

CS-405 Secure Coding – Static Analysis

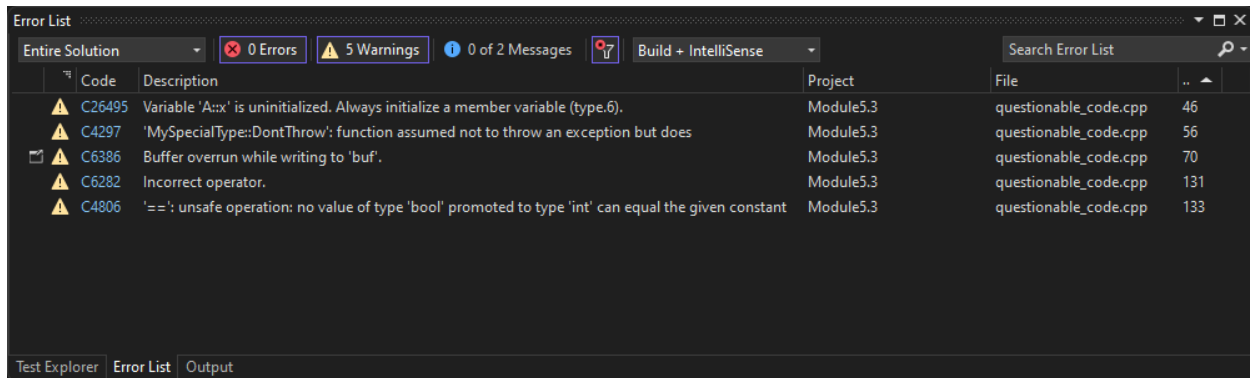
Eric Slutz

Southern New Hampshire University

STATIC CODE ANALYSIS	3
VISUAL STUDIO STATIC CODE ANALYSIS RESULTS	3
CPPCHECK STATIC CODE ANALYSIS RESULTS	4
SUMMARY OF STATIC CODE ANALYSIS RESULTS	4

Static code analysis

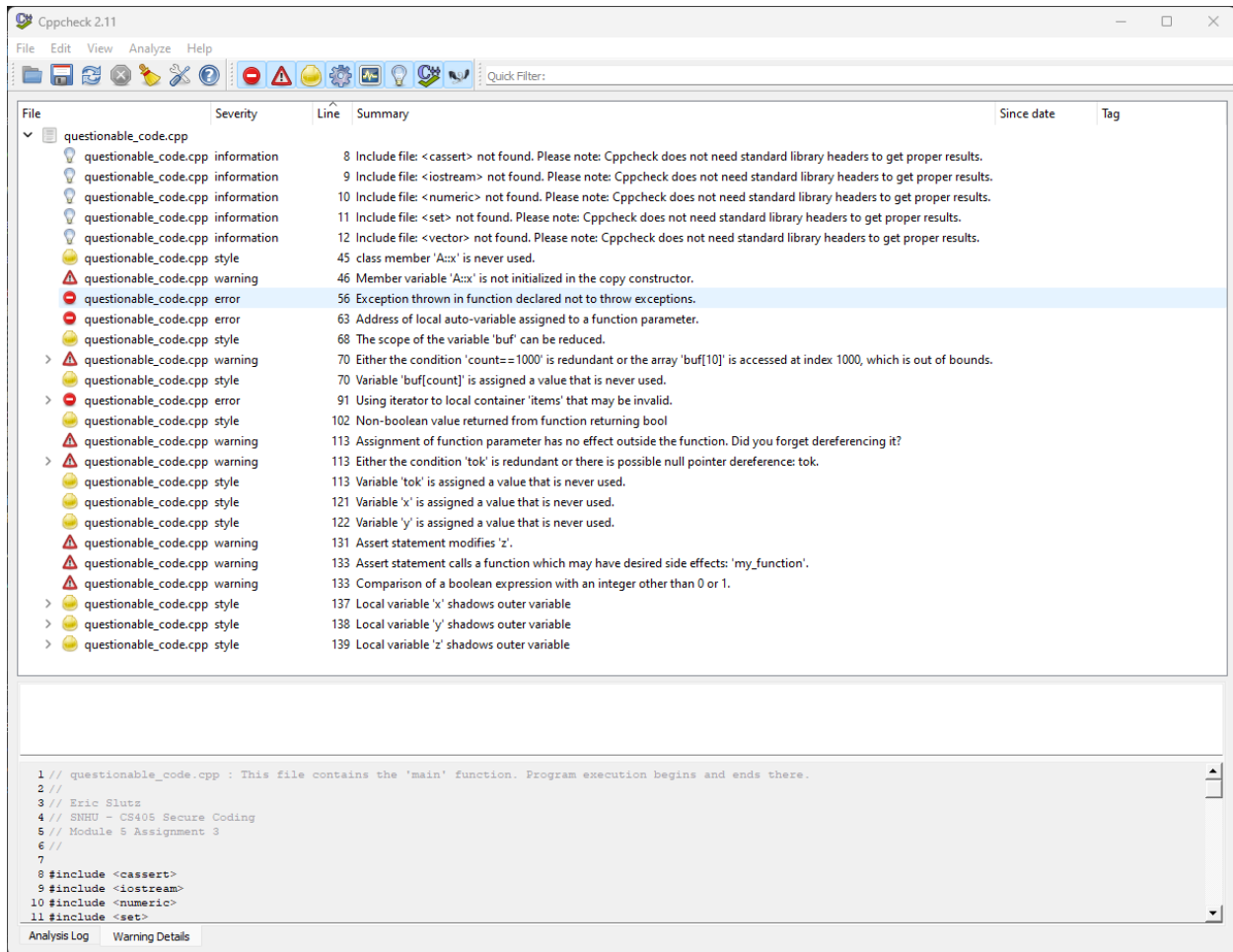
Visual Studio static code analysis results



The screenshot shows the Visual Studio Error List window. At the top, it indicates '0 Errors' and '5 Warnings'. The list contains five items, all warnings, related to the file 'questionable_code.cpp' in 'Module5.3'. The items are as follows:

Code	Description	Project	File	Line
C26495	Variable 'A::x' is uninitialized. Always initialize a member variable (type.6).	Module5.3	questionable_code.cpp	46
C4297	'MySpecialType::DontThrow': function assumed not to throw an exception but does	Module5.3	questionable_code.cpp	56
C6386	Buffer overrun while writing to 'buf'.	Module5.3	questionable_code.cpp	70
C6282	Incorrect operator.	Module5.3	questionable_code.cpp	131
C4806	'==': unsafe operation: no value of type 'bool' promoted to type 'int' can equal the given constant	Module5.3	questionable_code.cpp	133

Cppcheck static code analysis results



Summary of static code analysis results

In the table below, you can see all the issues that the static code analysis found in both Visual Studio and Cppcheck. Visual Studio found five issues and did not find any issues that Cppcheck did not find. Cppcheck found 20 issues, 15 of which that Visual Studio did not find. In addition, for the issues where both analysis tools flagged a problem the issue descriptions were much more verbose and informative from Cppcheck as compared to Visual Studio. Visual Studio labeled all of these issues as warnings. Cppcheck again gave more information, assigning each issues a severity level of information, style, warning, or error.

Issue	Class member 'A::x' is never used.				Line	45
Mitigation	Remove unused members.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	Member variable 'A::x' is not initialized in the copy constructor.				Line	46
Mitigation	Initialize the variable.					
Result Found	Visual Studio	Yes	Cppcheck	Yes		

Issue	Exception thrown in function declared not to throw exceptions.				Line	56
Mitigation	Don't throw an exception or remove 'noexcept'.					
Result Found	Visual Studio	Yes	Cppcheck	Yes		

Issue	Address of local auto-variable assigned to a function parameter.				Line	63
Mitigation	Do not assign local-variable to a function parameter.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	The scope of the variable 'buf' can be reduced.				Line	68
Mitigation	Reduce the scope.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	Either the condition ‘count==1000’ is redundant or the array ‘buf[10]’ is accessed at index 1000, which is out of bounds.				Line	70
Mitigation	Fix the conditional ‘count==1000’.					
Result Found	Visual Studio	Yes	Cppcheck	Yes		

Issue	Variable ‘buf[count]’ is assigned a value that is never used.				Line	70
Mitigation	Either use the value or remove it.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	Using iterator to local container ‘items’ that may be invalid.				Line	91
Mitigation	Iterate from zero to container length.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	Non-boolean value returned from function returning bool.				Line	102
Mitigation	Return a boolean value or change return type.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	Assignment of function parameter has no effect outside the function. Did you forget dereferencing it?				Line	113
Mitigation	Remove dereferencing of the assignment function.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	Either the condition 'tok' is redundant or there is possible null pointer dereference: tok.				Line	113
Mitigation	Check for dereference or remove redundant condition.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	Variable 'tok' is assigned a value that is never used.				Line	113
Mitigation	Remove unused variable.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	Variable 'x' is assigned a value that is never used.				Line	121
Mitigation	Remove unused variable.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	Variable 'y' is assigned a value that is never used.				Line	122
Mitigation	Remove unused variable.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	Assert statement modifies 'z'.				Line	131
Mitigation	Assert should not modify any values.					

Result Found	Visual Studio	Yes	Cppcheck	Yes	
---------------------	----------------------	-----	-----------------	-----	--

Issue	Assert statement calls a function which may have desired side effects: 'my_function'.				Line	133
Mitigation	Update assert statement function call.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	Comparison of a boolean expression with an integer other than 0 or 1.				Line	133
Mitigation	Only compare boolean with other booleans or integer 0 or 1.					
Result Found	Visual Studio	Yes	Cppcheck	Yes		

Issue	Local variable 'x' shadows outer variable.				Line	137
Mitigation	Change the variable name.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	Local variable 'y' shadows outer variable.				Line	138
Mitigation	Change the variable name.					
Result Found	Visual Studio	No	Cppcheck	Yes		

Issue	Local variable 'z' shadows outer variable.				Line	139
Mitigation	Change the variable name.					
Result Found	Visual Studio	No	Cppcheck	Yes		