

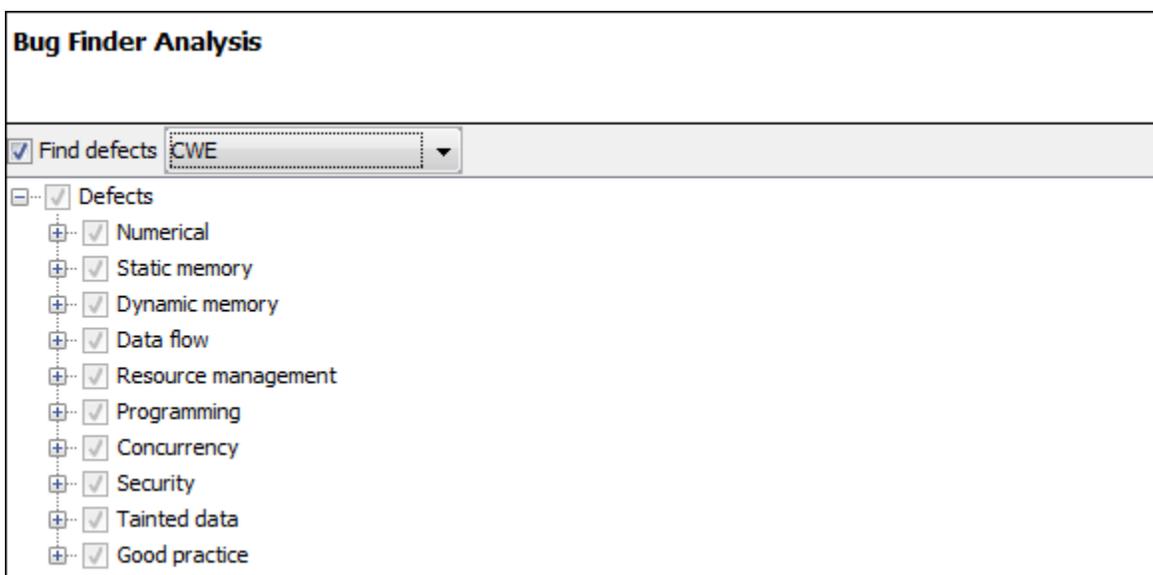
Check C/C++ Code for Security Standards

Using results of a Polyspace® analysis, you can check your code for the following security standards:

- CWE™: See also [CWE Coding Standard and Polyspace Results](#).
- CERT C99: See also [CERT C Coding Standard and Polyspace Results](#).
- ISO/IEC TS 17961: See also [ISO/IEC TS 17961 Coding Standard and Polyspace Results](#).

To adhere to a security standard, follow this workflow.

Step 1: Check Code Against Standard



Check your code for the subset of defects and coding rules that correspond to the standard.

- CWE: Use the CWE subset for the option **Find defects (-checkers)**.
- CERT C99: Use both the option to check defects and the option to check coding rules.
 - **Find defects (-checkers)**: Use **CERT-rules** or **CERT-all**.
 - **Check MISRA C:2012 (-misra3)**: Use **CERT-rules** or **CERT-all**.

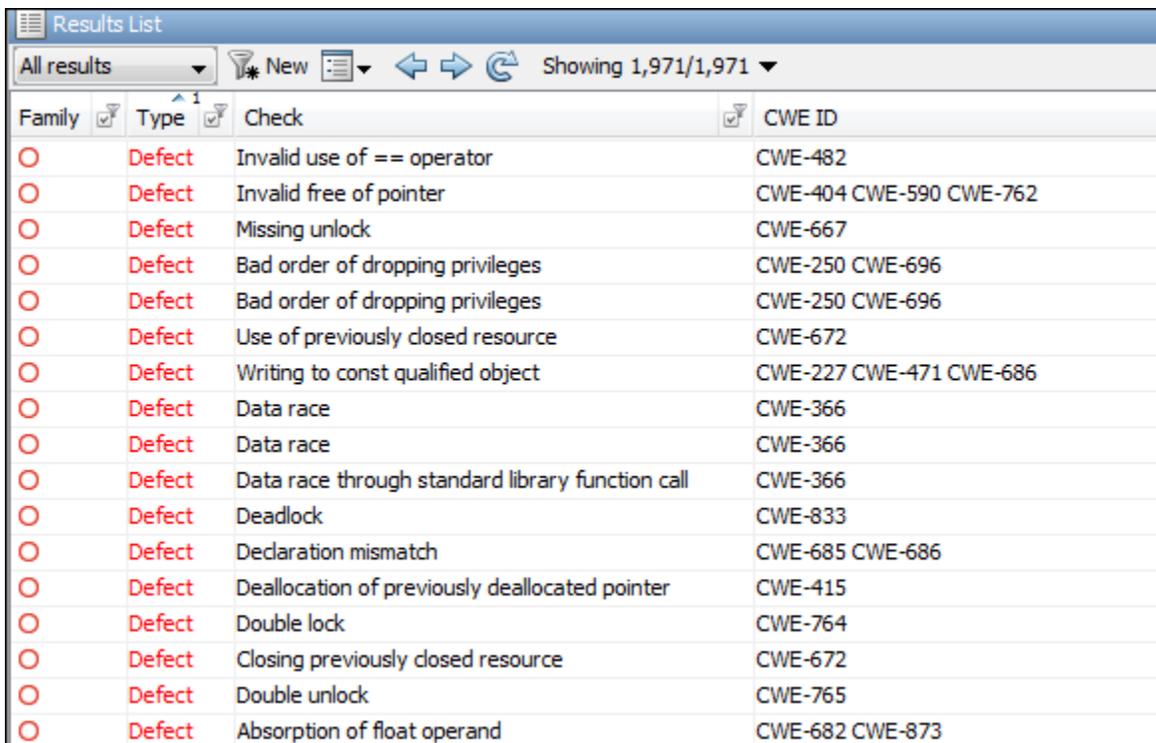
If you run a Code Prover analysis, the run-time errors are mapped to the CERT C standard. All Code Prover run-time checkers are enabled by default.

- ISO/IEC TS 17961: Use both the option to check defects and the option to check coding rules.
 - **Find defects (-checkers)**: Use **ISO-17961**.
 - **Check MISRA C:2012 (-misra3)**: Use **ISO-17961**.

Additional Information

- *Can I look for more defects than the subset that corresponds to the standard?*
Choose all for the options to find defects and coding rules. The analysis looks for all results that it can find, including results mapped to the standard.
You can later filter out results that do not map to a security standard.
- *Can I look for specific IDs instead of all supported IDs from a standard?*
Choose custom for the options to find defects and coding rules. Select defects and coding rules corresponding to specific IDs only.
Save your configuration as a template so that you can reuse it later.
For information on:
 - Which defect or coding rule maps to which ID, see [CWE](#), [CERT C99](#) or [ISO/IEC TS 17961](#).
 - Using configuration templates, see [Create Project Using Configuration Template](#).

Step 2: See Results with IDs from Standard



Family	Type	Check	CWE ID
	Defect	Invalid use of == operator	CWE-482
	Defect	Invalid free of pointer	CWE-404 CWE-590 CWE-762
	Defect	Missing unlock	CWE-667
	Defect	Bad order of dropping privileges	CWE-250 CWE-696
	Defect	Bad order of dropping privileges	CWE-250 CWE-696
	Defect	Use of previously closed resource	CWE-672
	Defect	Writing to const qualified object	CWE-227 CWE-471 CWE-686
	Defect	Data race	CWE-366
	Defect	Data race	CWE-366
	Defect	Data race through standard library function call	CWE-366
	Defect	Deadlock	CWE-833
	Defect	Declaration mismatch	CWE-685 CWE-686
	Defect	Deallocation of previously deallocated pointer	CWE-415
	Defect	Double lock	CWE-764
	Defect	Closing previously closed resource	CWE-672
	Defect	Double unlock	CWE-765
	Defect	Absorption of float operand	CWE-682 CWE-873

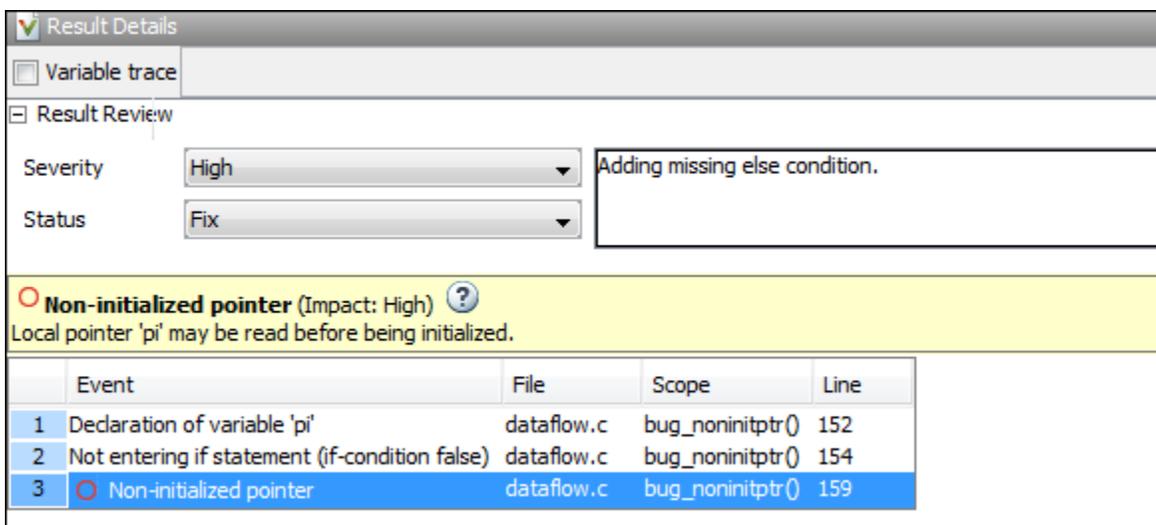
After analysis, see results that correspond to the security standard.

To see the IDs from a security standard, on the **Results List** pane, check the **CWE ID**, **CERT ID** or **ISO-17961 ID** column. If you do not see the column, right-click any column header and enable the column.

Additional Information

- *If I did not choose a security standard before analysis, can I focus on the subset after analysis?*
Narrow your review scope only to results that correspond to a security standard. Instead of **All results** in **Results List**, select **CWE checks**, **CERT checks** or **ISO-17961 checks**.
- *If both a defect and coding rule corresponds to the same security standard ID, will the analysis show both results?*
The defect and coding rule violation both appear in your results list.
If you fix the issue, both results disappear in the next run. If you justify the issue, add your comments for one result and use auto-completion for the other.

Step 3: Fix or Justify Results with Standard IDs



Result Details

Variable trace

Result Review

Severity: High

Status: Fix

Adding missing else condition.

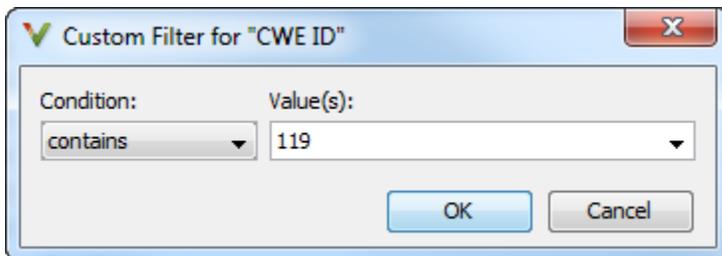
Non-initialized pointer (Impact: High) ?
Local pointer 'pi' may be read before being initialized.

	Event	File	Scope	Line
1	Declaration of variable 'pi'	dataflow.c	bug_noninitptr()	152
2	Not entering if statement (if-condition false)	dataflow.c	bug_noninitptr()	154
3	Non-initialized pointer	dataflow.c	bug_noninitptr()	159

Fix or justify each result. To keep track of your progress, assign the status, To **fix** or **Justified**. For results that you justified, enter comments with your rationale.

Additional Information

- *Can I focus on a single ID after analysis? For instance, can I review all violations of a specific CWE ID together?*
You can filter all results that correspond to a specific ID and review them together.
For instance, on the **CWE ID** column, click the  (filter) icon. From the drop-down list, select **Custom**.
Use the **contains** filter.



Custom Filter for "CWE ID"

Condition: contains

Value(s): 119

OK Cancel

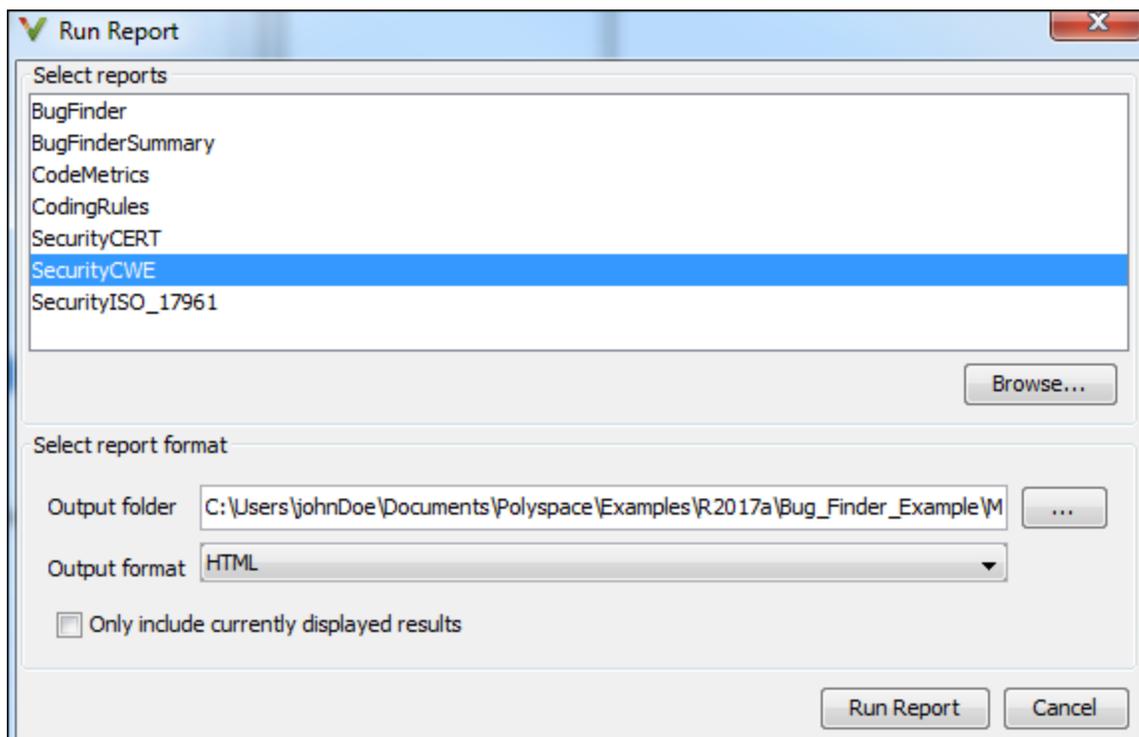
- *Can I review only specific IDs?*

If you ran analysis for all IDs from a standard but want to focus on specific IDs only:

1. *Address each desired ID individually:* Use the custom filter to filter each ID that you want to focus on. Review the results for that ID. In other words, fix or justify the results. Assign the status, To **fix** or **Justified**. For results that you justified, enter comments with your rationale.
2. *Filter out addressed IDs:* Filter out results with **To fix** or **Justified status**.
3. *Assign common status to remaining IDs:* Assign a common status and comment to the remaining defects. To batch-edit these results, **Shift**-select them and add the status and comment.
If you want to create a new status for these IDs, select **Tools > Preferences** and use the **Review Statuses** tab.

In this way, you can make sure that a generated report shows your rationale for IDs that you did not fix.

Step 4: Generate Reports



If you rerun analysis, the results show only the results that you did not fix, along with your rationale for not fixing. Generate a report that shows how you addressed violations of the standard.

To create a report tailored for a security standard, use one of the following templates during report generation:

- CWE: **SecurityCWE**
- CERT C99: **SecurityCERT**
- ISO/IEC TS 17961: **SecurityISO _ 17961**

For more information, see [Generate Reports](#).

Additional Information

- *How is a security standard report template different from other templates?*
In the chapter on defects or coding rules, a separate column shows the security standard ID for each result.
- *If I did not choose a security standard before analysis, can I focus on that subset in the report?*
If you ran analysis for all defects and coding rules, after analysis, narrow your review scope. Instead of All results in Results List, select CWE checks, CERT checks or ISO-17961 checks. Then, generate a filtered report.
For information on filtered reports, see Generate Reports.
- *How do I ensure from the report that the analysis looked for violations of all supported security standard IDs?*
The report appendix shows your options used. To make sure that Bug Finder looked for all supported IDs, check the appendix.
See if the security standard subset or the all subset was used for the following options:
 - *Find defects (-checkers)*
 - *Check MISRA C:2012 (-misra3)*