Mark Eilers

CS 405: Secure Coding

5-3 Activity: Static Code Analysis

April 7, 2024

5-3 Activity: Static Code Analysis

The process for analyzing the provided C++ code involves comparing warnings and errors between Visual Studio and CppCheck. Firstly, a Visual Studio Console project is set up with the given file as the sole source. The code is compiled, and the resulting warnings and errors are examined within the Visual Studio Error list. Simultaneously, a CppCheck project is configured to analyze the Visual Studio project. Settings are adjusted in CppCheck to ensure comprehensive analysis, including enabling inline suppressions, checking for inconclusive errors, and setting the C++ Standard to C++17.

After configuring CppCheck, the analysis is executed, and the results are saved in XML format. During the analysis, all messages generated by CppCheck that are not present in the Visual Studio Error list are identified. Each unique message is evaluated to determine whether it poses a risk to the code (classified as RISK or NOT RISK). Furthermore, it is noted which system, either Visual Studio or CppCheck, detected the issue. For each discrepancy between the tools, a brief description of the identified issue is provided.

Upon completion of the analysis, a comprehensive summary is compiled. This summary includes an overview of the warnings and errors identified by Visual Studio, a comparison of these findings with those from CppCheck, and an assessment of the effectiveness of each tool in detecting potential issues. The summary ends by emphasizing the importance of utilizing multiple analysis tools to ensure code quality and mitigate risks effectively.

A screenshot of a computer

Description automatically generatedA computer screen shot of a black screen

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA computer screen shot of a black screen

Description automatically generated