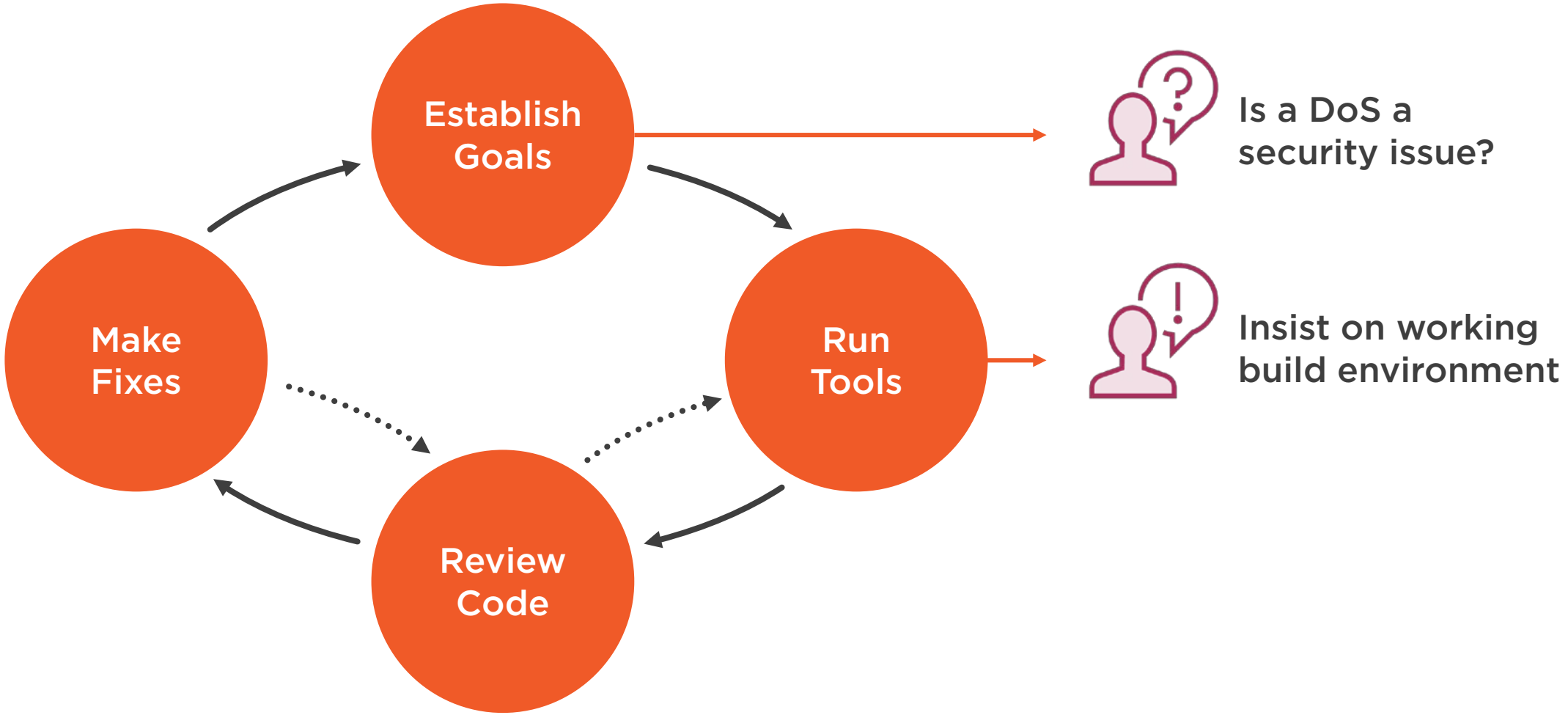
- FPs
- FNs



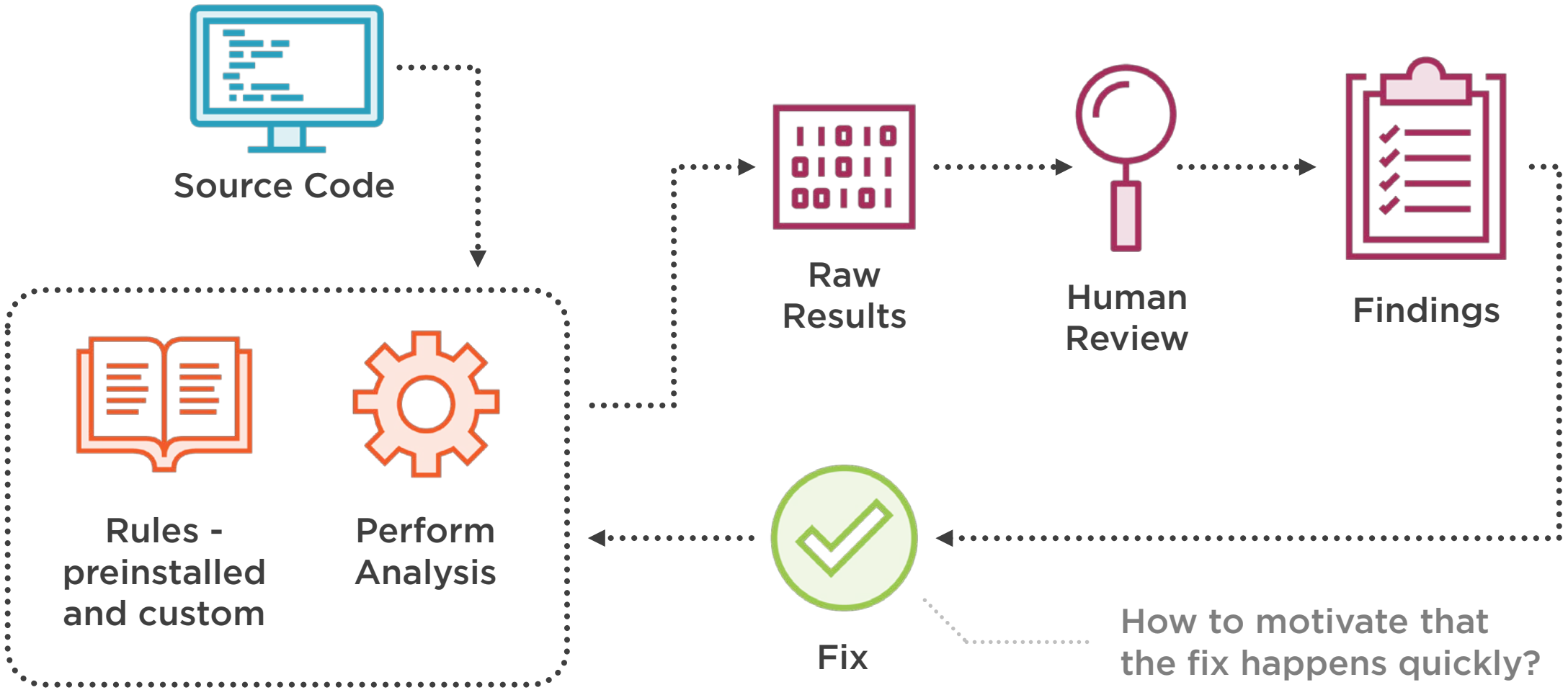
When Using Automated Tools

- Roll them out slowly and carefully
- Central SAS dynamic testing

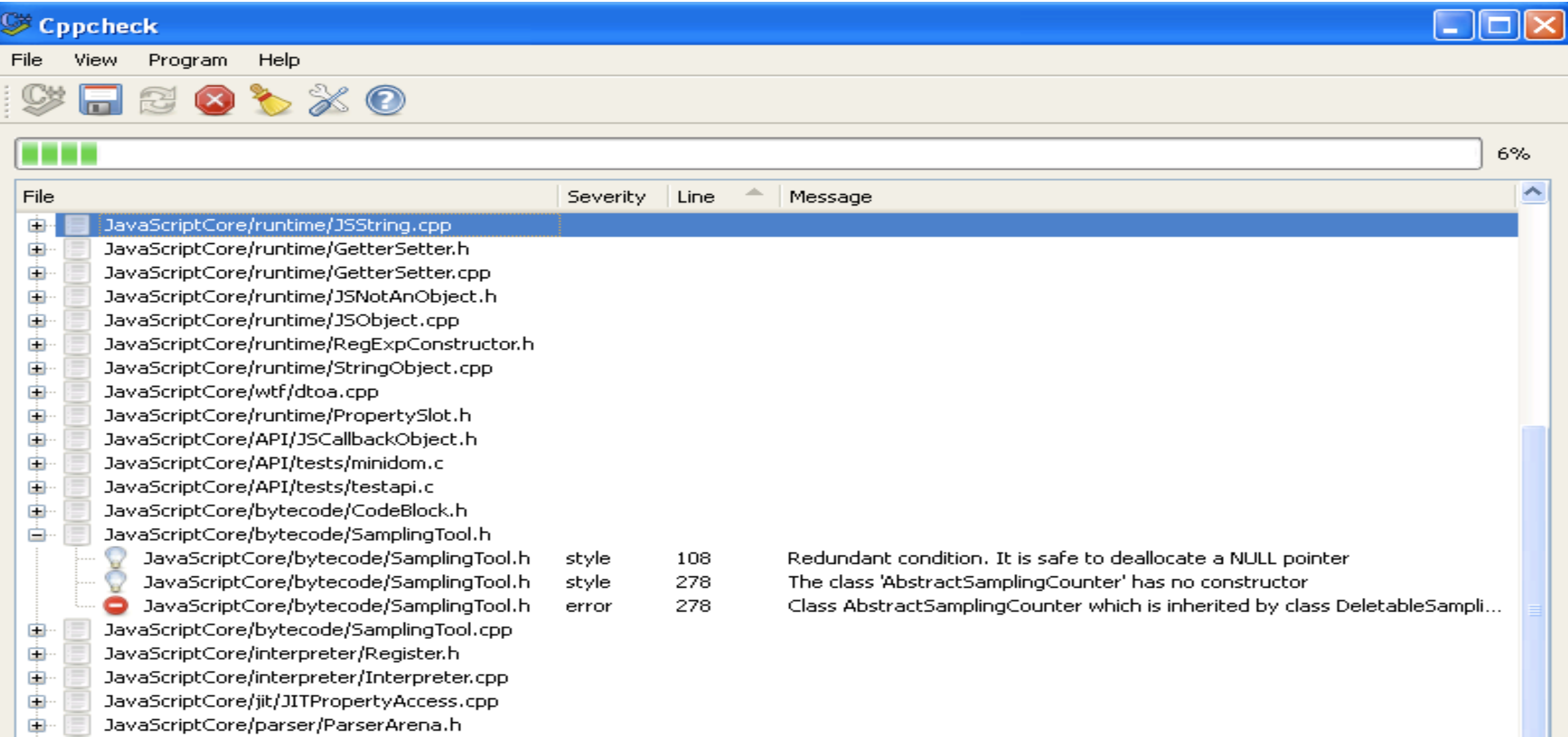
Static Review Cycle



Functional View of Static Analysis



CppCheck

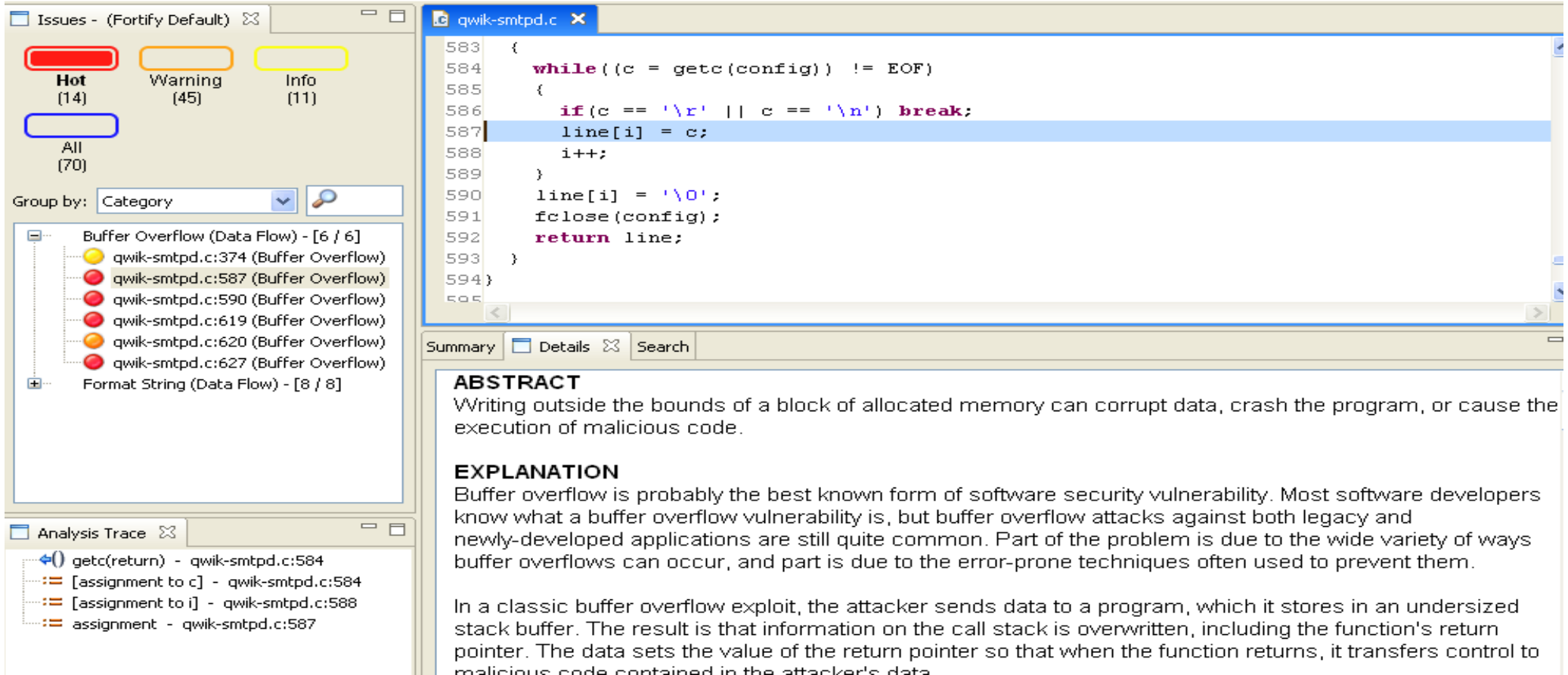

Cppcheck
File
View
Program
Help
6%
File
Severity
Line
Message
JavaScriptCore/runtime/JSString.cpp
JavaScriptCore/runtime/GetterSetter.h
JavaScriptCore/runtime/GetterSetter.cpp
JavaScriptCore/runtime/JSNotAnObject.h
JavaScriptCore/runtime/JSObject.cpp
JavaScriptCore/runtime/RegExpConstructor.h
JavaScriptCore/runtime/StringObject.cpp
JavaScriptCore/wtf/dtoa.cpp
JavaScriptCore/runtime/PropertySlot.h
JavaScriptCore/API/JSCallbackObject.h
JavaScriptCore/API/tests/minidom.c
JavaScriptCore/API/tests/testapi.c
JavaScriptCore/bytecode/CodeBlock.h
JavaScriptCore/bytecode/SamplingTool.h
JavaScriptCore/bytecode/SamplingTool.h style 108 Redundant condition. It is safe to deallocate a NULL pointer
JavaScriptCore/bytecode/SamplingTool.h style 278 The class 'AbstractSamplingCounter' has no constructor
JavaScriptCore/bytecode/SamplingTool.h error 278 Class AbstractSamplingCounter which is inherited by class DeletableSampli...
JavaScriptCore/bytecode/SamplingTool.cpp
JavaScriptCore/interpreter/Register.h
JavaScriptCore/interpreter/Interpreter.cpp
JavaScriptCore/jit/JITPropertyAccess.cpp
JavaScriptCore/parser/ParserArena.h

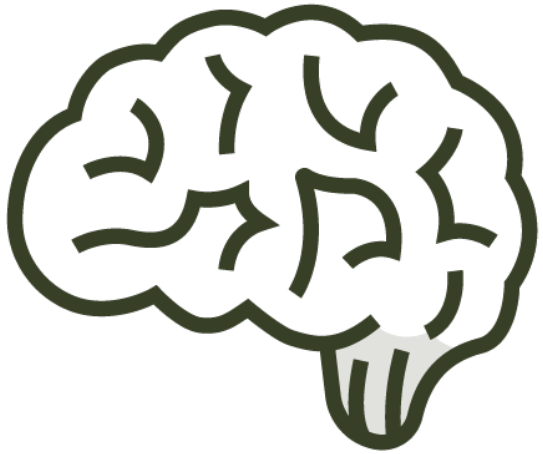
Importance of Good SA Reports

Grouping and Sorting Results

Elimination Unwanted Results

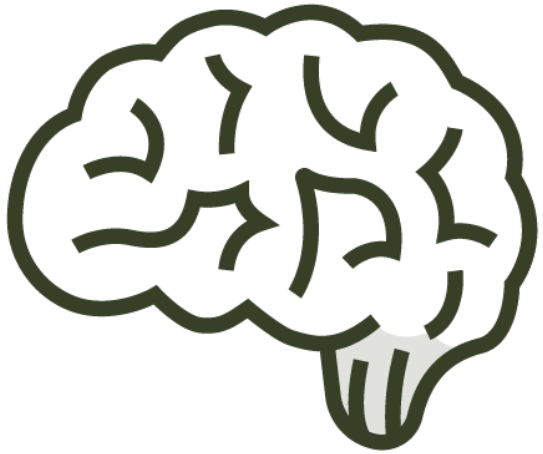
Explaining the Significance of the Results





Prioritizing Reports is Important

- Particularly if just starting with static for the first time



SA Tools

- Do not have a strong reputation for being useful to highly complex projects

Summary

Why Useful?

When to Include?

What's Next?