RESORT Coverage for CWE: Java

RESORT Code Analysis Version 2016 and CWE 2.9

CWE ID	RESORT Code Checker
15	External Control of System or Configuration Setting
22	Path Traversal
23	Relative Path Traversal
36	Absolute Path Traversal
78	OS Command Injection
79	Cross-site Scripting
80	Basic XSS
81	Improper Neutralization of Script in an Error Message Web Page
83	Improper Neutralization of Script in Attributes in a Web Page
89	SQL Injection
90	LDAP Injection
91	XML Injection
95	Eval Injection
99	Resource Injection
111	Direct Use of Unsafe JNI
113	HTTP Response Splitting
114	Process Control
129	Improper Validation of Array Index
134	Uncontrolled Format String
190	Integer Overflow or Wraparound
191	Integer Underflow (Wrap or Wraparound)
193	Off-by-one Error
197	Numeric Truncation Error
209	Information Exposure Through an Error Message
226	Sensitive Information Uncleared Before Release
247	DEPRECATED (Duplicate): Reliance on DNS Lookups in a Security Decision
248	Uncaught Exception
252	Unchecked Return Value
253	Incorrect Check of Function Return Value
256	Plaintext Storage of a Password
259	Use of Hard-coded Password
315	Cleartext Storage of Sensitive Information in a Cookie
319	Cleartext Transmission of Sensitive Information
321	Use of Hard-coded Cryptographic Key
325	Missing Required Cryptographic Step
327	Use of a Broken or Risky Cryptographic Algorithm
328	Reversible One-Way Hash
329	Not Using a Random IV with CBC Mode
336	Same Seed in PRNG

338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
362	Race Condition
367	Time-of-check Time-of-use (TOCTOU) Race Condition
369	Divide By Zero
378	Creation of Temporary File With Insecure Permissions
379	Creation of Temporary File in Directory with Incorrect Permissions
382	J2EE Bad Practices: Use of System.exit()
383	J2EE Bad Practices: Direct Use of Threads
390	Detection of Error Condition Without Action
395	Use of NullPointerException Catch to Detect NULL Pointer Dereference
396	Declaration of Catch for Generic Exception
397	Declaration of Throws for Generic Exception
398	Indicator of Poor Code Quality
400	Resource Exhaustion
404	Improper Resource Shutdown or Release
459	Incomplete Cleanup
470	Unsafe Reflection
476	NULL Pointer Dereference
477	Use of Obsolete Functions
478	Missing Default Case in Switch Statement
481	Assigning instead of Comparing
482	Comparing instead of Assigning
483	Incorrect Block Delimitation
484	Omitted Break Statement in Switch
486	Comparison of Classes by Name
491	Object Hijack
492	Use of Inner Class Containing Sensitive Data
493	Critical Public Variable Without Final Modifier
499	Serializable Class Containing Sensitive Data
500	Public Static Field Not Marked Final
506	Embedded Malicious Code
510	Trapdoor
511	Logic/Time Bomb
523	Unprotected Transport of Credentials
526	Information Exposure Through Environmental Variables
533	Information Exposure Through Server Log Files
534	Information Exposure Through Debug Log Files
535	Information Exposure Through Shell Error Message
539	Information Exposure Through Persistent Cookies
546	Suspicious Comment
549	Missing Password Field Masking
561	Dead Code
566	Authorization Bypass Through User-Controlled SQL Primary Key

568	finalize() Method Without super.finalize()
570	Expression is Always False
571	Expression is Always True
572	Call to Thread run() instead of start()
579	J2EE Bad Practices: Non-serializable Object Stored in Session
580	clone() Method Without super.clone()
581	Object Model Violation: Just One of Equals and Hashcode Defined
582	Array Declared Public, Final, and Static
584	Return Inside Finally Block
585	Empty Synchronized Block
586	Explicit Call to Finalize()
597	Use of Wrong Operator in String Comparison
598	Information Exposure Through Query Strings in GET Request
600	Uncaught Exception in Servlet
601	Open Redirect
605	Multiple Binds to the Same Port
606	Unchecked Input for Loop Condition
607	Public Static Final Field References Mutable Object
609	Double-Checked Locking
613	Insufficient Session Expiration
614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
615	Information Exposure Through Comments
617	Reachable Assertion
643	XPath Injection
667	Improper Locking
674	Uncontrolled Recursion
681	Incorrect Conversion between Numeric Types
698	Execution After Redirect (EAR)
759	Use of a One-Way Hash without a Salt
760	Use of a One-Way Hash with a Predictable Salt
764	Multiple Locks of a Critical Resource
765	Multiple Unlocks of a Critical Resource
772	Missing Release of Resource after Effective Lifetime
775	Missing Release of File Descriptor or Handle after Effective Lifetime
789	Uncontrolled Memory Allocation
832	Unlock of a Resource that is not Locked
835	Infinite Loop

Soft4Soft Co., Ltd.

501 ETRI CTC Center, 218, Gajeong-ro, Yuseong-gu, Daejeon, 305-700, KOREA

TEL. +82-2-553-9464, www.soft4soft.com, Email: info@soft4soft.com