Built-in Test Configurations

The following table includes 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
Code Smells	Rules based on the Code Smells document (available at http://xp.c2.com/CodeSmell.html) by Kent Beck and Martin Fowler.
Critical Rules	Includes most Severity 1 rules, as well as rules in the Flow Analysis Fast configuration.
Demo Configuration	Includes rules for demonstrating various techniques of code analysis. May not be suitable for large code bases.
Find Duplicated Code	Applies static code analysis rules that report duplicate code. Duplicate code may indicate poor application design and lead to maintainability issues.
Find Memory Problems	Includes rules for finding memory management issues in the code.
Find Unused Code	Includes rules for identifying unused/dead code.
Flow Analysis Standard	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. 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.
Internationalize Code	Applies static code analysis to expose code that is likely to impede internationalization efforts.
Metrics	Computes values for several code metrics.
Recommended Rules	The default configuration of recommended rules. Covers most Severity 1 and Severity 2 rules. Includes rules in the Flow Analysis Fast configuration.
Thread Safe Programming	Rules that uncover code which will be dangerous to run in multi-threaded environments— as well as help prevent common threading problems such as deadlocks, race conditions, a missed notification, infinite loops, and data corruption.
TDD Best Practices	The TDD (Test Driven Development) Best Practices configuration includes rules based on the Code Smells document (available at http://xp.c2.com/CodeSmell.html), rules that check whether the JUnit test classes are comprehensive for the tested class, and rules from the Critical Rules test configuration.
JUnit 4 Best Practices	Includes rules that help you improve the quality of your JUnit 4 unit tests.
JUnit 5 Best Practices	Includes rules that help you improve the quality of your JUnit 5 unit tests.

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 Jtest'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. 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. 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. 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. 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.
CERT for Java	Includes rules that find issues identified in the CERT standard.
UL 2900	Includes rules that find issues identified in the UL-2900 standard.

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
Calculate Application Coverage	Processes the application coverage data to generate a coverage.xml file. See Application Coverage.
Unit Tests	Includes the unit test execution data in the generated report file

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	ParasoftRule ID(s)
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	• CWE.119.ARRAY • CWE.119.ARRAYINP • CWE.119.FREE • CWE.119.BSA • CWE.119.BUSSB
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	• CWE.79.TDXSS • CWE.79.EACM • CWE.79.VPPD • CWE.79.TDRESP • CWE.79.ARXML • CWE.79.TDXML • CWE.79.TDDIG

CWE-20	Improper Input Validation	• CWE.20.TDLIB • CWE.20.APIBS • CWE.20.TDLOG • CWE.20.PLUGIN • CWE.20.EV • CWE.20.DFV • CWE.20.ARRAY • CWE.20.ARRAYINP • CWE.20.FREE • CWE.20.BSA • CWE.20.BUSSB • CWE.20.TDRFL • CWE.20.NATV • CWE.20.NATIW • CWE.20.TDINPUT • CWE.20.TDRESP • CWE.20.IOF • CWE.20.ICO • CWE.20.CACO • CWE.20.INTOVERF • CWE.20.CLP • CWE.20.SYSP • CWE.20.UCO • CWE.20.CSVFV • CWE.20.AEAF • CWE.20.TDNET • CWE.20.VRD • CWE.20.CAI • CWE.20.TDXSS • CWE.20.EACM • CWE.20.VPPD • CWE.20.ARXML • CWE.20.TDXML • CWE.20.TDDIG • CWE.20.TDCMD • CWE.20.UPS • CWE.20.TDSQL • CWE.20.TDXPATH • CWE.20.TDJXPATH • CWE.20.TDLDAP • CWE.20.XPIJ • CWE.20.DCEMSL • CWE.20.ASAPI • CWE.20.TDCODE
CWE-200	Information Exposure	• CWE.200.CONSEN • CWE.200.SENSLOG • CWE.200.EWSSEC • CWE.200.PEO • CWE.200.ACPST • CWE.200.SENS • CWE.200.SIO • CWE.200.FT
CWE-125	Out-of-bounds Read	• CWE.125.ARRAY • CWE.125.ARRAYINP
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	• CWE.89.UPS • CWE.89.TDSQL
CWE-416	Use After Free	• CWE.416.FREE

CWE-190	Integer Overflow or Wraparound	• CWE.190.IOF • CWE.190.BSA • CWE.190.ICO • CWE.190.CACO • CWE.190.INTOVERF • CWE.190.CLP
CWE-352	Cross-Site Request Forgery (CSRF)	• CWE.352.TDXSS • CWE.352.VPPD • CWE.352.EACM • CWE.352.UOSC • CWE.352.TDRESP • CWE.352.DCSRFJAVA • CWE.352.DCSRFXML • CWE.352.REQMAP
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.787.ARRAYINP
CWE-287	Improper Authentication	• CWE.287.HCCS • CWE.287.PCCF • CWE.287.UPWD • CWE.287.PTPT • CWE.287.PWDXML • CWE.287.WPWD • CWE.287.UTAX • CWE.287.WCPWD • CWE.287.HCCK • CWE.287.PLAIN • CWE.287.HV • CWE.287.VSI • CWE.287.HTTPRHA • CWE.287.DNSL • CWE.287.MLVP • CWE.287.PWDPROP • CWE.287.USC • CWE.287.TDPASSWD • CWE.287.CAM • CWE.287.SSM • CWE.287.UOSC • CWE.287.PBFA • CWE.287.CKTS
CWE-476	NULL Pointer Dereference	• CWE.476.NP • CWE.476.DEREF
CWE-732	Incorrect Permission Assignment for Critical Resource	• CWE.732.SCHTTP
CWE-434	Unrestricted Upload of File with Dangerous Type	• CWE.434.TDFNAMES
CWE-611	Improper Restriction of XML External Entity Reference	• CWE.611.DXXE • CWE.611.XMLVAL

CWE-94	Improper Control of Generation of Code ('Code Injection')	• CWE.94.DCEMSL • CWE.94.ASAPI • CWE.94.TDCODE
CWE-798	Use of Hard-coded Credentials	• CWE.798.HCCS • CWE.798.PCCF • CWE.798.UPWD • CWE.798.PTPT • CWE.798.PWDXML • CWE.798.WPWD • CWE.798.UTAX • CWE.798.WCPWD • CWE.798.HCCK
CWE-400	Uncontrolled Resource Consumption	• CWE.400.DMDS • CWE.400.ISTART • CWE.400.TDALLOC • CWE.400.LEAKS
CWE-772	Missing Release of Resource after Effective Lifetime	• CWE.772.LEAKS • CWE.772.CLOSE • CWE.772.LML
CWE-426	Untrusted Search Path	• CWE.426.PBRTE
CWE-502	Deserialization of Untrusted Data	• CWE.502.SC • CWE.502.RWAF • CWE.502.SSSD • CWE.502.MASP • CWE.502.AUXD • CWE.502.VOBD
CWE-269	Improper Privilege Management	• CWE.269.LDP • CWE.269.PCL • CWE.269.DPANY
CWE-295	Improper Certificate Validation	• CWE.295.HV • CWE.295.VSI

CWE Weaknesses On the Cusp Mapping

CWE ID	CWE Name	ParasoftRule ID(s)
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')	• CWE.835.AIL • CWE.835.PCIF
CWE-522	Insufficiently Protected Credentials	• CWE.522.UPWD • CWE.522.PWDXML • CWE.522.USC • CWE.522.UTAX • CWE.522.PWDPROP • CWE.522.PLAIN • CWE.522.TDPASSWD • CWE.522.PCCF • CWE.522.PTPT • CWE.522.WCPWD • CWE.522.WPWD

CWE-704	Incorrect Type Conversion or Cast	• CWE.704.AGBPT • CWE.704.CPTS • CWE.704.IDCD • CWE.704.CLP
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	• CWE.362.DCL • CWE.362.TOCTOU
CWE-918	Server-Side Request Forgery (SSRF)	• CWE.918.TDNET
CWE-415	Double Free	• CWE.415.
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')	• CWE.601.TDNET • CWE.601.TDRESP • CWE.601.UCO • CWE.601.VRD
CWE-863	Incorrect Authorization	• CWE.863.DSR • CWE.863.SRCD
CWE-862	Missing Authorization	• CWE.862.PERMIT • CWE.862.LCA
CWE-532	Inclusion of Sensitive Information in Log Files	• CWE.532.CONSEN • CWE.532.SENSLOG
CWE-306	Missing Authentication for Critical Function	• CWE.306.CAM • CWE.306.SSM • CWE.306.UOSC • CWE.306.USC
CWE-384	Session Fixation	• CWE.384.ISL
CWE-326	Inadequate Encryption Strength	• CWE.326.AISSAJAVA • CWE.326.ICA • CWE.326.SRD • CWE.326.AUNC • CWE.326.AISSAXML • CWE.326.MDSALT • CWE.326.CKTS
CWE-770	Allocation of Resources Without Limits or Throttling	• CWE.770.ISTART • CWE.770.TDALLOC
CWE-617	Reachable Assertion	• CWE.617.ASSERT

CWE 4.0 Mapping

CWE ID	CWE Name	ParasoftRule ID(s)

CWE-6	J2EE Misconfiguration: Insufficient Session-ID Length	• CWE.6.SLID
CWE-7	J2EE Misconfiguration: Missing Custom Error Page	• CWE.7.SEP
CWE-8	J2EE Misconfiguration: Entity Bean Declared Remote	• CWE.8.RR
CWE-9	J2EE Misconfiguration: Weak Access Permissions for EJB Methods	• CWE.9.DPANY
CWE-15	External Control of System or Configuration Setting	• CWE.15.SYSP • CWE.15.UCO
CWE-20	Improper Input Validation	• CWE.20.TDLIB • CWE.20.APIBS • CWE.20.TDLOG • CWE.20.PLUGIN • CWE.20.EV • CWE.20.DFV • CWE.20.ARRAY • CWE.20.ARRAYINP • CWE.20.FREE • CWE.20.BSA • CWE.20.BUSSB • CWE.20.TDRFL • CWE.20.NATV • CWE.20.NATIW • CWE.20.TDINPUT • CWE.20.TDRESP • CWE.20.IOF • CWE.20.ICO • CWE.20.CACO • CWE.20.INTOVERF • CWE.20.CLP • CWE.20.SYSP • CWE.20.UCO • CWE.20.CSVFV • CWE.20.AEAF • CWE.20.TDNET • CWE.20.VRD • CWE.20.CAI • CWE.20.TDXSS • CWE.20.EACM • CWE.20.VPPD • CWE.20.ARXML • CWE.20.TDXML • CWE.20.TDDIG • CWE.20.TDCMD • CWE.20.UPS • CWE.20.TDSQL • CWE.20.TDXPATH • CWE.20.TDJXPATH • CWE.20.TDLDAP • CWE.20.XPIJ • CWE.20.DCEMSL • CWE.20.ASAPI • CWE.20.TDCODE
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.TDXSS • CWE.79.EACM • CWE.79.VPPD • CWE.79.TDRESP • CWE.79.ARXML • CWE.79.TDXML • CWE.79.TDDIG
CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	• CWE.80.ARXML • CWE.80.TDXML • CWE.80.TDDIG
CWE-81	Improper Neutralization of Script in an Error Message Web Page	• CWE.81.ARXML
CWE-83	Improper Neutralization of Script in Attributes in a Web Page	• CWE.83.ARXML
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	• CWE.89.UPS • CWE.89.TDSQL
CWE-90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	• CWE.90.TDLDAP
CWE-91	XML Injection (aka Blind XPath Injection)	• CWE.91.TDXML • CWE.91.TDXPATH • CWE.91.TDJXPATH • CWE.91.XPIJ
CWE-94	Improper Control of Generation of Code ('Code Injection')	• CWE.94.DCEMSL • CWE.94.ASAPI • 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.TDNET • CWE.99.DFV
CWE-102	Struts: Duplicate Validation Forms	• CWE.102.DFV
CWE-103	Struts: Incomplete validate() Method Definition	• CWE.103.CSVFV
CWE-104	Struts: Form Bean Does Not Extend Validation Class	• CWE.104.AEAF
CWE-106	Struts: Plug-in Framework not in Use	• CWE.106.PLUGIN
CWE-109	Struts: Validator Turned Off	• CWE.109.EV
CWE-111	Direct Use of Unsafe JNI	• CWE.111.NATV • CWE.111.NATIW

CWE-113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')	• CWE.113.TDRESP
CWE-114	Process Control	• CWE.114.TDLIB • CWE.114.APIBS
CWE-117	Improper Output Neutralization for Logs	• CWE.117.TDLOG
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	• CWE.119.ARRAY • CWE.119.ARRAYINP • CWE.119.FREE • CWE.119.BSA • CWE.119.BUSSB
CWE-125	Out-of-bounds Read	• CWE.125.ARRAY • CWE.125.ARRAYINP
CWE-129	Improper Validation of Array Index	• CWE.129.CAI • CWE.129.ARRAY • CWE.129.ARRAYINP
CWE-131	Incorrect Calculation of Buffer Size	• CWE.131.ARRAY
CWE-134	Use of Externally-Controlled Format String	• CWE.134.TDINPUT
CWE-185	Incorrect Regular Expression	• CWE.185.REP
CWE-190	Integer Overflow or Wraparound	• CWE.190.IOF • CWE.190.BSA • CWE.190.ICO • CWE.190.CACO • CWE.190.INTOVERF • CWE.190.CLP
CWE-191	Integer Underflow (Wrap or Wraparound)	• CWE.191.BSA • CWE.191.INTOVERF
CWE-193	Off-by-one Error	• CWE.193.AOBO
CWE-200	Information Exposure	• CWE.200.CONSEN • CWE.200.SENSLOG • CWE.200.EWSSEC • CWE.200.PEO • CWE.200.ACPST • CWE.200.SENS • CWE.200.SIO • CWE.200.FT
CWE-209	Information Exposure Through an Error Message	• CWE.209.PEO • CWE.209.ACPST • CWE.209.SENS • CWE.209.SIO

CWE-212	Improper Cross-boundary Removal of Sensitive Data	• CWE.212.FT
CWE-213	Intentional Information Exposure	• CWE.213.CONSEN
CWE-215	Information Exposure Through Debug Information	• CWE.215.EWSSEC
CWE-245	J2EE Bad Practices: Direct Management of Connections	• CWE.245.JDBCTEMPLATE
CWE-246	J2EE Bad Practices: Direct Use of Sockets	• CWE.246.AUS • CWE.246.SS • CWE.246.NSF
CWE-250	Execution with Unnecessary Privileges	• CWE.250.LDP • CWE.250.PCL
CWE-252	Unchecked Return Value	• CWE.252.CRRV • CWE.252.CHECKRET
CWE-256	Unprotected Storage of Credentials	• CWE.256.PLAIN • CWE.256.PWDPROP • CWE.256.TDPASSWD • CWE.256.PWDXML • CWE.256.UPWD • CWE.256.PCCF • CWE.256.PTPT • CWE.256.UTAX • CWE.256.WCPWD • CWE.256.WPWD
CWE-258	Empty Password in Configuration File	• CWE.258.PWDPROP
CWE-260	Password in Configuration File	• CWE.260.UTAX • CWE.260.PWDPROP
CWE-261	Weak Cryptography for Passwords	• CWE.261.CKTS
CWE-269	Improper Privilege Management	• CWE.269.LDP • CWE.269.PCL • CWE.269.DPANY

CWE-287	Improper Authentication	• CWE.287.HCCS • CWE.287.PCCF • CWE.287.UPWD • CWE.287.PTPT • CWE.287.PWDXML • CWE.287.WPWD • CWE.287.UTAX • CWE.287.WCPWD • CWE.287.HCCK • CWE.287.PLAIN • CWE.287.HV • CWE.287.VSI • CWE.287.HTTPRHA • CWE.287.DNSL • CWE.287.MLVP • CWE.287.PWDPROP • CWE.287.USC • CWE.287.TDPASSWD • CWE.287.CAM • CWE.287.SSM • CWE.287.UOSC • CWE.287.PBFA • CWE.287.CKTS
CWE-290	Authentication Bypass by Spoofing	• CWE.290.HTTPRHA • CWE.290.DNSL
CWE-295	Improper Certificate Validation	• CWE.295.HV • CWE.295.VSI
CWE-297	Improper Validation of Certificate with Host Mismatch	• CWE.297.VSI
CWE-306	Missing Authentication for Critical Function	• CWE.306.CAM • CWE.306.SSM • CWE.306.UOSC • CWE.306.USC
CWE-307	Improper Restriction of Excessive Authentication Attempts	• CWE.307.PBFA
CWE-309	Use of Password System for Primary Authentication	• CWE.309.MLVP
CWE-311	Missing Encryption of Sensitive Data	• CWE.311.HTTPS • CWE.311.USC • CWE.311.SENS • CWE.311.PWDPROP • CWE.311.PWDXML • CWE.311.PLAIN • CWE.311.PLC • CWE.311.UOSC • CWE.311.HCNA
CWE-312	Cleartext Storage of Sensitive Information	• CWE.312.PWDPROP • CWE.312.PLAIN • CWE.312.PLC
CWE-313	Cleartext Storage in a File or on Disk	• CWE.313.PLAIN
CWE-315	Cleartext Storage of Sensitive Information in a Cookie	• CWE.315.PLC

CWE-319	Cleartext Transmission of Sensitive Information	• CWE.319.HCNA
CWE-321	Use of Hard-coded Cryptographic Key	• CWE.321.HCCK
CWE-325	Missing Required Cryptographic Step	• CWE.325.SIKG • CWE.325.MCMDU
CWE-326	Inadequate Encryption Strength	• CWE.326.AISSAJAVA • CWE.326.ICA • CWE.326.SRD • CWE.326.AUNC • CWE.326.AISSAXML • CWE.326.MDSALT • CWE.326.CKTS
CWE-327	Use of a Broken or Risky Cryptographic Algorithm	• CWE.327.AISSAJAVA • CWE.327.ICA • CWE.327.SRD • CWE.327.ACMD • CWE.327.AUNC • CWE.327.AISSAXML • CWE.327.MDSALT
CWE-328	Reversible One-Way Hash	• CWE.328.AISSAJAVA • CWE.328.ICA • CWE.328.SRD • CWE.328.AUNC • CWE.328.AISSAXML • CWE.328.MDSALT
CWE-329	Not Using a Random IV with CBC Mode	• CWE.329.ENPP • CWE.329.IVR
CWE-336	Same Seed in Pseudo-Random Number Generator (PRNG)	• CWE.336.ENPP
CWE-337	Predictable Seed in Pseudo-Random Number Generator (PRNG)	• CWE.337.ENPP
CWE-338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	• CWE.338.SRD
CWE-346	Origin Validation Error	• CWE.346.JXCORS
CWE-347	Improper Verification of Cryptographic Signature	• CWE.347.VJFS
CWE-350	Reliance on Reverse DNS Resolution for a Security-Critical Action	• CWE.350.DNSL

CWE-352	Cross-Site Request Forgery (CSRF)	• CWE.352.TDXSS • CWE.352.VPPD • CWE.352.EACM • CWE.352.UOSC • CWE.352.TDRESP • CWE.352.DCSRFJAVA • CWE.352.DCSRFXML • CWE.352.REQMAP
CWE-359	Exposure of Private Information ('Privacy Violation')	• CWE.359.CONSEN
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	• CWE.362.DCL • CWE.362.TOCTOU
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition	• CWE.367.TOCTOU
CWE-369	Divide By Zero	• CWE.369.ZERO
CWE-375	Returning a Mutable Object to an Untrusted Caller	• CWE.375.RA
CWE-377	Insecure Temporary File	• CWE.377.ATF
CWE-382	J2EE Bad Practices: Use of System.exit()	• CWE.382.EXIT • CWE.382.JVM
CWE-383	J2EE Bad Practices: Direct Use of Threads	• CWE.383.THR
CWE-384	Session Fixation	• CWE.384.ISL
CWE-390	Detection of Error Condition Without Action	• CWE.390.LGE
CWE-391	Unchecked Error Condition	• CWE.391.AECB
CWE-395	Use of NullPointerException Catch to Detect NULL Pointer Dereference	• CWE.395.NCNPE
CWE-396	Declaration of Catch for Generic Exception	• CWE.396.NCE
CWE-397	Declaration of Throws for Generic Exception	• CWE.397.NTX • CWE.397.NTERR
CWE-400	Uncontrolled Resource Consumption	• CWE.400.DMDS • CWE.400.ISTART • CWE.400.TDALLOC • CWE.400.LEAKS
CWE-401	Missing Release of Memory after Effective Lifetime	• CWE.401.LML

CWE-404	Improper Resource Shutdown or Release	• CWE.404.COCO • CWE.404.CRWD • CWE.404.ODBIL • CWE.404.LEAKS • CWE.404.FCF • CWE.404.CLOSE • CWE.404.LML
CWE-413	Improper Resource Locking	• CWE.413.LORD
CWE-416	Use After Free	• CWE.416.FREE
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.LV
CWE-457	Use of Uninitialized Variable	• CWE.457.NP • CWE.457.NOTINITCTOR • CWE.457.UIRC • CWE.457.NOTEXPLINIT
CWE-459	Incomplete Cleanup	• CWE.459.LEAKS • CWE.459.FCF
CWE-470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	• CWE.470.TDRFL • CWE.470.APIBS
CWE-476	NULL Pointer Dereference	• CWE.476.NP • CWE.476.DEREF
CWE-477	Use of Obsolete Function	• CWE.477.DPRAPI
CWE-478	Missing Default Case in Switch Statement	• CWE.478.PDS
CWE-481	Assigning instead of Comparing	• CWE.481.ASI
CWE-483	Incorrect Block Delimitation	• CWE.483.BLK • CWE.483.EBI • CWE.483.EB
CWE-484	Omitted Break Statement in Switch	• CWE.484.SBC • CWE.484.DAV
CWE-486	Comparison of Classes by Name	• CWE.486.CMP • CWE.486.AUG

CWE-487	Reliance on Package-level Scope	• CWE.487.AF
CWE-491	Public cloneable() Method Without Final ('Object Hijack')	• CWE.491.CLONE
CWE-495	Private Data Structure Returned From A Public Method	• CWE.495.RA
CWE-496	Public Data Assigned to Private Array-Typed Field	• CWE.496.CAP
CWE-497	Exposure of System Data to an Unauthorized Control Sphere	• CWE.497.SENS • CWE.497.PEO
CWE-499	Serializable Class Containing Sensitive Data	• CWE.499.SIF • CWE.499.SER
CWE-500	Public Static Field Not Marked Final	• CWE.500.SPFF
CWE-501	Trust Boundary Violation	• CWE.501.TDSESSION
CWE-502	Deserialization of Untrusted Data	• CWE.502.SC • CWE.502.RWAF • CWE.502.SSSD • CWE.502.MASP • CWE.502.AUXD • CWE.502.VOBD
CWE-506	Embedded Malicious Code	• CWE.506.HCCK • CWE.506.RDM
CWE-511	Logic/Time Bomb	• CWE.511.RDM
CWE-521	Weak Password Requirements	• CWE.521.MLVP • CWE.521.PWDPROP
CWE-522	Insufficiently Protected Credentials	• CWE.522.UPWD • CWE.522.PWDXML • CWE.522.USC • CWE.522.UTAX • CWE.522.PWDPROP • CWE.522.PLAIN • CWE.522.TDPASSWD • CWE.522.PCCF • CWE.522.PTPT • CWE.522.WCPWD • CWE.522.WPWD
CWE-523	Unprotected Transport of Credentials	• CWE.523.USC
CWE-532	Inclusion of Sensitive Information in Log Files	• CWE.532.CONSEN • CWE.532.SENSLOG

CWE-543	Use of Singleton Pattern Without Synchronization in a Multithreaded Context	• CWE.543.IASF • CWE.543.ILI
CWE-546	Suspicious Comment	• CWE.546.TODOJAVA • CWE.546.TODOPROP • CWE.546.TODOXML
CWE-555	J2EE Misconfiguration: Plaintext Password in Configuration File	• CWE.555.UPWD • CWE.555.PWDXML
CWE-561	Dead Code	• CWE.561.CC • CWE.561.DEREF • CWE.561.SWITCH • CWE.561.PM
CWE-563	Assignment to Variable without Use	• CWE.563.UPPF • CWE.563.VOVR • CWE.563.AURV • CWE.563.UP • CWE.563.POVR • CWE.563.PF
CWE-568	finalize() Method Without super.finalize()	• CWE.568.FCF
CWE-570	Expression is Always False	• CWE.570.CC • CWE.570.UCIF
CWE-571	Expression is Always True	• CWE.571.CC • CWE.571.UCIF
CWE-572	Call to Thread run() instead of start()	• CWE.572.IRUN
CWE-576	EJB Bad Practices: Use of Java I/O	• CWE.576.JIO
CWE-577	EJB Bad Practices: Use of Sockets	• CWE.577.AUS
CWE-578	EJB Bad Practices: Use of Class Loader	• CWE.578.ACL
CWE-579	J2EE Bad Practices: Non-serializable Object Stored in Session	• CWE.579.ONS • CWE.579.SNSO
CWE-580	clone() Method Without super.clone()	• CWE.580.SCLONE
CWE-581	Object Model Violation: Just One of Equals and Hashcode Defined	• CWE.581.OVERRIDE
CWE-582	Array Declared Public, Final, and Static	• CWE.582.PSFA • CWE.582.IMM

CWE-583	finalize() Method Declared Public	• CWE.583.MFP
CWE-584	Return Inside Finally Block	• CWE.584.ARCF
CWE-585	Empty Synchronized Block	• CWE.585.SNE
CWE-586	Explicit Call to Finalize()	• CWE.586.NCF
CWE-594	J2EE Framework: Saving Unserializable Objects to Disk	• CWE.594.SIVS
CWE-595	Comparison of Object References Instead of Object Contents	• CWE.595.UEIC
CWE-600	Uncaught Exception in Servlet	• CWE.600.CETS
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')	• CWE.601.TDNET • CWE.601.TDRESP • CWE.601.UCO • CWE.601.VRD
CWE-605	Multiple Binds to the Same Port	• CWE.605.HCNA
CWE-607	Public Static Final Field References Mutable Object	• CWE.607.RMO • CWE.607.IMM
CWE-609	Double-Checked Locking	• CWE.609.DCL
CWE-611	Improper Restriction of XML External Entity Reference	• CWE.611.DXXE • CWE.611.XMLVAL
CWE-613	Insufficient Session Expiration	• CWE.613.STTL • CWE.613.RUIM
CWE-614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	• CWE.614.UOSC
CWE-617	Reachable Assertion	• CWE.617.ASSERT
CWE-643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')	• CWE.643.TDXPATH • CWE.643.TDJXPATH
CWE-644	Improper Neutralization of HTTP Headers for Scripting Syntax	• CWE.644.TDRESP
CWE-652	Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')	• CWE.652.TDXPATH • CWE.652.XPIJ

CWE-662	Improper Synchronization	• CWE.662.DIFCS • CWE.662.IASF • CWE.662.ILI • CWE.662.CLOSE • CWE.662.LOCK • CWE.662.DLOCK • CWE.662.LORD • CWE.662.RLF • CWE.662.STR • CWE.662.UWNA • CWE.662.CSFS • CWE.662.TSHL • CWE.662.ORDER • CWE.662.DCL • CWE.662.IRUN
CWE-665	Improper Initialization	• CWE.665.NOTINITCTOR • CWE.665.NOTEXPLINIT • CWE.665.NP • CWE.665.UIRC • CWE.665.ISTART • CWE.665.TDALLOC • CWE.665.LV
CWE-667	Improper Locking	• CWE.667.CLOSE • CWE.667.LOCK • CWE.667.DLOCK • CWE.667.LORD • CWE.667.RLF • CWE.667.STR • CWE.667.UWNA • CWE.667.CSFS • CWE.667.TSHL • CWE.667.ORDER • CWE.667.DCL
CWE-674	Uncontrolled Recursion	• CWE.674.FLRC
CWE-676	Use of Potentially Dangerous Function	• CWE.676.SRD
CWE-680	Integer Overflow to Buffer Overflow	• CWE.680.BSA
CWE-681	Incorrect Conversion between Numeric Types	• CWE.681.IDCD • CWE.681.CLP

CWE-691	Insufficient Control Flow Management	• CWE.691.ANL • CWE.691.PERMIT • CWE.691.PBFA • CWE.691.AIL • CWE.691.PCIF • CWE.691.DCEMSL • CWE.691.ASAPI • CWE.691.TDCODE • CWE.691.DCL • CWE.691.TOCTOU • CWE.691.ASI • CWE.691.ASSERT • CWE.691.BLK • CWE.691.EBI • CWE.691.EB • CWE.691.SBC • CWE.691.DAV • CWE.691.DIFCS • CWE.691.IASF • CWE.691.ILI • CWE.691.CLOSE • CWE.691.LOCK • CWE.691.DLOCK • CWE.691.LORD • CWE.691.RLF • CWE.691.STR • CWE.691.UWNA • CWE.691.CSFS • CWE.691.TSHL • CWE.691.ORDER • CWE.691.IRUN • CWE.691.FLRC • CWE.691.CETS • CWE.691.EXIT • CWE.691.JVM • CWE.691.NCNPE • CWE.691.NCE • CWE.691.NTX • CWE.691.NTERR • CWE.691.ARCF • CWE.691.DPPM • CWE.691.DPAM • CWE.691.SPAM
CWE-704	Incorrect Type Conversion or Cast	• CWE.704.AGBPT • CWE.704.CPTS • CWE.704.IDCD • CWE.704.CLP
CWE-732	Incorrect Permission Assignment for Critical Resource	• CWE.732.SCHTTP
CWE-749	Exposed Dangerous Method or Function	• CWE.749.DPPM • CWE.749.DPAM • CWE.749.SPAM
CWE-755	Improper Handling of Exceptional Conditions	• CWE.755.CIET • CWE.755.SEP • CWE.755.LGE • CWE.755.PEO • CWE.755.ACPST • CWE.755.SENS • CWE.755.SIO • CWE.755.NCNPE • CWE.755.NCE
CWE-759	Use of a One-Way Hash without a Salt	• CWE.759.MDSALT

CWE-764	Multiple Locks of a Critical Resource	• CWE.764.DLOCK
CWE-770	Allocation of Resources Without Limits or Throttling	• CWE.770.ISTART • CWE.770.TDALLOC
CWE-771	Missing Reference to Active Allocated Resource	• CWE.771.LEAKS
CWE-772	Missing Release of Resource after Effective Lifetime	• CWE.772.LEAKS • CWE.772.CLOSE • CWE.772.LML
CWE-778	Insufficient Logging	• CWE.778.ENFL
CWE-787	Out-of-bounds Write	• CWE.787.ARRAY • CWE.787.ARRAYINP
CWE-789	Uncontrolled Memory Allocation	• CWE.789.TDALLOC
CWE-798	Use of Hard-coded Credentials	• CWE.798.HCCS • CWE.798.PCCF • CWE.798.UPWD • CWE.798.PTPT • CWE.798.PWDXML • CWE.798.WPWD • CWE.798.UTAX • CWE.798.WCPWD • CWE.798.HCCK
CWE-806	Buffer Access Using Size of Source Buffer	• CWE.806.BUSSB
CWE-807	Reliance on Untrusted Inputs in a Security Decision	• CWE.807.PLC • CWE.807.UOSC • CWE.807.HGRSI • CWE.807.DNSL
CWE-829	Inclusion of Functionality from Untrusted Control Sphere	• CWE.829.TDXPATH • CWE.829.TDFILES • CWE.829.TDFNAMES • CWE.829.TDLIB
CWE-832	Unlock of a Resource that is not Locked	• CWE.832.LORD
CWE-833	Deadlock	• CWE.833.RLF • CWE.833.STR • CWE.833.UWNA • CWE.833.CSFS • CWE.833.TSHL • CWE.833.ORDER
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')	• CWE.835.AIL • CWE.835.PCIF

CWE-836	Use of Password Hash Instead of Password for Authentication	• CWE.836.PLAIN
CWE-838	Inappropriate Encoding for Output Context	• CWE.838.SEO
CWE-841	Improper Enforcement of Behavioral Workflow	• CWE.841.PERMIT
CWE-862	Missing Authorization	• CWE.862.PERMIT • CWE.862.LCA
CWE-863	Incorrect Authorization	• CWE.863.DSR • CWE.863.SRCD
CWE-918	Server-Side Request Forgery (SSRF)	• CWE.918.TDNET
CWE-1004	Sensitive Cookie Without 'HttpOnly' Flag	• CWE.1004.SCHTTP