PARASOFT

Parasoft Support for CWE in Java - Jtest 10.x

The following table shows how Mitre's Common Weakness Enumeration (CWE) maps to Parasoft's static analysis rules for Java.

CWE ID	CWE Name/Description	Parasoft Rule ID(s)
CWE-5	J2EE Misconfiguration: Data Transmission Without Encryption	PROPS.PLAIN
CWE-6	J2EE Misconfiguration: Insufficient Session-ID Length	SECURITY.UEC.SLID
CWE-7	J2EE Misconfiguration: Missing Custom Error Page	SECURITY.UEC.SEP
CWE-8	J2EE Misconfiguration: Entity Bean Declared Remote	EJB.RR
CWE-9	J2EE Misconfiguration: Weak Access Permissions for EJB Methods	EJB.DPANY
CWE-15	External Control of System or Configuration Setting	SECURITY.BV.SYSP SERVLET.UCO
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	BD.SECURITY.TDFNAMES
CWE-23	Relative Path Traversal	BD.SECURITY.TDFNAMES
CWE-36	Absolute Path Traversal	BD.SECURITY.TDFNAMES
CWE-73	External Control of File Name or Path	BD.SECURITY.TDFNAMES
CWE-77	Command Injection	BD.SECURITY.TDCMD
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	BD.SECURITY.TDCMD BD.SECURITY.TDENV
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	SECURITY.IBA.CDBV BD.SECURITY.TDRESP BD.SECURITY.TDXSS
CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	SECURITY.WSC.ARXML BD.SECURITY.TDRESP BD.SECURITY.TDXML BD.SECURITY.TDXSS BD.SECURITY.TDDIG
CWE-81	Improper Neutralization of Script in an Error Message Web Page	SECURITY.WSC.ARXML

CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	SECURITY.IBA.UPS BD.SECURITY.TDSQL
CWE-90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	BD.SECURITY.TDLDAP
CWE-91	XML Injection (aka Blind XPath Injection)	BD.SECURITY.TDXML SECURITY.IBA.XPIJ BD.SECURITY.TDXPATH
CWE-99	Improper Control of Resource Identifiers ('Resource Injection')	BD.SECURITY.TDNET
CWE-102	Struts: Duplicate Validation Forms	STRUTS.DFV
CWE-103	Struts: Incomplete validate() Method Definition	SECURITY.IBA.CSVFV
CWE-104	Struts: Form Bean Does Not Extend Validation Class	SECURITY.IBA.AEAF
CWE-106	Struts: Plug-in Framework not in Use	STRUTS.PLUGIN
CWE-109	Struts: Validator Turned Off	STRUTS.EV
CWE-111	Direct Use of Unsafe JNI	PORT.NATV SECURITY.IBA.NATIW SECURITY.WSC.APIBS
CWE-113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')	BD.SECURITY.TDRESP
CWE-114	Process Control	BD.SECURITY.TDLIB SECURITY.WSC.APIBS
CWE-117	Improper Output Neutralization for Logs	BD.SECURITY.TDLOG
CWE-129	Improper Validation of Array Index	PB.RE.CAI BD.PB.ARRAY BD.PB.ARRAYINP
CWE-180	Incorrect Behavior Order: Validate Before Canonicalize	SECURITY.WSC.SSM BD.SECURITY.TDRESP BD.SECURITY.TDXSS
CWE-185	Incorrect Regular Expression	PB.API.REP
CWE-190	Integer Overflow or Wraparound	PB.NUM.IOF PB.NUM.BSA PB.NUM.ICO PB.NUM.CACO
CWE-191	Integer Underflow (Wrap or Wraparound)	PB.NUM.BSA
CWE-193	Off-by-one Error	PB.LOGIC.AOBO
CWE-197	Numeric Truncation Error	PB.NUM.CLP

CWE-209	Information Exposure Through an Error Message	SECURITY.ESD.PEO SECURITY.WSC.ACPST BD.SECURITY.SENS
CWE-213	Intentional Information Exposure	SECURITY.ESD.CONSEN
CWE-245	J2EE Bad Practices: Direct Management of Connections	SPRING.JDBCTEMPLATE
CWE-246	J2EE Bad Practices: Direct Use of Sockets	EJB.AUS SECURITY.WSC.SS SECURITY.BV.NSF
CWE-248	Uncaught Exception	SERVLET.CETS
CWE-250	Execution with Unnecessary Privileges	SECURITY.EAB.LDP SECURITY.EAB.PCL
CWE-252	Unchecked Return Value	PB.LOGIC.CRRV
CWE-256	Plaintext Storage of a Password	PROPS.PLAIN SECURITY.UEC.PWDPROP
CWE-258	Empty Password in Configuration File	SECURITY.UEC.PWDPROP
CWE-259	Use of Hard-coded Password	SECURITY.WSC.HCCS PORT.HCNA
CWE-260	Password in Configuration File	SECURITY.UEC.UTAX
CWE-261	Weak Cryptography for Passwords	SECURITY.WSC.CKTS
CWE-284	Improper Access Control	EJB.DPANY
CWE-291	Reliance on IP Address for Authentication	SECURITY.WSC.DNSL
CWE-306	Missing Authentication for Critical Function	SECURITY.WSC.CAM SECURITY.WSC.PAC SECURITY.WSC.PPF SECURITY.WSC.SSM SECURITY.WSC.UOSC SECURITY.WSC.USC
CWE-309	Use of Password System for Primary Authentication	STRUTS.MLVP
CWE-311	Missing Encryption of Sensitive Data	SECURITY.ESD.CONSEN SECURITY.ESD.PEO SECURITY.UEC.HTTPS SECURITY.WSC.USC
CWE-312	Cleartext Storage of Sensitive Information	SECURITY.UEC.PWDPROP
CWE-313	Cleartext Storage in a File or on Disk	PROPS.PLAIN
CWE-315	Cleartext Storage of Sensitive Information in a Cookie	SECURITY.ESD.PLC

CWE-319	Cleartext Transmission of Sensitive Information	BD.SECURITY.TDSQL PORT.HCNA
CWE-321	Use of Hard-coded Cryptographic Key	SECURITY.WSC.HCCK
CWE-326	Inadequate Encryption Strength	SECURITY.WSC.ICA
CWE-327	Use of a Broken or Risky Cryptographic Algorithm	SECURITY.WSC.ICA SECURITY.WSC.SRD
CWE-328	Reversible One-Way Hash	SECURITY.WSC.ICA
CWE-329	Not Using a Random IV with CBC Mode	SECURITY.WSC.ENPP SECURITY.WSC.IVR
CWE-330	Use of Insufficiently Random Values	SECURITY.WSC.SRD
CWE-336	Same Seed in PRNG	SECURITY.WSC.ENPP
CWE-337	Predictable Seed in PRNG	SECURITY.WSC.ENPP
CWE-338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	SECURITY.WSC.SRD
CWE-345	Insufficient Verification of Data Authenticity	BD.SECURITY.TDENV
CWE-347	Improper Verification of Cryptographic Signature	SECURITY.WSC.VJFS
CWE-348	Use of Less Trusted Source	BD.SECURITY.CUSTOM
CWE-350	Reliance on Reverse DNS Resolution for a Security-Critical Action	SECURITY.WSC.DNSL
CWE-352	Cross-Site Request Forgery (CSRF)	BD.SECURITY.TDRESP SECURITY.ESD.UPCT BD.SECURITY.VPPD SECURITY.WSC.PAC SECURITY.WSC.PACC SECURITY.WSC.PPF SECURITY.WSC.UOSC
CWE-359	Exposure of Private Information ('Privacy Violation')	SECURITY.ESD.CONSEN
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	PB.CUB.TOCTOU TRS.DCL
CWE-366	Race Condition within a Thread	BD.TRS.TSHL
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition	PB.CUB.TOCTOU
CWE-369	Divide By Zero	BD.PB.ZERO
CWE-375	Returning a Mutable Object to an Untrusted Caller	SECURITY.ESD.RA

CWE-376	Temporary File Issues		
CWE-377	Insecure Temporary File	SECURITY.IBA.ATF	
CWE-382	J2EE Bad Practices: Use of System.exit()	CODSTA.BP.EXIT SECURITY.EAB.JVM	
CWE-383	J2EE Bad Practices: Direct Use of Threads	SECURITY.DRC.THR	
CWE-384	Session Fixation	SECURITY.WSC.ISL	
CWE-390	Detection of Error Condition Without Action	SECURITY.UEHL.LGE	
CWE-391	Unchecked Error Condition	PB.TYPO.AECB	
CWE-395	Use of NullPointerException Catch to Detect NULL Pointer Dereference	EXCEPT.NCNPE	
CWE-396	Declaration of Catch for Generic Exception	CODSTA.EPC.NCE	
CWE-397	Declaration of Throws for Generic Exception	CODSTA.BP.NTX EXCEPT.NTERR	
CWE-398	Indicator of Poor Code Quality	CODSTA.BP.BLOCK PB.USC.AES	PB.USC.SAFL
CWE-401	Improper Release of Memory Before Removing Last Reference ('Memory Leak')	SERVLET.LML	
CWE-404	Improper Resource Shutdown or Release	BD.RES.LEAKS PB.CLOSE JDBC.COCO OPT.CRWD HIBERNATE.CHS JDBC.ODBIL JDBC.RRWD HIBERNATE.CSF JDBC.CDBC OPT.CCR OPT.CIO	
CWE-413	Improper Resource Locking	TRS.LORD	
CWE-416	Use After Free	BDS.RES.FREE	
CWE-431	Missing Handler	SERVLET.CETS	
CWE-434	Unrestricted Upload of File with Dangerous Type	BD.SECURITY.TDFNAMES	
CWE-457	Use of Uninitialized Variable	BD.PB.NOTINITCTOR INIT.UIRC	
CWE-459	Incomplete Cleanup.	BD.RES.LEAKS	
CWE-470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	BD.SECURITY.TDRFL SECURITY.WSC.APIBS	

CWE-476	NULL Pointer Dereference	BD.EXCEPT.NP BD.PB.DEREF
CWE-477	Use of Obsolete Functions	PB.API.DPRAPI
CWE-478	Missing Default Case in Switch Statement	PB.PDS
CWE-481	Assigning instead of Comparing	PB.TYPO.ASI
CWE-483	Incorrect Block Delimitation	CODSTA.BP.BLK PB.CUB.EBI PB.TYPO.EB
CWE-484	Omitted Break Statement in Switch	PB.CUB.SBC PB.TYPO.DAV
CWE-486	Comparison of Classes by Name	SECURITY.EAB.CMP
CWE-487	Reliance on Package-level Scope	OOP.AF
CWE-491	Public cloneable() Method Without Final ('Object Hijack')	SECURITY.WSC.CLONE
CWE-494	Download of Code Without Integrity Check	SECURITY.WSC.USC
CWE-495	Private Array-Typed Field Returned From A Public Method.	SECURITY.ESD.RA
CWE-496	Public Data Assigned to Private Array-Typed Field	SECURITY.WSC.CAP
CWE-497	Exposure of System Data to an Unauthorized Control Sphere	BD.SECURITY.SENS SECURITY.ESD.ACW SECURITY.ESD.PEO
CWE-499	Serializable Class Containing Sensitive Data	SECURITY.ESD.SIF SECURITY.WSC.SER
CWE-500	Public Static Field Not Marked Final	SECURITY.EAB.SPFF SECURITY.WSC.FIMU
CWE-502	Deserialization of Untrusted Data	SERIAL.RWAF BD.SECURITY.SSSD PB.API.MASP SECURITY.WSC.DSER
CWE-506	Embedded Malicious Code	SECURITY.WSC.HCCK
CWE-511	Logic/Time Bomb	SECURITY.WSC.RDM PORT.EXEC
CWE-522	Insufficiently Protected Credentials	SECURITY.UEC.PTPT
CWE-523	Unprotected Transport of Credentials	SECURITY.WSC.USC
CWE-533	Information Exposure Through Server Log Files	SECURITY.ESD.CONSEN
CWE-534	Information Exposure Through Debug Log Files	SECURITY.ESD.CONSEN

CWE-543	Use of Singleton Pattern Without Synchronization in a Multithreaded Context	TRS.IASFTRS.ILI
CWE-545	Use of Dynamic Class Loading	SECURITY.WSC.APIBS
CWE-546	Suspicious Comment	CODSTA.ORG.TODO
CWE-547	Use of Hard-coded, Security-relevant Constants	SECURITY.WSC.HCCS
CWE-555	J2EE Misconfiguration: Plaintext Password in Configuration File	HIBERNATE.UPWD SECURITY.UEC.PWDXML
CWE-561	Dead Code	BD.PB.CC BD.PB.DEREF BD.PB.SWITCH UC.PM
CWE-563	Assignment to Variable without Use ('Unused Variable')	GLOBAL.UPPF UC.AURV UC.PF BD.PB.VOVR UC.UP UC.DEAD UC.UCIF UC.PM
CWE-566	Authorization Bypass Through User-Controlled SQL Primary Key	SECURITY.IBA.AUSS
CWE-568	finalize() Method Without super.finalize().	GC.FCF
CWE-570	Expression is Always False	BD.PB.CC UC.UCIF
CWE-571	Expression is Always True	BD.PB.CC UC.UCIF
CWE-572	Call to Thread run() instead of start()	TRS.IRUN
CWE-576	EJB Bad Practices: Use of Java I/O	EJB.JIO
CWE-577	EJB Bad Practices: Use of Sockets	EJB.AUS
CWE-578	EJB Bad Practices: Use of Class Loader	EJB.ACL
CWE-579	J2EE Bad Practices: Non-serializable Object Stored in Session	PB.API.ONS SERIAL.SNSO
CWE-580	clone() Method Without super.clone()	CODSTA.EPC.SCLONE
CWE-581	Object Model Violation: Just One of Equals and Hashcode Defined	CODSTA.OIM.OVERRIDE
CWE-582	Array Declared Public, Final, and Static.	PB.CUB.PSFA PB.CUB.IMM

CWE-583	finalize() Method Declared Public	OOP.MFP
CWE-584	Return Inside Finally Block.	PB.CUB.ARCF
CWE-585	Empty Synchronized Block	UC.SNE
CWE-586	Explicit Call to Finalize()	GC.NCF
CWE-594	J2EE Framework: Saving Unserializable Objects to Disk	EJB.EJB3.SIVS
CWE-595	Comparison of Object References Instead of Object Contents.	PB.CUB.UEIC
CWE-597	Use of Wrong Operator in String Comparison	PB.CUB.UEIC
CWE-598	Information Exposure Through Query Strings in GET Request	SECURITY.ESD.UPCT
CWE-600	Uncaught Exception in Servlet	SERVLET.CETS
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')	BD.SECURITY.TDNET BD.SECURITY.TDRESP SECURITY.IBA.VRD SERVLET.UCO
CWE-605	Multiple Binds to the Same Port	PORT.HCNA
CWE-607	Public Static Final Field References Mutable Object	PB.CUB.RMO PB.CUB.IMM
CWE-609	Double-Checked Locking	TRS.DCL
CWE-613	Insufficient Session Expiration	SECURITY.UEC.STTL
CWE-614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	SECURITY.WSC.UOSC
CWE-643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')	BD.SECURITY.TDXPATH BD.SECURITY.TDJXPATH
CWE-644	Improper Neutralization of HTTP Headers for Scripting Syntax	BD.SECURITY.TDRESP
CWE-647	Use of Non-Canonical URL Paths for Authorization Decisions	SECURITY.IBA.CDBV
CWE-652	Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')	BD.SECURITY.TDXPATH BD.SECURITY.TDXML SECURITY.IBA.XPIJ
CWE-653	Insufficient Compartmentalization	
CWE-662	Improper Synchronization	PB.CUB.TOCTOU
CWE-665	Improper Initialization	BD.PB.NOTEXPLINIT
CWE-667	Improper Locking.	PB.CLOSE BD.TRS.LOCK
CWE-674	Uncontrolled Recursion	PB.LOGIC.FLRC BD.TRS.LOCK
CWE-680	Integer Overflow to Buffer Overflow	PB.NUM.BSA

CWE-681	Incorrect Conversion between Numeric Types	PB.NUM.IDCD PB.NUM.CLP
CWE-690	Unchecked Return Value to NULL Pointer Dereference	BD.EXCEPT.NP PB.RE.MCRN PB.EAR
CWE-691	Insufficient Control Flow Management.	CODSTA.READ.ANL PB.USC.AES
CWE-704	Incorrect Type Conversion or Cast	CODSTA.EPC.AGBPT OPT.CPTS PB.NUM.IDCD PB.NUM.CLP
CWE-712	OWASP Top Ten 2007 Category A1 - Cross Site Scripting (XSS)	BD.SECURITY.TDXSS BD.SECURITY.TDRESP SECURITY.IBA.CDBV BD.SECURITY.VPPD
CWE-713	OWASP Top Ten 2007 Category A2 - Injection Flaws	BD.SECURITY.TDCMD
CWE-714	OWASP Top Ten 2007 Category A3 - Malicious File Execution	BD.SECURITY.TDLIB
CWE-715	OWASP Top Ten 2007 Category A4 - Insecure Direct Object Reference	PB.CUB.RMO SECURITY.EAB.MPT SECURITY.ESD.RA EJB.EJB3.PERMIT SECURITY.ESD.UPCT BD.SECURITY.VPPD SECURITY.WSC.PAC SECURITY.WSC.PACC
CWE-716	OWASP Top Ten 2007 Category A5 - Cross Site Request Forgery (CSRF)	BD.SECURITY.TDRESP SECURITY.ESD.UPCT BD.SECURITY.VPPD SECURITY.WSC.PPF SECURITY.WSC.UOSC
CWE-717	OWASP Top Ten 2007 Category A6 - Information Leakage and Improper Error Handling	BD.SECURITY.SENS SECURITY.UEHL.LGE SECURITY.WSC.ACPST
CWE-718	OWASP Top Ten 2007 Category A7 - Broken Authentication and Session Management	SECURITY.BV.DSSM SECURITY.ESD.SIO SECURITY.WSC.SSM SECURITY.UEC.LCA SECURITY.WSC.PPF SECURITY.WSC.UOSC

CWE-724	OWASP Top Ten 2004 Category A3 - Broken Authentication and Session Management	SECURITY.BV.DSSM SECURITY.ESD.SIO SECURITY.WSC.SSM SECURITY.UEC.LCA SECURITY.WSC.PPF SECURITY.WSC.UOSC
CWE-725	OWASP Top Ten 2004 Category A4 - Cross-Site Scripting (XSS) Flaws	BD.SECURITY.TDXSS BD.SECURITY.TDRESP SECURITY.IBA.CDBV BD.SECURITY.VPPD
CWE-727	OWASP Top Ten 2004 Category A6 - Injection Flaws	BD.SECURITY.TDCMD
CWE-732	Incorrect Permission Assignment for Critical Resource	SECURITY.WSC.PACC
CWE-749	Exposed Dangerous Method or Function	GLOBAL.DPPM GLOBAL.DPAM GLOBAL.SPAM
CWE-751	2009 Top 25 - Insecure Interaction Between Components.	SECURITY.IBA.VRD
CWE-764	Multiple Locks of a Critical Resource	BD.TRS.DLOCK
CWE-772	Missing Release of Resource after Effective Lifetime	OPT.CRWD JDBC.RRWD HIBERNATE.CSF JDBC.CDBC HIBERNATE.CHS OPT.CCR OPT.CIO BD.RES.LEAKS PB.CLOSE JDBC.COCO JDBC.ODBIL
CWE-775	Missing Release of File Descriptor or Handle after Effective Lifetime	PB.CLOSE BD.RES.LEAKS
CWE-778	Insufficient logging	SECURITY.BV.ENFL
CWE-780	Use of RSA Algorithm without OAEP	SECURITY.WSC.ICA
CWE-798	Use of Hard-coded Credentials	SECURITY.WSC.HCCS SECURITY.UEC.PCCF HIBERNATE.UPWD SECURITY.UEC.PTPT SECURITY.UEC.PWDXML SECURITY.UEC.WPWD SECURITY.UEC.UTAX SECURITY.UEC.WCPWD

CWE-807	Reliance on Untrusted Inputs in a Security Decision	SECURITY.ESD.PLC SECURITY.WSC.UOSC
CWE-832	Unlock of a Resource that is not Locked	BD.TRS.LOCK TRS.LORD TRS.RLF
CWE-833	Deadlock.	TRS.STR BD.TRS.TSHL TRS.CSFS TRS.RLF BD.TRS.LOCK TRS.THSL TRS.UWNA
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')	PB.LOGIC.AIL CODSTA.READ.PCIF
CWE-836	Use of Password Hash Instead of Password for Authentication	PROPS.PLAIN
CWE-845	CERT Java Secure Coding Section 00 - Input Validation and Data Sanitization (IDS)	BD.SECURITY.TDSQL BD.SECURITY.TDLOG PB.API.VAFS PORT.EXEC BD.SECURITY.SENS BD.SECURITY.TDXML
CWE-846	CERT Java Secure Coding Section 01 - Declarations and Initialization (DCL)	GLOBAL.ACD BD.CO.ITMOD
CWE-847	CERT Java Secure Coding Section 02 - Expressions (EXP)	PB.USC.NASSIG BD.EXCEPT.NP PB.CUB.UEIC
CWE-848	CERT Java Secure Coding Section 03 - Numeric Types and Operations (NUM)	PB.NUM.{ICO,BSA,CACO} BD.PB.ZERO PB.NUM.UBD PB.NUM.NAN PB.NUM.FPLIPB.NUM.BBDCC PB.NUM.CLP PB.NUM.AIC
CWE-849	CERT Java Secure Coding Section 04 - Object Orientation (OBJ)	GLOBAL.DPPF CODSTA.EPC.AGBPT CODSTA.POD.UPT SECURITY.WSC.CLONE SECURITY.EAB.CPCL SECURITY.EAB.MPT SECURITY.EAB.SMO OOP.MUCOP SECURITY.ESD.RA SECURITY.WSC.MCNC SECURITY.WSC.INNER SECURITY.EAB.CMP SECURITY.EAB.SPFF EXCEPT.EPNFC PB.CUB.PSFA

CWE-850	CERT Java Secure Coding Section 05 - Methods (MET)	PB.API.DPRAPI TRS.THRD OOP.OPM PB.CUB.CTOR SECURITY.WSC.CFM OOP.AHSM CODSTA.OIM.OVERRIDE MOBILE.AUI EJB.MNDF GC.FCF GC.FM GC.IFF GC.NCF PB.API.OF UC.EF UC.FCSF
CWE-851	CERT Java Secure Coding Section 06 - Exceptional Behavior (ERR)	SECURITY.UEHL.LGE UC.UCATCH SECURITY.WSC.ACPST SERVLET.CETS SECURITY.ESD.ACW PB.CUB.ARCF PB.CUB.ATSF CODSTA.BP.NTX EXCEPT.NTERR EXCEPT.NCNPE CODSTA.BP.EXIT SECURITY.EAB.JVM
CWE-852	CERT Java Secure Coding Section 07 - Visibility and Atomicity (VNA)	TRS.LORD TRS.MRAV TRS.SSUG
CWE-853	CERT Java Secure Coding Section 08 - Locking (LCK)	TRS.SOPF, TRS.SCS, TRS.SOL, TRS.IASF, TRS.LORD, TRS.RLF, BD.TRS.LOCK, TRS.TSHL, BD.TRS.TSHL, TRS.DCL
CWE-854	CERT Java Secure Coding Section 09 - Thread APIs (THI)	TRS.IRUN, TRS.AUTG, TRS.ANF, TRS.UWIL, TRS.THRD
CWE-856	CERT Java Secure Coding Section 11 - Thread-Safety Miscellaneous (TSM)	TRS.CTRE, TRS.CSTART, SECURITY.WSC.FIMU
CWE-857	CERT Java Secure Coding Section 12 - Input Output (FIO)	SECURITY.IBA.ATF BD.RES.LEAKS OPT.CIO OPT.CCR PORT.EXEC PB.LOGIC.CRRV BD.SECURITY.SENS HIBERNATE.LHII SECURITY.ESD.PEO SECURITY.ESD.CONSEN OPT.CRWD
CWE-858	CERT Java Secure Coding Section 13 - Serialization (SER)	SERIAL.DUID SERIAL.ROWO SECURITY.ESD.SIF SECURITY.WSC.SCSER SERIAL.RRSC SERIAL.IRX
CWE-859	CERT Java Secure Coding Section 14 - Platform Security (SEC)	SECURITY.BV.ACL CODSTA.BP.ARM BD.SECURITY.TDRFL SECURITY.WSC.SCF SECURITY.WSC.VJFS
CWE-860	CERT Java Secure Coding Section 15 - Runtime Environment (ENV)	PORT.ENV

CWE-861	CERT Java Secure Coding Section 49 - Miscellaneous (MSC)	SECURITY.WSC.USC PB.TYPO.EB SECURITY.WSC.SRD SECURITY.WSC.HCCS SECURITY.WSC.HCCK SECURITY.WSC.AHCA BD.RES.LEAKS TRS.RLF BD.CO.ITMOD TRS.ILI
CWE-862	Missing Authorization	EJB.EJB3.PERMIT SECURITY.UEC.LCA
CWE-863	Incorrect Authorization	SECURITY.UEC.DSR SECURITY.UEC.SRCD