Built-in Test Configurations

The following tables include the test configurations shipped in the [INSTALL]/configs/builtin directory.

Static Analysis

This group includes universal static analysis test configurations. See Security Compliance Pack for test configurations that enforce security coding standards.

Built-in Test Configuration	Description
Recommended Rules	The default configuration of recommended rules. Covers most Severity 1 and Severity 2 rules. Includes rules in the Flow Analysis Fast configuration.
Recommended .NET Core Rules	Includes rules that identify high-severity defects in .NET Core projects.
Find Duplicated Code	Applies static code analysis rules that report duplicate code. Duplicate code may indicate poor application design and lead to maintainability issues.
Metrics	Computes values for several code metrics.
Flow Analysis	Detects complex runtime errors without requiring test cases or application execution. Defects detected include using uninitialized or invalid memory, null pointer dereferencing, array and buffer overflows, division by zero, memory and resource leaks, and dead code. This requires a special Flow Analysis license option.
Flow Analysis Aggressive	Includes rules for deep flow analysis of code. A significant amount of time may be required to run this configuration.
Flow Analysis Fast	Includes rules for shallow depth of flow analysis, which limits the number of potentially acceptable defects from being reported.
Critical Rules	Includes most Severity 1 rules, as well as rules in the Flow Analysis Fast configuration.
Demo	Includes rules for demonstrating various techniques of code analysis. May not be suitable for large code bases.
Find Memory Issues	Includes rules for finding memory management issues in the code.
Find Unimplemented Scenarios	Includes rules for finding unimplemented scenarios in the code.
Find Unused Code	Includes rules for identifying unused/dead code.
Check Code Compatibility against .NET [2.0 , 3.0, 3.5, 4.0 Client Profile, 4.0 Full, 4.5, 4.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8]	Includes a set of test configurations that validates the code's compatibility with the specified version of . NET framework.
IEC 62304 (Template)	A template test configuration for applying the IEC 62304 Medical standard.
Microsoft Managed Recommended Rules	Applies the Microsoft Managed Recommended Rules that identify the most critical issues in your managed code

Security Compliance Pack

This compliance pack includes test configurations that help you enforce security coding standards and practices. See Compliance Packs Rule Mapping for information how the standards are mapped to dotTEST's rules.

Security Compliance Pack requires dedicated license features to be activated. Contact Parasoft Support for more details on licensing.

Displaying compliance results on DTP

Some test configurations in this category have a corresponding "Compliance" extension on DTP, which allows you to view your security compliance status, generate compliance reports, and monitor the progress towards your security compliance goals. See the "Extensions for DTP" section in the DTP documentation for the list of available extensions, requirements, and usage.

Built-in Test Configuration	Description

CWE 4.0	Includes rules that find issues identified in the CWE standard v4.0. ℹ This test configuration is part of Parasoft Compliance Pack solution that allows you to monitor compliance with industry standards using the "Compliance" extensions on DTP.
CWE Top 25 2019	Includes rules that find issues classified as Top 25 Most Dangerous Programming Errors of the CWE standard. ℹ This test configuration is part of Parasoft Compliance Pack solution that allows you to monitor compliance with industry standards using the "Compliance" extensions on DTP.
CWE Top 25 + On the Cusp 2019	Includes rules that find issues classified as Top 25 Most Dangerous Programming Errors of the CWE standard or included on the CWE Weaknesses On the Cusp list. ℹ This test configuration is part of Parasoft Compliance Pack solution that allows you to monitor compliance with industry standards using the "Compliance" extensions on DTP.
OWASP Top 10-2017	Includes rules that find issues identified in OWASP's Top 10 standard. ℹ This test configuration is part of Parasoft Compliance Pack solution that allows you to monitor compliance with industry standards using the "Compliance" extensions on DTP.
PCI DSS 3.2	Includes rules that find issues identified in PCI Data Security Standard version 3.2.
Security Assessment	General test configuration that finds security issues.
UL 2900	Includes rules that find issues identified in the UL-2900 standard.
Microsoft Secure Coding Guidelines	Includes rules that enforce Microsoft Secure Coding Guidelines.

Unit Testing and Collecting Coverage

This group includes test configurations that allow you to run and collect coverage data for unit tests.

Built-in Test Configuration	Description
Run VSTest Tests	Runs NUnit, MSTest, and xUnit tests that are found in the scope of analysis.
Run VSTest Tests with Coverage	Runs NUnit, MSTest, and xUnit tests that are found in the scope of analysis and monitors coverage.
Run NUnit Tests[1]	Runs NUnit tests that are found in the scope of analysis.
Run NUnit Tests with Coverage[1]	Runs NUnit tests that are found in the scope of analysis and monitors coverage.
Execute MSTests[1]	Executes MSTests tests.
Execute MSTests with Coverage[1]	Executes MSTests tests and collects coverage.
Calculate Application Coverage	Processes the application coverage data to generate a coverage.xml file. See Application Coverage for Web Applications.
Collect Static Coverage	Generates the static coverage data necessary for application coverage. See Application Coverage for Web Applications.

[1] A legacy test configuration. Run your test with `Run VSTest Tests` or `Run VSTest Tests with Coverage`.

Compliance Packs Rule Mapping

This section includes rule mapping for the CWE standard. The mapping information for other standards is available in the PDF rule mapping files shipped with Compliance Packs.

CWE Top 25 Mapping

CWE ID	CWE name/description	Parasoft rule ID(s)
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	• CWE.119.ARRAY

CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	• CWE.79.VPPD • CWE.79.TDRESP • CWE.79.TDXSS
CWE-20	Improper Input Validation	• CWE.20.ARRAY • CWE.20.VPPD • CWE.20.TDNET • CWE.20.TDFNAMES • CWE.20.TDCMD • CWE.20.TDRESP • CWE.20.TDXSS • CWE.20.TDSQL • CWE.20.TDSQLC
CWE-200	Information Exposure	• CWE.200.SENS • CWE.200.PEO • CWE.200.ACPST • CWE.200.CSG
CWE-125	Out-of-bounds Read	• CWE.125.ARRAY
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	• CWE.89.TDSQL • CWE.89.TDSQLC
CWE-416	Use After Free	• CWE.416.DISP • CWE.416.FIN
CWE-190	Integer Overflow or Wraparound	• CWE.190.AIWIL • CWE.190.INTOVERF
CWE-352	Cross-Site Request Forgery (CSRF)	• CWE.352.VPPD • CWE.352.TDRESP • CWE.352.VAFT
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	• CWE.22.TDFNAMES
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	• CWE.78.TDCMD
CWE-787	Out-of-bounds Write	• CWE.787.ARRAY
CWE-287	Improper Authentication	• CWE.287.TDPASSWD • CWE.287.AAM • CWE.287.UAAMC • CWE.287.LUAFLA • CWE.287.IIPHEU
CWE-476	NULL Pointer Dereference	• CWE.476.NR • CWE.476.DEREF • CWE.476.CNFA
CWE-732	Incorrect Permission Assignment for Critical Resource	• CWE.732.ADSVSP

CWE-434	Unrestricted Upload of File with Dangerous Type	• CWE.434.TDFNAMES
CWE-611	Improper Restriction of XML External Entity Reference	• CWE.611.PDTDP • CWE.611.USXRS
CWE-94	Improper Control of Generation of Code ('Code Injection')	• CWE.94.TDCODE
CWE-798	Use of Hard-coded Credentials	• CWE.798.HARDCONN • CWE.798.HPW
CWE-400	Uncontrolled Resource Consumption	• CWE.400.LEAKS
CWE-772	Missing Release of Resource after Effective Lifetime	• CWE.772.LEAKS
CWE-426	Untrusted Search Path	• CWE.426.PBRTE
CWE-502	Deserialization of Untrusted Data	• CWE.502.IIDC • CWE.502.UIS • CWE.502.IDC • CWE.502.MGODWSPA
CWE-269	Improper Privilege Management	• CWE.269.IDENTITY
CWE-295	Improper Certificate Validation	• CWE.295.DNICV

CWE Weaknesses On the Cusp Mapping

CWE ID	CWE name/description	Parasoft rule ID(s)
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')	• CWE.835.IVFLC • CWE.835.IVFLI • CWE.835.NSIVFLN
CWE-522	Insufficiently Protected Credentials	• CWE.522.TDPASSWD
CWE-704	Incorrect Type Conversion or Cast	• CWE.704.ECLTS
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	• CWE.362.LOCKSETGET • CWE.362.DIFCS
CWE-918	Server-Side Request Forgery (SSRF)	• CWE.918.TDNET
CWE-415	Double Free	• N/A
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')	• CWE.601.TDNET

CWE-863	Incorrect Authorization	• CWE.863.AAM • CWE.863.UAAMC • CWE.863.AUTH
CWE-862	Missing Authorization	• CWE.862.UAA
CWE-532	Inclusion of Sensitive Information in Log Files	• CWE.532.ALSI
CWE-306	Missing Authentication for Critical Function	• CWE.306.ADSVSP
CWE-384	Session Fixation	• N/A
CWE-326	Inadequate Encryption Strength	• CWE.326.ICA
CWE-770	Allocation of Resources Without Limits or Throttling	• CWE.770.TDALLOC
CWE-617	Reachable Assertion	• CWE.617.ATA

CWE 4.0 Mapping

CWE ID	CWE name/description	Parasoft rule ID(s)
CWE-20	Improper Input Validation	• CWE.20.ARRAY • CWE.20.VPPD • CWE.20.TDNET • CWE.20.TDFNAMES • CWE.20.TDCMD • CWE.20.TDRESP • CWE.20.TDXSS • CWE.20.TDSQL • CWE.20.TDSQLC
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	• CWE.22.TDFNAMES
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	• CWE.77.TDCMD
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	• CWE.78.TDCMD
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	• CWE.79.VPPD • CWE.79.TDRESP • CWE.79.TDXSS
CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	• CWE.80.VPPD • CWE.80.TDRESP
CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	• CWE.88.TDCMD • CWE.88.VPPD

CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	• CWE.89.TDSQL • CWE.89.TDSQLC
CWE-90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	• CWE.90.TDLDAP
CWE-94	Improper Control of Generation of Code ('Code Injection')	• CWE.94.TDCODE
CWE-95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	• CWE.95.TDCODE
CWE-99	Improper Control of Resource Identifiers ('Resource Injection')	• CWE.99.TDFNAMES • CWE.99.TDNET
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	• CWE.119.ARRAY
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	• CWE.120.AUK
CWE-125	Out-of-bounds Read	• CWE.125.ARRAY
CWE-129	Improper Validation of Array Index	• CWE.129.ARRAY
CWE-131	Incorrect Calculation of Buffer Size	• CWE.131.AUK
CWE-134	Use of Externally-Controlled Format String	• CWE.134.TDINPUT
CWE-190	Integer Overflow or Wraparound	• CWE.190.AIWIL • CWE.190.INTOVERF
CWE-191	Integer Underflow (Wrap or Wraparound)	• CWE.191.AIWIL • CWE.191.INTOVERF
CWE-197	Numeric Truncation Error	• CWE.197.ECLSII
CWE-200	Information Exposure	• CWE.200.SENS • CWE.200.PEO • CWE.200.ACPST • CWE.200.CSG
CWE-201	Information Exposure Through Sent Data	• CWE.201.SELSPLAT
CWE-209	Information Exposure Through an Error Message	• CWE.209.SENS • CWE.209.PEO • CWE.209.ACPST
CWE-212	Improper Cross-boundary Removal of Sensitive Data	• CWE.212.CSG

CWE-250	Execution with Unnecessary Privileges	• CWE.250.AUEP
CWE-252	Unchecked Return Value	• CWE.252.RETVAL • CWE.252.CHECKRET
CWE-256	Unprotected Storage of Credentials	• CWE.256.TDPASSWD
CWE-259	Use of Hard-coded Password	• CWE.259.HPW
CWE-269	Improper Privilege Management	• CWE.269.IDENTITY
CWE-285	Improper Authorization	• CWE.285.TDSQL
CWE-287	Improper Authentication	• CWE.287.TDPASSWD • CWE.287.AAM • CWE.287.UAAMC • CWE.287.LUAFLA • CWE.287.IIPHEU
CWE-295	Improper Certificate Validation	• CWE.295.DNICV
CWE-306	Missing Authentication for Critical Function	• CWE.306.ADSVSP
CWE-307	Improper Restriction of Excessive Authentication Attempts	• CWE.307.LUAFLA
CWE-316	Cleartext Storage of Sensitive Information in Memory	• CWE.316.RSFSS • CWE.316.SSFP
CWE-326	Inadequate Encryption Strength	• CWE.326.ICA
CWE-327	Use of a Broken or Risky Cryptographic Algorithm	• CWE.327.ICA • CWE.327.DNCCKS • CWE.327.ACCA
CWE-328	Reversible One-Way Hash	• CWE.328.ICA
CWE-329	Not Using a Random IV with CBC Mode	• CWE.329.ACCA
CWE-330	Use of Insufficiently Random Values	• CWE.330.USSCR
CWE-350	Reliance on Reverse DNS Resolution for a Security-Critical Action	• CWE.350.IIPHEU
CWE-352	Cross-Site Request Forgery (CSRF)	• CWE.352.VPPD • CWE.352.TDRESP • CWE.352.VAFT

CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	• CWE.362.LOCKSETGET • CWE.362.DIFCS
CWE-369	Divide By Zero	• CWE.369.ZERO
CWE-391	Unchecked Error Condition	• CWE.391.LGE
CWE-395	Use of NullPointerException Catch to Detect NULL Pointer Dereference	• CWE.395.NCNRE
CWE-396	Declaration of Catch for Generic Exception	• CWE.396.NCSAE
CWE-397	Declaration of Throws for Generic Exception	• CWE.397.NTSAE
CWE-400	Uncontrolled Resource Consumption	• CWE.400.LEAKS
CWE-401	Missing Release of Memory after Effective Lifetime	• CWE.401.DBDTFF • CWE.401.DCDSF • CWE.401.DCID • CWE.401.DDFODB • CWE.401.SRIF • CWE.401.TICUFDS • CWE.401.TIID • CWE.401.CBDM • CWE.401.IDWF • CWE.401.MDPP • CWE.401.ASC
CWE-402	Transmission of Private Resources into a New Sphere ('Resource Leak')	• CWE.402.CSG
CWE-412	Unrestricted Externally Accessible Lock	• CWE.412.NLT
CWE-416	Use After Free	• CWE.416.DISP • CWE.416.FIN
CWE-426	Untrusted Search Path	• CWE.426.PBRTE
CWE-434	Unrestricted Upload of File with Dangerous Type	• CWE.434.TDFNAMES
CWE-456	Missing Initialization of a Variable	• CWE.456.NOTEXPLINIT
CWE-457	Use of Uninitialized Variable	• CWE.457.NOTEXPLINIT
CWE-470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	• CWE.470.TDRFL
CWE-476	NULL Pointer Dereference	• CWE.476.NR • CWE.476.DEREF • CWE.476.CNFA

CWE-480	Use of Incorrect Operator	• CWE.480.PUO
CWE-481	Assigning instead of Comparing	• CWE.481.AWC
CWE-494	Download of Code Without Integrity Check	• CWE.494.IREC
CWE-499	Serializable Class Containing Sensitive Data	• CWE.499.CSG
CWE-502	Deserialization of Untrusted Data	• CWE.502.IIDC • CWE.502.UIS • CWE.502.IDC • CWE.502.MGODWSPA
CWE-522	Insufficiently Protected Credentials	• CWE.522.TDPASSWD
CWE-532	Inclusion of Sensitive Information in Log Files	• CWE.532.ALSI
CWE-546	Suspicious Comment	• CWE.546.TODO
CWE-561	Dead Code	• CWE.561.UC
CWE-563	Assignment to Variable without Use	• CWE.563.POVR • CWE.563.VOVR
CWE-570	Expression is Always False	• CWE.570.CC
CWE-571	Expression is Always True	• CWE.571.CC
CWE-595	Comparison of Object References Instead of Object Contents	• CWE.595.REVT
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')	• CWE.601.TDNET
CWE-611	Improper Restriction of XML External Entity Reference	• CWE.611.PDTDP • CWE.611.USXRS
CWE-613	Insufficient Session Expiration	• CWE.613.ISE
CWE-617	Reachable Assertion	• CWE.617.ATA
CWE-662	Improper Synchronization	• CWE.662.DIFCS
CWE-676	Use of Potentially Dangerous Function	• CWE.676.APDM

CWE-681	Incorrect Conversion between Numeric Types	• CWE.681.ECLTS
CWE-704	Incorrect Type Conversion or Cast	• CWE.704.ECLTS
CWE-732	Incorrect Permission Assignment for Critical Resource	• CWE.732.ADSVSP
CWE-759	Use of a One-Way Hash without a Salt	• CWE.759.SALT
CWE-760	Use of a One-Way Hash with a Predictable Salt	• CWE.760.SALT
CWE-770	Allocation of Resources Without Limits or Throttling	• CWE.770.TDALLOC
CWE-772	Missing Release of Resource after Effective Lifetime	• CWE.772.LEAKS
CWE-780	Use of RSA Algorithm without OAEP	• CWE.780.UOWR
CWE-787	Out-of-bounds Write	• CWE.787.ARRAY
CWE-789	Uncontrolled Memory Allocation	• CWE.789.TDALLOC
CWE-798	Use of Hard-coded Credentials	• CWE.798.HARDCONN • CWE.798.HPW
CWE-807	Reliance on Untrusted Inputs in a Security Decision	• CWE.807.AUTH
CWE-827	Improper Control of Document Type Definition	• CWE.827.PDTDP
CWE-829	Inclusion of Functionality from Untrusted Control Sphere	• CWE.829.DMSC • CWE.829.ADLL
CWE-833	Deadlock	• CWE.833.ORDER
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')	• CWE.835.IVFLC • CWE.835.IVFLI • CWE.835.NSIVFLN
CWE-838	Inappropriate Encoding for Output Context	• CWE.838.AIHUE
CWE-862	Missing Authorization	• CWE.862.UAA
CWE-863	Incorrect Authorization	• CWE.863.AAM • CWE.863.UAAMC • CWE.863.AUTH

CWE-918	Server-Side Request Forgery (SSRF)	• CWE.918.TDNET