Module Five Static Code Analysis

Jordan Whitney

CS-405 Secure Coding

Professor: Alan Spencer

8/01/2025

The Cppcheck static code analysis is more of a variety of issues in the source code that wasn’t detected by Visual Studio and its built-in code analysis. It flagged several warnings and errors, including non-boolean values returned from functions expected to return bool. The findings reflect potential risks such as undefined behavior, memory corruption, and logic errors that can undermine both the correctness and security of the program.

Visual Studio’s static analysis focuses on compile-time errors, some logic warnings, and conformance to language rules. There are usually no warnings about redundant conditions, assignment of local variables to function parameters without dereferencing, or issues like variable shadowing. Meaning that the developers relying on Visual Studio could miss these vulnerabilities.

Buffer overflows and uninitialized member variables are severe, as they can lead to unpredictable behavior like data leakage or exploitation. Allowing the risk associated with these issues ranging from a medium level to a high level.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.