

Category	CWE Entries
00 IDS	CWE-015: External Control of System or Configuration Setting
00 IDS	CWE-023: Relative Path Traversal
00 IDS	CWE-036: Absolute Path Traversal
00 IDS	CWE-078: OS Command Injection
00 IDS	CWE-080: Basic XSS
00 IDS	CWE-081: Improper Neutralization of Script in an Error Message Web Page
00 IDS	CWE-083: Improper Neutralization of Script in Attributes in a Web Page
00 IDS	CWE-089: SQL Injection
00 IDS	CWE-090: LDAP Injection
16 JNI	CWE-111: Direct Use of Unsafe JNI
00 IDS	CWE-113: HTTP Response Splitting
49 MSC	CWE-114: Process Control
03 NUM	CWE-129: Improper Validation of Array Index
03 NUM	CWE-129: Improper Validation of Array Index(external input)
00 IDS	CWE-134: Uncontrolled Format String
03 NUM	CWE-190: Integer Overflow or Wraparound
03 NUM	CWE-190: Integer Overflow or Wraparound(external input)
03 NUM	CWE-191: Integer Underflow (Wrap or Wraparound)
03 NUM	CWE-191: Integer Underflow (Wrap or Wraparound)(external input)
02 EXP	CWE-193: Off-by-one Error
03 NUM	CWE-197: Numeric Truncation Error
06 ERR	CWE-209: Information Exposure Through an Error Message
49 MSC	CWE-226: Sensitive Information Uncleared Before Release
06 ERR	CWE-248: Uncaught Exception
12 FIO	CWE-252: Unchecked Return Value
12 FIO	CWE-253: Incorrect Check of Function Return Value
00 IDS	CWE-256: Plaintext Storage of a Password
00 IDS	CWE-259: Use of Hard-coded Password
00 IDS	CWE-315: Cleartext Storage of Sensitive Information in a Cookie
00 IDS	CWE-319: Cleartext Transmission of Sensitive Information
00 IDS	CWE-319: Cleartext Transmission of Sensitive Information
00 IDS	CWE-321: Use of Hard-coded Cryptographic Key
49 MSC	CWE-325: Missing Required Cryptographic Step
49 MSC	CWE-327: Use of a Broken or Risky Cryptographic Algorithm
49 MSC	CWE-328: Reversible One-Way Hash
49 MSC	CWE-329: Not Using a Random IV with CBC Mode
49 MSC	CWE-336: Same Seed in PRNG
49 MSC	CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
03 NUM	CWE-369: Divide By Zero
03 NUM	CWE-369: Divide By Zero(external input)
12 FIO	CWE-378: Creation of Temporary File With Insecure Permissions
12 FIO	CWE-379: Creation of Temporary File in Directory with Incorrect Permissions
49 MSC	CWE-382: J2EE Bad Practices: Use of System.exit()
09 THI	CWE-383: J2EE Bad Practices: Direct Use of Threads
06 ERR	CWE-390: Detection of Error Condition Without Action
06 ERR	CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference

06 ERR	CWE-396: Declaration of Catch for Generic Exception
06 ERR	CWE-397: Declaration of Throws for Generic Exception
49 MSC	CWE-398: Indicator of Poor Code Quality
03 NUM	CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')
49 MSC	CWE-404: Improper Resource Shutdown or Release
49 MSC	CWE-459: Incomplete Cleanup
00 IDS	CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')
02 EXP	CWE-476: NULL Pointer Dereference
05 MET	CWE-477: Use of Obsolete Functions
49 MSC	CWE-478: Missing Default Case in Switch Statement
02 EXP	CWE-481: Assigning instead of Comparing
02 EXP	CWE-482: Comparing instead of Assigning
49 MSC	CWE-483: Incorrect Block Delimitation
49 MSC	CWE-484: Omitted Break Statement in Switch
04 OBJ	CWE-486: Comparison of Classes by Name
05 MET	CWE-491: Public cloneable() Method Without Final ('Object Hijack')
13 SER	CWE-499: Serializable Class Containing Sensitive Data
04 OBJ	CWE-500: Public Static Field Not Marked Final
00 IDS	CWE-506: Embedded Malicious Code
49 MSC	CWE-510: Trapdoor
49 MSC	CWE-511: Logic/Time Bomb
49 MSC	CWE-523: Unprotected Transport of Credentials
15 ENV	CWE-526: Information Exposure Through Environmental Variables
49 MSC	CWE-533: Information Exposure Through Server Log Files
49 MSC	CWE-534: Information Exposure Through Debug Log Files
49 MSC	CWE-535: Information Exposure Through Shell Error Message
49 MSC	CWE-539: Information Exposure Through Persistent Cookies
49 MSC	CWE-546: Suspicious Comment
49 MSC	CWE-549: Missing Password Field Masking
49 MSC	CWE-561: Dead Code
00 IDS	CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key
05 MET	CWE-568: finalize() Method Without super.finalize()
02 EXP	CWE-570: Expression is Always False
02 EXP	CWE-571: Expression is Always True
09 THI	CWE-572: Call to Thread run() instead of start()
13 SER	CWE-579: J2EE Bad Practices: Non-serializable Object Stored in Session
05 MET	CWE-580: clone() Method Without super.clone()
05 MET	CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined
01 DCL	CWE-582: Array Declared Public, Final, and Static
06 ERR	CWE-584: Return Inside Finally Block
08 LCK	CWE-585: Empty Synchronized Block
05 MET	CWE-586: Explicit Call to Finalize()
02 EXP	CWE-597: Use of Wrong Operator in String Comparison
49 MSC	CWE-598: Information Exposure Through Query Strings in GET Request
06 ERR	CWE-600: Uncaught Exception in Servlet
00 IDS	CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
49 MSC	CWE-605: Multiple Binds to the Same Port
00 IDS	CWE-606: Unchecked Input for Loop Condition
04 OBJ	CWE-607: Public Static Final Field References Mutable Object

08 LCK	CWE-609: Double-Checked Locking
49 MSC	CWE-613: Insufficient Session Expiration
49 MSC	CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
49 MSC	CWE-615: Information Exposure Through Comments
05 MET	CWE-617: Reachable Assertion
00 IDS	CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection')
08 LCK	CWE-667: Improper Locking
49 MSC	CWE-674: Uncontrolled Recursion
03 NUM	CWE-681: Incorrect Conversion between Numeric Types
49 MSC	CWE-698: Execution After Redirect (EAR)
49 MSC	CWE-759: Use of a One-Way Hash without a Salt
49 MSC	CWE-760: Use of a One-Way Hash with a Predictable Salt
08 LCK	CWE-764: Multiple Locks of a Critical Resource
08 LCK	CWE-765: Multiple Unlocks of a Critical Resource
49 MSC	CWE-772: Missing Release of Resource after Effective Lifetime(DB)
49 MSC	CWE-772: Missing Release of Resource after Effective Lifetime(I/O)
49 MSC	CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime
00 IDS	CWE-789: Uncontrolled Memory Allocation
08 LCK	CWE-832: Unlock of a Resource that is not Locked
49 MSC	CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')