

The title of the document, "Coverity Coverage for Common Weakness Enumeration (CWE)", displayed in white text on a purple background. The background image shows a person in a yellow jacket steering a boat on blue water.

Table of contents

Android Security.....	2
C#	3
C/C++ & Objective-C	6
Java.....	11
JavaScript.....	22
Node.js.....	24
PHP	25
Python.....	27
Ruby	28
Scala	30
Swift	31
VB.NET.....	32

Android Security

Coverity Coverage for CWE: Android Security		
Coverity Software Testing Platform version 2018.12		
CWE	Name	Coverity checker
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	• PATH_MANIPULATION
78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	• OS_CMD_INJECTION
79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	• XSS
89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	• SQLI
94	Improper Control of Generation of Code ('Code Injection')	• SQLIREGEX_INJECTION
99	Improper Control of Resource Identifiers ('Resource Injection')	• URL_MANIPULATION
209	Information Exposure Through an Error Message	• SENSITIVE_DATA_LEAK
215	Information Exposure Through Debug Information	• ANDROID_DEBUG_MODE
259	Use of Hard-coded Password	• HARDCODED_CREDENTIALS
296	Improper Following of a Certificate's Chain of Trust	• BAD_CERT_VERIFICATION
297	Improper Validation of Certificate with Host Mismatch	• BAD_CERT_VERIFICATION
299	Improper Check for Certificate Revocation	• BAD_CERT_VERIFICATION
311	Missing Encryption of Sensitive Data	• SENSITIVE_DATA_LEAK
312	Cleartext Storage of Sensitive Information	• SENSITIVE_DATA_LEAK
313	Cleartext Storage in a File or on Disk	• SENSITIVE_DATA_LEAK
317	Cleartext Storage of Sensitive Information in GUI	• SENSITIVE_DATA_LEAK
319	Cleartext Transmission of Sensitive Information	• SENSITIVE_DATA_LEAK
321	Use of Hard-coded Cryptographic Key	• HARDCODED_CREDENTIALS
327	Use of a Broken or Risky Cryptographic Algorithm	• RISKY_CRYPTO
328	Reversible One-Way Hash	• RISKY_CRYPTO
330	Use of Insufficiently Random Values	• MOBILE_ID_MISUSE
336	Same Seed in PRNG	• PREDICTABLE_RANDOM_SEED
337	Predictable Seed in PRNG	• PREDICTABLE_RANDOM_SEED
470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	• UNSAFE_REFLECTION
502	Deserialization of Untrusted Data	• UNSAFE_DESERIALIZATION
532	Information Exposure Through Log Files	• SENSITIVE_DATA_LEAK
538	File and Directory Information Exposure	• UNRESTRICTED_ACCESS_TO_FILE • EXPOSED_PREFERENCES
611	Improper Restriction of XML External Entity Reference ('XXE')	• XML_EXTERNAL_ENTITY
759	Use of a One-Way Hash without a Salt	• WEAK_PASSWORD_HASH
760	Use of a One-Way Hash with a Predictable Salt	• WEAK_PASSWORD_HASH
776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	• XML_EXTERNAL_ENTITY

Coverity Coverage for CWE: Android Security
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
798	Use of Hard-coded Credentials	• HARDCODED_CREDENTIALS
827	Improper Control of Document Type Definition	• XML_EXTERNAL_ENTITY
916	Use of Password Hash With Insufficient Computational Effort	• WEAK_PASSWORD_HASH
921	Storage of Sensitive Data in a Mechanism without Access Control	• UNRESTRICTED_ACCESS_TO_FILE
926	Improper Export of Android Application Components	• MISSING_PERMISSION_ON_EXPORTED_COMPONENT
927	Use of Implicit Intent for Sensitive Communication	• IMPLICIT_INTENT • SENSITIVE_DATA_LEAK • MISSING_PERMISSION_FOR_BROADCAST

C#

Coverity Coverage for CWE: C#
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
10	ASP.NET Environment Issues	• CONFIG.ASP_VIEWSTATE_MAC
11	Security Misconfiguration	• CONFIG.ENABLED_DEBUG_MODE • CONFIG.ENABLED_TRACE_MODE
12	Missing Custom Error Page	• CONFIG.MISSING_CUSTOM_ERROR_PAGE
13	Unencrypted Connection String Password	• CONFIG.CONNECTION_STRING_PASSWORD
20	Improper Input Validation	• OS_CMD_INJECTION • PATH_MANIPULATION • XSS
21	Pathname Traversal and Equivalence Errors	• PATH_MANIPULATION
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	• PATH_MANIPULATION
23	Relative Path Traversal	• PATH_MANIPULATION
36	Absolute Path Traversal	• PATH_MANIPULATION
73	External Control of File Name or Path	• UNRESTRICTED_DISPATCH
77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	• OS_CMD_INJECTION
78	Improper Neutralization of Special Elements used in an OS Command ('OSCommand Injection')	• OS_CMD_INJECTION
79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	• XSS

Coverity Coverage for CWE: C#
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	• XSS
82	Improper Neutralization of Script in Attributes of IMG Tags in a Web Page	• XSS
83	Improper Neutralization of Script in Attributes in a Web Page	• XSS
85	Doubled Character XSS Manipulations	• XSS
86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages	• XSS
87	Improper Neutralization of Alternate XSS Syntax	• XSS
88	Argument Injection or Modification	• OS_CMD_INJECTION
89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	• SQL_NOT_CONSTANT • SQLI
90	Improper Neutralization of Special Elements used in an LDAP Query	• LDAP_INJECTION
91	XML Injection (aka Blind XPath Injection)	• XML_INJECTION
94	Improper Control of Generation of Code ('Code Injection')	• NOSQL_QUERY_INJECTION • REGEX_INJECTION • SCRIPT_CODE_INJECTION • UNKNOWN_LANGUAGE_INJECTION • XPATH_INJECTION
117	Improper Output Neutralization for Logs	• LOG_INJECTION
171	Cleansing, Canonicalization, and Comparison Errors	• BAD_EQ
190	Integer Overflow or Wraparound	• OVERFLOW_BEFORE_WIDEN
200	Information Exposure	• ASPNET_MVC_VERSION_HEADER • CONFIG.ASPNET_VERSION_HEADER • CONFIG.COOKIE_MISSING_HTTPONLY
209	Information Exposure Through an Error Message	• SENSITIVE_DATA_LEAK
259	Use of Hard-coded Password	• HARDCODED_CREDENTIALS
285	Missing Authorization Check	• MISSING_AUTHZ
313	Cleartext Storage in a File or on Disk	• UNENCRYPTED_SENSITIVE_DATA • SENSITIVE_DATA_LEAK
315	Cleartext Storage of Sensitive Information in a Cookie	• UNENCRYPTED_SENSITIVE_DATA
319	Cleartext Transmission of Sensitive Information	• UNENCRYPTED_SENSITIVE_DATA • SENSITIVE_DATA_LEAK
321	Use of Hard-coded Cryptographic Key	• HARDCODED_CREDENTIALS
327	Use of a Broken or Risky Cryptographic Algorithm	• RISKY_CRYPTO
328	Reversible One-Way Hash	• RISKY_CRYPTO
330	Use of Insufficiently Random Values	• INSECURE_RANDOM
352	Cross-Site Request Forgery (CSRF)	• CSRF
366	Race Condition within a Thread	• GUARDED_BY_VIOLATION • NON_STATIC_GUARDING_STATIC • VOLATILE_ATOMIcity

Coverity Coverage for CWE: C#
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
369	Divide By Zero	• DIVIDE_BY_ZERO
390	Detection of Error Condition Without Action	• MISSING_THROW
398	Indicator of Poor Code Quality	• UNEXPECTED_CONTROL_FLOW • COPY_PASTE_ERROR • IDENTICAL_BRANCHES • PROPERTY_MIXUP
403	Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak')	• RESOURCE_LEAK
404	Improper Resource Shutdown or Release	• RESOURCE_LEAK
476	NULL Pointer Dereference	• FORWARD_NULL • NULL_RETURNS • REVERSE_INULL
480	Use of Incorrect Operator	• CONSTANT_EXPRESSION_RESULT
502	Deserialization of Untrusted Data	• UNSAFE_DESERIALIZATION
519	Disabled View State MAC generation	• CONFIG.ASP_VIEWSTATE_MAC
532	Information Exposure Through Log Files	• SENSITIVE_DATA_LEAK
543	Use of Singleton Pattern Without Synchronization in a Multithreaded Context	• BAD_LOCK_OBJECT • LOCK_EVASION
561	Dead Code	• DEADCODE • UNREACHABLE
563	Assignment to Variable without Use ('Unused Variable')	• UNUSED_VALUE
569	Expression Issues	• CONSTANT_EXPRESSION_RESULT
570	Expression is Always False	• BAD_EQ_TYPES
573	Improper Following of Specification by Caller	• CALL_SUPER • MISSING_RESTORE
595	Comparison of Object References Instead of Object Contents	• BAD_EQ
601	URL Redirection to Untrusted Site ('Open Redirect')	• OPEN_REDIRECT
609	Double-Checked Locking	• LOCK_EVASION
610	Externally Controlled Reference to a Resource in Another Sphere	• HEADER_INJECTION
611	Improper Restriction of XML External Entity Reference ('XXE')	• XML_EXTERNAL_ENTITY
670	Always-Incorrect Control Flow Implementation	• STRAY_SEMICOLON
683	Function Call With Incorrect Order of Arguments	• SWAPPED_ARGUMENTS
759	Use of a One-Way Hash without a Salt	• WEAK_PASSWORD_HASH
760	Use of a One-Way Hash with a Predictable Salt	• WEAK_PASSWORD_HASH
776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	• XML_EXTERNAL_ENTITY
778	Insufficient Logging	• UNLOGGED_SECURITY_EXCEPTION
783	Operator Precedence Logic Error	• CONSTANT_EXPRESSION_RESULT

Coverity Coverage for CWE: C#
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
798	Use of Hard-coded Credentials	• HARDCODED_CREDENTIALS
827	Improper Control of Document Type Definition	• XML_EXTERNAL_ENTITY
833	Deadlock	• LOCK_INVERSION
835	Loop with Unreachable Exit Condition ('Infinite Loop')	• INFINITE_LOOP
863	Incorrect Authorization	• CONFIG.DEAD_AUTHORIZATION_RULE
916	Use of Password Hash With Insufficient Computational Effort	• WEAK_PASSWORD_HASH

C/C++ & Objective-C

Coverity Coverage for CWE: C/C++ & Objective-C
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
20	Improper Input Validation	• TAINTED_SCALAR • TAINTED_STRING • USER_POINTER
22	Filesystem path, filename, or URI manipulation	• PATH_MANIPULATION
78	OS Command Injection	• OS_CMD_INJECTION
89	SQL injection	• SQLI
119	Improper Restriction of Operations within the Bounds of a Memory Buffer	• ARRAY_VS_SINGLETON • BAD_ALLOC_ARITHMETIC • COM.BSTR.CONV • INCOMPATIBLE_CAST • INTEGER_OVERFLOW • INVALIDATE_ITERATOR • MISMATCHED_ITERATOR • OVERRUN • REVERSE_NEGATIVE
120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	• BUFFER_SIZE • SIZECHECK • STRING_OVERFLOW • STRING_SIZE
125	Out-of-bounds Read	• INTEGER_OVERFLOW • OVERRUN
129	Improper Validation of Array Index	• NEGATIVE_RETURNS • REVERSE_NEGATIVE • TAINTED_SCALAR
131	Incorrect Calculation of Buffer Size	• BAD_ALLOC_STRLLEN • SIZECHECK

Coverity Coverage for CWE: C/C++ & Objective-C
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
134	Uncontrolled Format String	• PARSE_WARNINGS • TAINTED_STRING
170	Improper Null Termination	• BUFFER_SIZE • READLINK • SIZECHECK • STRING_NULL
188	Reliance on Data/Memory Layout	• INCOMPATIBLE_CAST
190	Integer Overflow or Wraparound	• INTEGER_OVERFLOW • OVERFLOW_BEFORE_WIDEN • PARSE_WARNINGS
194	Unexpected Sign Extension	• SIGN_EXTENSION
195	Signed to Unsigned Conversion Error	• MISRA_CAST
197	Numeric Truncation Error	• CHAR_IO • MISRA_CAST • NO_EFFECT
243	Creation of chroot Jail Without Changing Working Directory	• CHROOT
248	Uncaught Exception	• UNCAUGHT_EXCEPT
252	Unchecked Return Value	• CHECKED_RETURN
253	Incorrect Check of Function Return Value	• BAD_COMPARE
259	Use of Hard-coded Password	• HARDCODED_CREDENTIALS
290	Authentication Bypass by Spoofing	• WEAK_GUARD
291	Reliance on IP Address for Authentication	• WEAK_GUARD
293	Using Referer Field for Authentication	• WEAK_GUARD
313	Cleartext Storage in a File or on Disk	• UNENCRYPTED_SENSITIVE_DATA
315	Cleartext Storage of Sensitive Information in a Cookie	• UNENCRYPTED_SENSITIVE_DATA
319	Cleartext Transmission of Sensitive Information	• UNENCRYPTED_SENSITIVE_DATA
321	Use of Hard-coded Cryptographic Key	• HARDCODED_CREDENTIALS
327	Use of a Broken or Risky Cryptographic Algorithm	• RISKY_CRYPTO
328	Reversible One-Way Hash	• RISKY_CRYPTO
350	Reliance on Reverse DNS Resolution for a Security-Critical Action	• WEAK_GUARD
366	Race Condition within a Thread	• MISSING_LOCK
367	Time-of-check Time-of-use (TOCTOU) Race Condition	• TOCTOU
369	Divide By Zero	• DIVIDE_BY_ZERO • PARSE_WARNINGS
377	Insecure Temporary File	• SECURE_TEMP
394	Unexpected Status Code or Return Value	• NEGATIVE_RETURNS • REVERSE_NEGATIVE

Coverity Coverage for CWE: C/C++ & Objective-C
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
398	Indicator of Poor Code Quality	<ul style="list-style-type: none"> • COPY_PASTE_ERROR • ENUM_AS_BOOLEAN • IDENTICAL_BRANCHES • MISMATCHED_ITERATOR • MIXED_ENUMS • NO_EFFECT • PASS_BY_VALUE • VIRTUAL_DTOR
400	Uncontrolled Resource Consumption ('Resource Exhaustion')	<ul style="list-style-type: none"> • STACK_USE
401	Improper Release of Memory Before Removing Last Reference ('Memory Leak')	<ul style="list-style-type: none"> • COM.BSTR.ALLOC • CTOR_DTOR_LEAK • NO_EFFECT • SYMBIAN.CLEANUP_STACK
404	Improper Resource Shutdown or Release	<ul style="list-style-type: none"> • RESOURCE_LEAK
415	Double Free	<ul style="list-style-type: none"> • SYMBIAN.CLEANUP_STACK • USE_AFTER_FREE
416	Use After Free	<ul style="list-style-type: none"> • COM.BAD_FREE • COM.BSTR.ALLOC • WRAPPER_ESCAPE • USE_AFTER_FREE
456	Missing Initialization of a Variable	<ul style="list-style-type: none"> • NO_EFFECT
457	Use of Uninitialized Variable	<ul style="list-style-type: none"> • PARSE_WARNINGS • UNINIT • UNINIT_CTOR
459	Incomplete Cleanup	<ul style="list-style-type: none"> • DELETE_ARRAY • SYMBIAN.CLEANUP_STACK
465	Pointer Issues	<ul style="list-style-type: none"> • NO_EFFECT
467	Use of sizeof() on a Pointer Type	<ul style="list-style-type: none"> • BAD_SIZEOF • SIZEOF_MISMATCH
475	Invalid printf format string	<ul style="list-style-type: none"> • PRINTF_ARGS
476	NULL Pointer Dereference	<ul style="list-style-type: none"> • FORWARD_NULL • NULL_RETURNS • REVERSE_INULL
480	Use of Incorrect Operator	<ul style="list-style-type: none"> • CONSTANT_EXPRESSION_RESULT • NO_EFFECT
481	Assigning instead of Comparing	<ul style="list-style-type: none"> • PARSE_WARNINGS
482	Comparing instead of Assigning	<ul style="list-style-type: none"> • NO_EFFECT
483	Incorrect Block Delimitation	<ul style="list-style-type: none"> • NESTING_INDENT_MISMATCH
484	Omitted Break Statement in Switch	<ul style="list-style-type: none"> • MISSING_BREAK

Coverity Coverage for CWE: C/C++ & Objective-C
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
561	Dead Code	• DEADCODE • UNREACHABLE
562	Return of Stack Variable Address	• PARSE_WARNINGS • RETURN_LOCAL
563	Assignment to Variable without Use ('Unused Variable')	• UNUSED_VALUE
569	Expression Issues	• CONSTANT_EXPRESSION_RESULT • SIZEOF_MISMATCH
570	Expression is Always False	• NO_EFFECT • PARSE_WARNINGS
573	Improper Following of Specification by Caller	• MISSING_RESTORE • OPEN_ARGS • VARARGS
584	Return Inside Finally Block	• PARSE_WARNINGS
590	Free of Memory not on the Heap	• BAD_FREE
597	Use of Wrong Operator in String Comparison	• BAD_COMPARE
606	Unchecked Input for Loop Condition	• NEGATIVE_RETURNS • TAINTED_SCALAR
617	Reachable Assertion	• LOCK
628	Function Call with Incorrectly Specified Arguments	• BAD_COMPARE • PARSE_WARNINGS
633	Weaknesses that Affect Memory	• COM.BSTR.ALLOC
643	XML Path (XPath) Language injection	• XPATH_INJECTION
662	Improper Synchronization	• ATOMICITY
665	Improper Initialization	• NO_EFFECT
667	Improper Locking	• LOCK • SLEEP
670	Always-Incorrect Control Flow Implementation	• STRAY_SEMICOLON
672	Operation on a Resource after Expiration or Release	• USE_AFTER_FREE
676	Use of Potentially Dangerous Function	• DC.STREAM_BUFFER • DC.STRING_BUFFER • DC.WEAK_CRYPT0 • DC.PREDICTABLE_KEY_PASSWORD • SECURE_CODING
681	Incorrect Conversion between Numeric Types	• MISRA_CAST
683	Function Call With Incorrect Order of Arguments	• SWAPPED_ARGUMENTS
685	Function Call With Incorrect Number of Arguments	• PARSE_WARNINGS
685	Extra argument to printf format specifier	• PRINTF_ARGS
686	Function Call With Incorrect Argument Type	• PARSE_WARNINGS

Coverity Coverage for CWE: C/C++ & Objective-C
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
686	Invalid type in argument to printf format specifier	• PRINTF_ARGS
687	Function Call With Incorrectly Specified Argument Value	• NEGATIVE_RETURNS
704	Incorrect Type Conversion or Cast	• INCOMPATIBLE_CAST • PARSE_WARNINGS
710	Coding Standards Violation	• ASSIGN_NOT_RETURNING_STAR_THIS • BAD_OVERRIDE • HFA • MISSING_COPY_OR_ASSIGN • MISSING_RETURN • SELF_ASSIGN
758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior	• DELETE_VOID • EVALUATION_ORDER
759	Use of a One-Way Hash without a Salt	• WEAK_PASSWORD_HASH
760	Use of a One-Way Hash with a Predictable Salt	• WEAK_PASSWORD_HASH
762	Mismatched Memory Management Routines	• ALLOC_FREE_MISMATCH
764	Multiple Locks of a Critical Resource	• LOCK
772	Missing Release of Resource after Effective Lifetime	• VIRTUAL_DTOR
775	Missing Release of File Descriptor or Handle after Effective Lifetime	• RESOURCE_LEAK
783	Operator Precedence Logic Error	• BAD_COMPARE • CONSTANT_EXPRESSION_RESULT • SIZEOF_MISMATCH
798	Use of Hard-coded Credentials	• HARDCODED_CREDENTIALS
833	Deadlock	• ORDER_REVERSAL
835	Loop with Unreachable Exit Condition ('Infinite Loop')	• INFINITE_LOOP
916	Use of Password Hash With Insufficient Computational Effort	• WEAK_PASSWORD_HASH

Java

Coverity Coverage for CWE: Java		
Coverity Software Testing Platform version 2018.12		
CWE	Name	Coverity checker
4	J2EE Environment Issues	• CONFIG
7	J2EE Misconfiguration: Missing Custom Error Page	• CONFIG
11	ASP.NET Misconfiguration: Creating Debug Binary	• CONFIG.ENABLED_DEBUG_MODE, CONFIG.ENABLED_TRACE_MODE
20	Improper Input Validation	• OS_CMD_INJECTION • PATH_MANIPULATION • SQLI • UNRESTRICTED_DISPATCH • UNSAFE_REFLECTION • XSS
21	Pathname Traversal and Equivalence Errors	• PATH_MANIPULATION
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	• JSP_DYNAMIC_INCLUDE • PATH_MANIPULATION
23	Relative Path Traversal	• FB.PT_RELATIVE_PATH_TRAVERSAL • PATH_MANIPULATION
36	Absolute Path Traversal	• FB.PT_ABSOLUTE_PATH_TRAVERSAL • PATH_MANIPULATION
73	External Control of File Name or Path	• UNRESTRICTED_DISPATCH
77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	• OS_CMD_INJECTION
78	Improper Neutralization of Special Elements used in an OS Command ('OSCommand Injection')	• OS_CMD_INJECTION, TAINTED_ENVIRONMENT_WITH_EXECUTION
79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	• FB.XSS_REQUEST_PARAMETER_TO_JSP_WRITER • FB.XSS_REQUEST_PARAMETER_TO_SERVLET_WRITER • XSS
80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	• XSS
81	Improper Neutralization of Script in an Error Message Web Page	• FB.XSS_REQUEST_PARAMETER_TO_SEND_ERROR
82	Improper Neutralization of Script in Attributes of IMG Tags in a Web Page	• XSS
83	Improper Neutralization of Script in Attributes in a Web Page	• XSS
85	Doubled Character XSS Manipulations	• XSS
86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages	• XSS
87	Improper Neutralization of Alternate XSS Syntax	• XSS
88	Argument Injection or Modification	• OS_CMD_INJECTION

Coverity Coverage for CWE: Java
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	<ul style="list-style-type: none"> • FB.SQL_NONCONSTANT_STRING_PASSED_TO_EXECUTE • FB.SQL_PREPARED_STATEMENT_GENERATED_FROM_NONCONSTANT_STRING • JSP_SQL_INJECTION • SQLI • SQL_NOT_CONSTANT
90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	<ul style="list-style-type: none"> • LDAP_INJECTION
91	XML Injection (aka Blind XPath Injection)	<ul style="list-style-type: none"> • XML_INJECTION
94	Improper Control of Generation of Code ('Code Injection')	<ul style="list-style-type: none"> • JAVA_CODE_INJECTION • JCR_INJECTION • NOSQL_QUERY_INJECTION • OGNL_INJECTION • REGEX_INJECTION • SCRIPT_CODE_INJECTION • UNKNOWN_LANGUAGE_INJECTION • XPATH_INJECTION
99	Improper Control of Resource Identifiers ('Resource Injection')	<ul style="list-style-type: none"> • URL_MANIPULATION
113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')	<ul style="list-style-type: none"> • FB.HRS_REQUEST_PARAMETER_TO_COOKIE • FB.HRS_REQUEST_PARAMETER_TO_HTTP_HEADER
185	Incorrect Regular Expression	<ul style="list-style-type: none"> • FB.RE_BAD_SYNTAX_FOR_REGULAR_EXPRESSION • FB.RE_CANT_USE_FILE_SEPARATOR_AS_REGULAR_EXPRESSION • FB.RE_POSSIBLE_UNINTENDED_PATTERN • REGEX_CONFUSION
190	Integer Overflow or Wraparound	<ul style="list-style-type: none"> • OVERFLOW_BEFORE_WIDEN

Coverity Coverage for CWE: Java
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
192	Integer Coercion Error	<ul style="list-style-type: none"> • FB.BX_BOXING_IMMEDIATELY_UNBOXED_TO_PERFORM_COERCION • FB.ICAST_BAD_SHIFT_AMOUNT • FB.ICAST_IDIV_CAST_TO_DOUBLE • FB.ICAST_INT_2_LONG_AS_INSTANT • FB.ICAST_INT_CAST_TO_DOUBLE_PASSED_TO_CEIL • FB.ICAST_INT_CAST_TO_FLOAT_PASSED_TO_ROUND • FB.ICAST_INTEGER_MULTIPLY_CAST_TO_LONG • FB.ICAST_QUESTIONABLE_UNSIGNED_RIGHT_SHIFT
200	Information Exposure	<ul style="list-style-type: none"> • CONFIG
209	Information Exposure Through an Error Message	<ul style="list-style-type: none"> • SENSITIVE_DATA_LEAK
218	DEPRECATED (Duplicate): Failure to provide confidentiality for stored data	<ul style="list-style-type: none"> • FB.EI_EXPOSE_STATIC_REP2 • FB.MS_CANNOT_BE_FINAL • FB.MS_EXPOSE_REP • FB.MS_FINAL_PKGPROTECT • FB.MS_MUTABLE_ARRAY • FB.MS_MUTABLE_HASHTABLE • FB.MS_OOI_PKGPROTECT • FB.MS_PKGPROTECT • FB.MS_SHOULD_BE_FINAL • FB.MS_SHOULD_BE_REFACTORED_TO_BE_FINAL
227	Improper Fulfillment of API Contract ('API Abuse')	<ul style="list-style-type: none"> • FB.AM_CREATES_EMPTY_JAR_FILE_ENTRY • FB.AM_CREATES_EMPTY_ZIP_FILE_ENTRY
247	DEPRECATED (Duplicate): Reliance on DNS Lookups in a Security Decision	<ul style="list-style-type: none"> • WEAK_GUARD
252	Unchecked Return Value	<ul style="list-style-type: none"> • CHECKED_RETURN
253	Incorrect Check of Function Return Value	<ul style="list-style-type: none"> • FB.RV_RETURN_VALUE_IGNORED_BAD_PRACTICE • ORM_LOAD_NULL_CHECK
259	Use of Hard-coded Password	<ul style="list-style-type: none"> • FB.DMI_CONSTANT_DB_PASSWORD • FB.DMI_EMPTY_DB_PASSWORD • HARDCODED_CREDENTIALS
285	Improper Authorization	<ul style="list-style-type: none"> • MISSING_AUTHZ
290	Authentication Bypass by Spoofing	<ul style="list-style-type: none"> • WEAK_GUARD

Coverity Coverage for CWE: Java
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
291	Reliance on IP Address for Authentication	• WEAK_GUARD
293	Using Referer Field for Authentication	• WEAK_GUARD
296	Improper Following of a Certificate's Chain of Trust	• BAD_CERT_VERIFICATION
297	Improper Validation of Certificate with Host Mismatch	• BAD_CERT_VERIFICATION
299	Improper Check for Certificate Revocation	• BAD_CERT_VERIFICATION
311	Missing Encryption of Sensitive Data	• SENSITIVE_DATA_LEAK • UNENCRYPTED_SENSITIVE_DATA
312	Cleartext Storage of Sensitive Information	• SENSITIVE_DATA_LEAK • UNENCRYPTED_SENSITIVE_DATA
313	Cleartext Storage in a File or on Disk	• SENSITIVE_DATA_LEAK • UNENCRYPTED_SENSITIVE_DATA
315	Cleartext Storage of Sensitive Information in a Cookie	• SENSITIVE_DATA_LEAK • UNENCRYPTED_SENSITIVE_DATA
317	Cleartext Storage of Sensitive Information in GUI	• SENSITIVE_DATA_LEAK
319	Cleartext Transmission of Sensitive Information	• SENSITIVE_DATA_LEAK • UNENCRYPTED_SENSITIVE_DATA
321	Use of Hard-coded Cryptographic Key	• HARDCODED_CREDENTIALS
327	Use of a Broken or Risky Cryptographic Algorithm	• RISKY_CRYPTO
328	Reversible One-Way Hash	• RISKY_CRYPTO
330	Use of Insufficiently Random Values	• MOBILE_ID_MISUSE • INSECURE_RANDOM
337	Predictable Seed in PRNG	• PREDICTABLE_RANDOM_SEED
350	Reliance on Reverse DNS Resolution for a Security-Critical Action	• WEAK_GUARD
352	Cross-Site Request Forgery (CSRF)	• CSRF
366	Race Condition within a Thread	• FB.IS_FIELD_NOT_GUARDED • FB.IS_INCONSISTENT_SYNC • FB.IS2_INCONSISTENT_SYNC • FB.STCAL_INVOKE_ON_STATIC_ CALENDAR_INSTANCE • FB.STCAL_INVOKE_ON_STATIC_DATE_ FORMAT_INSTANCE • FB.STCAL_STATIC_ CALENDAR_INSTANCE • FB.STCAL_STATIC_SIMPLE_DATE_ FORMAT_INSTANCE • GUARDED_BY_VIOLATION • NON_STATIC_GUARDING_STATIC • RACE_CONDITION • VOLATILE_ATOMIcity

Coverity Coverage for CWE: Java
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
369	Divide By Zero	• DIVIDE_BY_ZERO
374	Passing Mutable Objects to an Untrusted Method	• FB.EI_EXPOSE_REP • FB.EI_EXPOSE_REP2
382	J2EE Bad Practices: Use of System.exit()	• FB.DM_EXIT
384	Session Fixation	• CONFIG.SPRING_SECURITY_SESSION_FIXATION • SESSION_FIXATION
390	Detection of Error Condition Without Action	• MISSING_THROW
391	Unchecked Error Condition	• FB.DE_MIGHT_DROP • FB.DE_MIGHT_IGNORE
396	Declaration of Catch for Generic Exception	• FB.REC_CATCH_EXCEPTION
398	Indicator of Poor Code Quality	• COPY_PASTE_ERROR • IDENTICAL_BRANCHES • PROPERTY_MIXUP • UNEXPECTED_CONTROL_FLOW
403	Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak')	• RESOURCE_LEAK
404	Improper Resource Shutdown or Release	• RESOURCE_LEAK
425	Direct Request ('Forced Browsing')	• CONFIG
427	Uncontrolled Search Path Element	• UNSAFE_JNI
440	Expected Behavior Violation	• FB.DMI_ANNOTATION_IS_NOT_VISIBLE_TO_REFLECTION • FB.DMI_ARGUMENTS_WRONG_ORDER • FB.DMI_BAD_MONTH • FB.DMI_BIGDECIMAL_CONSTRUCTED_FROM_DOUBLE • FB.DMI_BLOCKING_METHODS_ON_URL • FB.DMI_CALLING_NEXT_FROM_HASNEXT • FB.DMI_COLLECTION_OF_URLS • FB.DMI_COLLECTIONS_SHOULD_NOT_CONTAIN_THEMSELVES • FB.DMI_DOH • FB.DMI_ENTRY_SETS_MAY_REUSE_ENTRY_OBJECTS • FB.DMI_FUTILE_ATTEMPT_TO_CHANGE_MAXPOOL_SIZE_OF_SCHEDULED_THREAD_POOL_EXECUTOR • FB.DMI_HARDCODED_ABSOLUTE_FILENAME • FB.DMI_INVOKING_HASHCODE_ON_ARRAY

Coverity Coverage for CWE: Java
 Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
440 (cont.)	Expected Behavior Violation (cont.)	<ul style="list-style-type: none"> • FB.DMI_INVOKING_TOSTRING_ON_ ANONYMOUS_ARRAY • FB.DMI_INVOKING_TOSTRING_ON_ARRAY • FB.DMI_LONG_BITS_TO_ DOUBLE_INVOKED_ON_INT • FB.DMI_NONSERIALIZABLE_OBJECT_WRITTEN • FB.DMI_RANDOM_USED_ONLY_ONCE • FB.DMI_SCHEDULED_THREAD_POOL_EXECUTOR_WITH_ZERO_CORE_THREADS • FB.DMI_THREAD_PASSED_WHERE_RUNNABLE_EXPECTED • FB.DMI_UNSUPPORTED_METHOD • FB.DMI_USELESS_SUBSTRING • FB.DMI_USING_REMOVEALL_TO_CLEAR_COLLECTION • FB.DMI_VACUOUS_CALL_TO_EASYMOCK_METHOD • FB.DMI_VACUOUS_SELF_COLLECTION_CALL • FB.RV_01_TO_INT • FB.RV_ABSOLUTE_VALUE_OF_HASHCODE • FB.RV_ABSOLUTE_VALUE_OF_RANDOM_INT • FB.RV_CHECK_COMPARETO_FOR_SPECIFIC_RETURN_VALUE • FB.RV_CHECK_FOR_POSITIVE_INDEXOF • FB.RV_DONT_JUST_NULL_CHECK_READLINE • FB.RV_EXCEPTION_NOT_THROWN • FB.RV_NEGATING_RESULT_OF_COMPARETO • FB.RV_REM_OF_HASHCODE • FB.RV_REM_OF_RANDOM_INT • FB.RV_RETURN_VALUE_IGNORED • FB.RV_RETURN_VALUE_IGNORED_INFERRED • FB.RV_RETURN_VALUE_IGNORED2 • FB.RV_RETURN_VALUE_OF_PUTIFABSENT_IGNORED

Coverity Coverage for CWE: Java
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	<ul style="list-style-type: none"> • UNSAFE_REFLECTION • UNSAFE_NAMED_QUERY
476	NULL Pointer Dereference	<ul style="list-style-type: none"> • FB.BC_NULL_INSTANCEOF • FB.NP_ALWAYS_NULL • FB.NP_ALWAYS_NULL_EXCEPTION • FB.NP_ARGUMENT_MIGHT_BE_NULL • FB.NP_BOOLEAN_RETURN_NULL • FB.NP_CLONE_COULD_RETURN_NULL • FB.NP_CLOSING_NULL • FB.NP_DEREFERENCE_OF_READLINE_VALUE • FB.NP_DOES_NOT_HANDLE_NULL • FB.NP_EQUALS_SHOULD_HANDLE_NULL_ARGUMENT • FB.NP_FIELD_NOT_INITIALIZED_IN_CONSTRUCTOR • FB.NP_GUARANTEED_DEREF • FB.NP_GUARANTEED_DEREF_ON_EXCEPTION_PATH • FB.NP_IMMEDIATE_DEREFERENCE_OF_READLINE • FB.NP_LOAD_OF_KNOWN_NULL_VALUE • FB.NP_METHOD_PARAMETER_RELAXING_ANNOTATION • FB.NP_METHOD_PARAMETER_TIGHTENS_ANNOTATION • FB.NP_METHOD_RETURN_RELAXING_ANNOTATION • FB.NP_NONNULL_FIELD_NOT_INITIALIZED_IN_CONSTRUCTOR • FB.NP_NONNULL_PARAM_VIOLATION • FB.NP_NONNULL_RETURN_VIOLATION • FB.NP_NULL_INSTANCEOF • FB.NP_NULL_ON_SOME_PATH • FB.NP_NULL_ON_SOME_PATH_EXCEPTION • FB.NP_NULL_ON_SOME_PATH_FROM_RETURN_VALUE • FB.NP_NULL_ON_SOME_PATH_MIGHT_BE_INFEASIBLE

Coverity Coverage for CWE: Java
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
476 (cont.)	NULL Pointer Dereference (cont.)	<ul style="list-style-type: none"> • FB.NP_NULL_PARAM_DEREF • FB.NP_NULL_PARAM_DEREF_ALL_TARGETS_DANGEROUS • FB.NP_NULL_PARAM_DEREF_NONVIRTUAL • FB.NP_OPTIONAL_RETURN_NULL • FB.NP_PARAMETER_MUST_BE_NONNULL_BUT_MARKED_AS_NULLABLE • FB.NP_STORE_INTO_NONNULL_FIELD • FB.NP_TOSTRING_COULD_RETURN_NULL • FB.NP_UNWRITTEN_FIELD • FB.NP_UNWRITTEN_PUBLIC_OR_PROTECTED_FIELD • FB.RCN_REDUNDANT_COMPARISON_OF_NULL_AND_NONNULL_VALUE • FB.RCN_REDUNDANT_COMPARISON_TWO_NULL_VALUES • FB.RCN_REDUNDANT_NULLCHECK_OF_NONNULL_VALUE • FB.RCN_REDUNDANT_NULLCHECK_OF_NULL_VALUE • FB.RCN_REDUNDANT_NULLCHECK_WOULD_HAVE_BEEN_A_NPE • FORWARD_NULL • NULL_RETURNS • REVERSE_INULL
480	Use of Incorrect Operator	• CONSTANT_EXPRESSION_RESULT
481	Assigning instead of Comparing	• FB.QBA_QUESTIONABLE_BOOLEAN_ASSIGNMENT
483	Incorrect Block Delimitation	• NESTING_INDENT_MISMATCH
484	Omitted Break Statement in Switch	<ul style="list-style-type: none"> • FB.SF_DEAD_STORE_DUE_TO_SWITCH_FALLTHROUGH • FB.SF_DEAD_STORE_DUE_TO_SWITCH_FALLTHROUGH_TO_THROW • FB.SF_SWITCH_FALLTHROUGH • MISSING_BREAK
501	Trust Boundary Violation	• TRUST_BOUNDARY_VIOLATION
502	Deserialization of Untrusted Data	• UNSAFE_DESERIALIZATION

Coverity Coverage for CWE: Java
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
532	Information Exposure Through Log Files	• SENSITIVE_DATA_LEAK
538	File and Directory Information Exposure	• EXPOSED_PREFERENCES • UNRESTRICTED_ACCESS_TO_FILE
543	Use of Singleton Pattern Without Synchronization in a Multithreaded Context	• BAD_LOCK_OBJECT • FB.LI_LAZY_INIT_STATIC • FB.LI_LAZY_INIT_UPDATE_STATIC • LOCK_EVASION • SINGLETON_RACE
561	Dead Code	• DEADCODE • UNREACHABLE
563	Assignment to Variable without Use ('Unused Variable')	• FB.DLS_DEAD_LOCAL_INCREMENT_IN_RETURN • FB.DLS_DEAD_LOCAL_STORE • FB.DLS_DEAD_LOCAL_STORE_IN_RETURN • FB.DLS_DEAD_LOCAL_STORE_OF_NULL • FB.DLS_DEAD_LOCAL_STORE_SHADOWS_FIELD • FB.DLS_DEAD_STORE_OF_CLASS_LITERAL • FB.DLS_OVERWRITTEN_INCREMENT • FB.IP_PARAMETER_IS_DEAD_BUT_OVERWRITTEN • UNUSED_VALUE
564	SQL Injection: Hibernate	• SQLI
567	Unsynchronized Access to Shared Data in a Multithreaded Context	• SERVLET_ATOMICITY
568	finalize() Method Without super.finalize()	• CALL_SUPER
569	Expression Issues	• CONSTANT_EXPRESSION_RESULT
570	Expression is Always False	• FB.BC_IMPOSSIBLE_CAST • FB.BC_IMPOSSIBLE_DOWNCAST • FB.BC_IMPOSSIBLE_DOWNCAST_OF_TOARRAY • FB.BC_IMPOSSIBLE_INSTANCEOF
571	Expression is Always True	• FB.BC_VACUOUS_INSTANCEOF
572	Call to Thread run() instead of start()	• FB.RU_INVOKE_RUN
573	Improper Following of Specification by Caller	• CALL_SUPER • INVALIDATE_ITERATOR • MISSING_RESTORE • ATTRIBUTE_NAME_CONFLICT

Coverity Coverage for CWE: Java
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
579	J2EE Bad Practices: Non-serializable Object Stored in Session	• FB.J2EE_STORE_OF_NON_SERIALIZABLE_OBJECT_INTO_SESSION
580	clone() Method Without super.clone()	• CALL_SUPER • FB.CN_IDIOM • FB.CN_IDIOM_NO_SUPER_CALL • FB.CN_IMPLEMENTES_CLONE_BUT_NOT_CLONEABLE
583	finalize() Method Declared Public	• FB.FI_PUBLIC_SHOULD_BE_PROTECTED
585	Empty Synchronized Block	• FB.ESYNC_EMPTY_SYNC • FB.NP_SYNC_AND_NULL_CHECK_FIELD
586	Explicit Call to Finalize()	• FB.FI_EMPTY • FB.FI_EXPLICIT_INVOCATION • FB.FI_FINALIZER_NULLS_FIELDS • FB.FI_FINALIZER_ONLY_NULLS_FIELDS • FB.FI_MISSING_SUPER_CALL • FB.FI_NULLIFY_SUPER • FB.FI_USELESS
595	Comparison of Object References Instead of Object Contents	• FB.EQ_ABSTRACT_SELF • FB.EQ_ALWAYS_FALSE • FB.EQ_ALWAYS_TRUE • FB.EQ_CHECK_FOR_OPERAND_NOT_COMPATIBLE_WITH_THIS • FB.EQ_COMPARETO_USE_OBJECT_EQUALS • FB.EQ_COMPARING_CLASS_NAMES • FB.EQ_DOESNT_OVERRIDE_EQUALS • FB.EQ_DONT_DEFINE_EQUALS_FOR_ENUM • FB.EQ_GETCLASS_AND_CLASS_CONSTANT • FB.EQ_OTHER_NO_OBJECT • FB.EQ_OTHER_USE_OBJECT • FB.EQ_OVERRIDING_EQUALS_NOT_SYMMETRIC • FB.EQ_SELF_NO_OBJECT • FB.EQ_SELF_USE_OBJECT • FB.EQ_UNUSUAL
596	Incorrect Semantic Object Comparison	• HIBERNATE_BAD_HASHCODE
597	Use of Wrong Operator in String Comparison	• FB.ES_COMPARING_PARAMETER_STRING_WITH_EQ • FB.ES_COMPARING_STRINGS_WITH_EQ

Coverity Coverage for CWE: Java
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
601	URL Redirection to Untrusted Site ('Open Redirect')	• OPEN_REDIRECT
609	Double-Checked Locking	• FB.DC_DOUBLECHECK
610	Externally Controlled Reference to a Resource in Another Sphere	• HEADER_INJECTION
611	Improper Restriction of XML External Entity Reference ('XXE')	• XML_EXTERNAL_ENTITY
613	Insufficient Session Expiration	• CONFIG.UNSAFE_SESSION_TIMEOUT
615	Information Exposure Through Comments	• CONFIG
643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')	• XPATH_INJECTION
650	Trusting HTTP Permission Methods on the Server Side	• CONFIG
662	Improper Synchronization	• ATOMICITY
670	Always-Incorrect Control Flow Implementation	• STRAY_SEMICOLON
672	Operation on a Resource after Expiration or Release	• USE_AFTER_FREE
674	Uncontrolled Recursion	• FB.IL_INFINITE_RECURSIVE_LOOP
676	Use of Potentially Dangerous Function	• DC.DANGEROUS
683	Function Call With Incorrect Order of Arguments	• SWAPPED_ARGUMENTS
731	OWASP Top Ten 2004 Category A10 – Insecure Configuration Management	• CONFIG
759	Use of a One-Way Hash without a Salt	• WEAK_PASSWORD_HASH
760	Use of a One-Way Hash with a Predictable Salt	• WEAK_PASSWORD_HASH
776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	• XML_EXTERNAL_ENTITY
778	Insufficient Logging	• UNLOGGED_SECURITY_EXCEPTION
783	Operator Precedence Logic Error	• CONSTANT_EXPRESSION_RESULT
798	Use of Hard-coded Credentials	• CONFIG • CONFIG.SPRING_SECURITY_REMEMBER_ME_HARDCODED_KEY • HARDCODED_CREDENTIALS

JavaScript

Coverity Coverage for CWE: JavaScript		
Coverity Software Testing Platform version 2018.12		
CWE	Name	Coverity checker
20	Improper Input Validation	• COOKIE_INJECTION
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	• PATH_MANIPULATION
74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	• CSS_INJECTION
78	Improper Neutralization of Special Elements used in an OS Command ('OSCommand Injection')	• OS_CMD_INJECTION
79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	• DOM_XSS • XSS • ANGULAR_BYPASS_SECURITY • ANGULAR_ELEMENT_REFERENCE
88	Argument Injection or Modification	• HEADER_INJECTION
89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	• SQLI
94	Improper Control of Generation of Code ('Code Injection')	• REGEX_INJECTION • NOSQL_QUERY_INJECTION • TEMPLATE_INJECTION • ANGULAR_EXPRESSION_INJECTION
95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	• SCRIPT_CODE_INJECTION
99	Improper Control of Resource Identifiers ('Resource Injection')	• URL_MANIPULATION • SESSIONSTORAGE_MANIPULATION • LOCALSTORAGE_MANIPULATION
209	Information Exposure Through an Error Message	• SENSITIVE_DATA_LEAK
285	Improper Authorization	• MISSING_AUTHZ
313	Cleartext Storage in a File or on Disk	• SENSITIVE_DATA_LEAK
313	Cleartext Sensitive Data in a Database	• SENSITIVE_DATA_LEAK
314	Cleartext Storage in the Registry	• SENSITIVE_DATA_LEAK
315	Cleartext Storage of Sensitive Information in a Cookie	• SENSITIVE_DATA_LEAK
317	Cleartext Storage of Sensitive Information in GUI	• SENSITIVE_DATA_LEAK
319	Cleartext Transmission of Sensitive Information	• SENSITIVE_DATA_LEAK
327	Use of a Broken or Risky Cryptographic Algorithm	• RISKY_CRYPTO
328	Reversible One-Way Hash	• RISKY_CRYPTO
346	Origin Validation Error	• UNCHECKED_ORIGIN
352	Cross-Site Request Forgery (CSRF)	• CSRF • CONFIG.HANA_XS_PREVENT_XSRF_DISABLED

Coverity Coverage for CWE: JavaScript
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
398	Indicator of Poor Code Quality	<ul style="list-style-type: none"> • COPY_PASTE_ERROR • IDENTICAL_BRANCHES • UNEXPECTED_CONTROL_FLOW • NO_EFFECT
476	NULL Pointer Dereference	<ul style="list-style-type: none"> • FORWARD_NULL • NULL_RETURNS • REVERSE_INULL
480	Use of Incorrect Operator	<ul style="list-style-type: none"> • CONSTANT_EXPRESSION_RESULT
482	Comparing instead of Assigning	<ul style="list-style-type: none"> • NO_EFFECT
483	Incorrect Block Delimitation	<ul style="list-style-type: none"> • NESTING_INDENT_MISMATCH
484	Omitted Break Statement in Switch	<ul style="list-style-type: none"> • MISSING_BREAK
532	Information Exposure Through Log Files	<ul style="list-style-type: none"> • CONFIG.SEQUELIZE_ENABLED_LOGGING • SENSITIVE_DATA_LEAK
561	Dead Code	<ul style="list-style-type: none"> • DEADCODE • UNREACHABLE
569	Expression Issues	<ul style="list-style-type: none"> • CONSTANT_EXPRESSION_RESULT
601	URL Redirection to Untrusted Site ('Open Redirect')	<ul style="list-style-type: none"> • OPEN_REDIRECT
611	Improper Restriction of XML External Entity Reference ('XXE')	<ul style="list-style-type: none"> • XML_EXTERNAL_ENTITY
628	Function Call with Incorrectly Specified Arguments	<ul style="list-style-type: none"> • EXPLICIT_THIS_EXPECTED
665	Improper Initialization	<ul style="list-style-type: none"> • NO_EFFECT
668	Exposure of Resource to Wrong Sphere	<ul style="list-style-type: none"> • UNRESTRICTED_MESSAGE_TARGET
670	Always-Incorrect Control Flow Implementation	<ul style="list-style-type: none"> • STRAY_SEMICOLON
688	Function Call With Incorrect Variable or Reference as Argument	<ul style="list-style-type: none"> • IDENTIFIER_TYPO
760	Use of a One-Way Hash with a Predictable Salt	<ul style="list-style-type: none"> • INSECURE_SALT
776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	<ul style="list-style-type: none"> • XML_EXTERNAL_ENTITY
778	Insufficient logging	<ul style="list-style-type: none"> • INSUFFICIENT_LOGGING
783	Operator Precedence Logic Error	<ul style="list-style-type: none"> • CONSTANT_EXPRESSION_RESULT
798	Use of Hard-coded Credentials	<ul style="list-style-type: none"> • HARDCODED_CREDENTIALS

Coverity Coverage for CWE: JavaScript
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
829	Inclusion of Functionality from Untrusted Control Sphere	• MISSING_IFRAME_SANDBOX
922	Insecure Storage of Sensitive Information	• LOCALSTORAGE_WRITE

Node.js

Coverity Coverage for CWE: Node.js
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	• PATH_MANIPULATION
78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	• OS_CMD_INJECTION
79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	• XSS
88	Argument Injection or Modification	• HEADER_INJECTION
89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	• SQLI
94	Improper Control of Generation of Code ('Code Injection')	• NOSQL_QUERY_INJECTION
95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	• SCRIPT_CODE_INJECTION
209	Information Exposure Through an Error Message	• SENSITIVE_DATA_LEAK
285	Improper Authorization	• MISSING_AUTHZ
313	Cleartext Storage in a File or on Disk	• SENSITIVE_DATA_LEAK
313	Cleartext Sensitive Data in a Database	• SENSITIVE_DATA_LEAK
314	Cleartext Storage in the Registry	• SENSITIVE_DATA_LEAK
315	Cleartext Storage of Sensitive Information in a Cookie	• SENSITIVE_DATA_LEAK
317	Cleartext Storage of Sensitive Information in GUI	• SENSITIVE_DATA_LEAK
319	Cleartext Transmission of Sensitive Information	• SENSITIVE_DATA_LEAK
327	Use of a Broken or Risky Cryptographic Algorithm	• RISKY_CRYPTO
328	Reversible One-Way Hash	• RISKY_CRYPTO
352	Cross-Site Request Forgery (CSRF)	• CONFIG.HANA_XS_PREVENT_XSRF_DISABLED • CSRF
398	Indicator of Poor Code Quality	• COPY_PASTE_ERROR • IDENTICAL_BRANCHES • NO_EFFECT

Coverity Coverage for CWE: Node.js
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
476	NULL Pointer Dereference	• FORWARD_NULL • NULL_RETURNS • REVERSE_INULL
480	Use of Incorrect Operator	• CONSTANT_EXPRESSION_RESULT
483	Incorrect Block Delimitation	• NESTING_INDENT_MISMATCH
484	Omitted Break Statement in Switch	• MISSING_BREAK
532	Information Exposure Through Log Files	• SENSITIVE_DATA_LEAK
561	Dead Code	• DEADCODE • UNREACHABLE
569	Expression Issues	• CONSTANT_EXPRESSION_RESULT
601	URL Redirection to Untrusted Site ('Open Redirect')	• OPEN_REDIRECT
665	Improper Initialization	• NO_EFFECT
688	Function Call With Incorrect Variable or Reference as Argument	• IDENTIFIER_TYPO
670	Always-Incorrect Control Flow Implementation	• STRAY_SEMICOLON
783	Operator Precedence Logic Error	• CONSTANT_EXPRESSION_RESULT
798	Use of Hard-coded Credentials	• HARDCODED_CREDENTIALS

PHP

Coverity Coverage for CWE: PHP
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
20	Improper Input Validation	• XSS • PATH_MANIPULATION
21	Pathname Traversal and Equivalence Errors	• PATH_MANIPULATION
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	• PATH_MANIPULATION
23	Relative Path Traversal	• PATH_MANIPULATION
36	Absolute Path Traversal	• PATH_MANIPULATION
74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	• XSS
78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	• OS_CMD_INJECTION
79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	• XSS
80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	• XSS
82	Improper Neutralization of Script in Attributes of IMG Tags in a Web Page	• XSS
83	Improper Neutralization of Script in Attributes in a Web Page	• XSS

Coverity Coverage for CWE: PHP
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
85	Doubled Character XSS Manipulations	• XSS
86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages	• XSS
87	Improper Neutralization of Alternate XSS Syntax	• XSS
88	Argument Injection or Modification	• HEADER_INJECTION
89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	• SQLI
95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	• SCRIPT_CODE_INJECTION
209	Information Exposure Through an Error Message	• SENSITIVE_DATA_LEAK
313	Cleartext Sensitive Data in a Database	• SENSITIVE_DATA_LEAK
313	Cleartext Storage in a File or on Disk	• SENSITIVE_DATA_LEAK
314	Cleartext Storage in the Registry	• SENSITIVE_DATA_LEAK
315	Cleartext Storage of Sensitive Information in a Cookie	• SENSITIVE_DATA_LEAK
317	Cleartext Storage of Sensitive Information in GUI	• SENSITIVE_DATA_LEAK
319	Cleartext Transmission of Sensitive Information	• SENSITIVE_DATA_LEAK
398	Indicator of Poor Code Quality	• COPY_PASTE_ERROR • IDENTICAL_BRANCHES • NO_EFFECT
476	NULL Pointer Dereference	• FORWARD_NULL
480	Use of Incorrect Operator	• CONSTANT_EXPRESSION_RESULT
482	Comparing instead of Assigning	• NO_EFFECT
483	Incorrect Block Delimitation	• NESTING_INDENT_MISMATCH
484	Omitted Break Statement in Switch	• MISSING_BREAK
502	Deserialization of Untrusted Data	• UNSAFE_DESERIALIZATION
532	Information Exposure Through Log Files	• SENSITIVE_DATA_LEAK
561	Dead Code	• UNREACHABLE • DEADCODE
569	Expression Issues	• CONSTANT_EXPRESSION_RESULT
611	Improper Restriction of XML External Entity Reference ('XXE')	• XML_EXTERNAL_ENTITY
665	Improper Initialization	• NO_EFFECT

Coverity Coverage for CWE: PHP

Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
670	Always-Incorrect Control Flow Implementation	• STRAY_SEMICOLON
688	Function Call With Incorrect Variable or Reference as Argument	• IDENTIFIER_TYPO
783	Operator Precedence Logic Error	• CONSTANT_EXPRESSION_RESULT
798	Use of Hard-coded Credentials	• HARDCODED_CREDENTIALS

Python

Coverity Coverage for CWE: Python

Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
20	Improper Input Validation	• XSS • PATH_MANIPULATION
21	Pathname Traversal and Equivalence Errors	• PATH_MANIPULATION
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	• PATH_MANIPULATION
23	Relative Path Traversal	• PATH_MANIPULATION
36	Absolute Path Traversal	• PATH_MANIPULATION
74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	• XSS
78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	• OS_CMD_INJECTION
79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	• XSS
80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	• XSS
82	Improper Neutralization of Script in Attributes of IMG Tags in a Web Page	• XSS
83	Improper Neutralization of Script in Attributes in a Web Page	• XSS
85	Doubled Character XSS Manipulations	• XSS
86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages	• XSS
87	Improper Neutralization of Alternate XSS Syntax	• XSS
89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	• SQLI
94	Improper Control of Generation of Code ('Code Injection')	• NOSQL_QUERY_INJECTION
95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	• SCRIPT_CODE_INJECTION
209	Information Exposure Through an Error Message	• SENSITIVE_DATA_LEAK
313	Cleartext Sensitive Data in a Database	• SENSITIVE_DATA_LEAK

Coverity Coverage for CWE: Python
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
313	Cleartext Storage in a File or on Disk	• SENSITIVE_DATA_LEAK
314	Cleartext Storage in the Registry	• SENSITIVE_DATA_LEAK
315	Cleartext Storage of Sensitive Information in a Cookie	• SENSITIVE_DATA_LEAK
317	Cleartext Storage of Sensitive Information in GUI	• SENSITIVE_DATA_LEAK
319	Cleartext Transmission of Sensitive Information	• SENSITIVE_DATA_LEAK
398	Indicator of Poor Code Quality	• COPY_PASTE_ERROR • IDENTICAL_BRANCHES
476	NULL Pointer Dereference	• FORWARD_NULL • REVERSE_INULL
480	Use of Incorrect Operator	• CONSTANT_EXPRESSION_RESULT
502	Deserialization of Untrusted Data	• UNSAFE_DESERIALIZATION
532	Information Exposure Through Log Files	• SENSITIVE_DATA_LEAK
561	Dead Code	• UNREACHABLE • DEADCODE
569	Expression Issues	• CONSTANT_EXPRESSION_RESULT
601	URL Redirection to Untrusted Site ('Open Redirect')	• OPEN_REDIRECT
611	Improper Restriction of XML External Entity Reference ('XXE')	• XML_EXTERNAL_ENTITY
688	Function Call With Incorrect Variable or Reference as Argument	• IDENTIFIER_TYPO
783	Operator Precedence Logic Error	• CONSTANT_EXPRESSION_RESULT

Ruby

Coverity Coverage for CWE: Ruby
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	• PATH_MANIPULATION • RUBY_VULNERABLE_LIBRARY
73	External Control of File Name or Path	• RUBY_VULNERABLE_LIBRARY
78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	• OS_CMD_INJECTION
79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	• RUBY_VULNERABLE_LIBRARY • UNESCAPED_HTML • XSS
83	Improper Neutralization of Script in Attributes in a Web Page	• XSS

Coverity Coverage for CWE: Ruby
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	• DYNAMIC_OBJECT_ATTRIBUTES • RUBY_VULNERABLE_LIBRARY • SQLI
94	Improper Control of Generation of Code ('Code Injection')	• REGEX_INJECTION
95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	• PATH_MANIPULATION • SCRIPT_CODE_INJECTION
113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting').	• RUBY_VULNERABLE_LIBRARY
183	Permissive Whitelist	• DYNAMIC_OBJECT_ATTRIBUTES
184	Incomplete Blacklist	• BLACKLIST_FOR_AUTHN
209	Information Exposure Through an Error Message	• SENSITIVE_DATA_LEAK
215	Information Exposure Through Debug Information	• SENSITIVE_DATA_LEAK
259	Use of Hard-coded Password	• HARDCODED_CREDENTIALS
263	Password Aging with Long Expiration	• RAILS_DEVISE_CONFIG
287	Improper Authentication	• UNSAFE_BASIC_AUTH
289	Authentication Bypass by Alternate Name	• RUBY_VULNERABLE_LIBRARY • UNSAFE_BASIC_AUTH
307	Improper Restriction of Excessive Authentication Attempts	• RAILS_DEVISE_CONFIG
321	Use of Hard-coded Cryptographic Key	• UNSAFE_SESSION_SETTING
352	Cross-Site Request Forgery (CSRF)	• CSRF
369	Divide By Zero	• DIVIDE_BY_ZERO
398	Indicator of Poor Code Quality	• COPY_PASTE_ERROR • IDENTICAL_BRANCHES • NO_EFFECT • UNEXPECTED_CONTROL_FLOW
400	Uncontrolled Resource Consumption ('Resource Exhaustion').	• RAILS_DEFAULT_ROUTES • RESOURCE_LEAK • RUBY_VULNERABLE_LIBRARY
470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	• UNSAFE_REFLECTION
476	NULL Pointer Dereference	• FORWARD_NULL • REVERSE_INULL
480	Use of Incorrect Operator	• CONSTANT_EXPRESSION_RESULT
482	Comparing instead of Assigning	• NO_EFFECT
483	Incorrect Block Delimitation	• NESTING_INDENT_MISMATCH
484	Omitted Break Statement in Switch	• MISSING_BREAK
502	Deserialization of Untrusted Data	• RUBY_VULNERABLE_LIBRARY • UNSAFE_DESERIALIZATION

Coverity Coverage for CWE: Ruby		
Coverity Software Testing Platform version 2018.12		
CWE	Name	Coverity checker
521	Weak Password Requirements	• RAILS_DEVISE_CONFIG
561	Dead Code	• DEADCODE • UNREACHABLE
569	Expression Issues	• CONSTANT_EXPRESSION_RESULT
599	Missing Validation of OpenSSL Certificate	• BAD_CERT_VERIFICATION
601	URL Redirection to Untrusted Site ('Open Redirect')	• OPEN_REDIRECT
614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	• INSECURE_COOKIE • UNSAFE_SESSION_SETTING
639	Authorization Bypass Through User-Controlled Key	• INSECURE_DIRECT_OBJECT_REFERENCE
642	External Control of Critical State Data	• SESSION_MANIPULATION
665	Improper Initialization	• NO_EFFECT
688	Function Call With Incorrect Variable or Reference as Argument	• IDENTIFIER_TYPO
704	Incorrect Type Conversion or Cast	• SQLI
777	Regular Expression without Anchors.	• REGEX_MISSING_ANCHOR
783	Operator Precedence Logic Error	• CONSTANT_EXPRESSION_RESULT
798	Use of Hard-coded Credentials	• UNSAFE_BASIC_AUTH
862	Missing Authorization	• RAILS_DEFAULT_ROUTES • RAILS_MISSING_FILTER_ACTION
915	Improperly Controlled Modification of Dynamically-Determined Object Attributes	• DYNAMIC_OBJECT_ATTRIBUTES
916	Use of Password Hash With Insufficient Computational Effort	• RAILS_DEVISE_CONFIG • WEAK_PASSWORD_HASH
1004	Sensitive Cookie Without 'HttpOnly' Flag	• INSECURE_COOKIE • UNSAFE_SESSION_SETTING

Scala

Coverity Coverage for CWE: Scala		
Coverity Software Testing Platform version 2018.12		
CWE	Name	Coverity checker
190	Integer Overflow or Wraparound	• OVERFLOW_BEFORE_WIDEN

Coverity Coverage for CWE: Scala
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
398	Indicator of Poor Code Quality	<ul style="list-style-type: none"> • COPY_PASTE_ERROR • IDENTICAL_BRANCHES • NO_EFFECT
476	NULL Pointer Dereference	<ul style="list-style-type: none"> • FORWARD_NULL • REVERSE_NULL
480	Use of Incorrect Operator	<ul style="list-style-type: none"> • CONSTANT_EXPRESSION_RESULT
482	Comparing instead of Assigning	<ul style="list-style-type: none"> • NO_EFFECT
483	Incorrect Block Delimitation	<ul style="list-style-type: none"> • NESTING_INDENT_MISMATCH
561	Dead Code	<ul style="list-style-type: none"> • DEADCODE
569	Expression Issues	<ul style="list-style-type: none"> • CONSTANT_EXPRESSION_RESULT
783	Operator Precedence Logic Error	<ul style="list-style-type: none"> • CONSTANT_EXPRESSION_RESULT

Swift

Coverity Coverage for CWE: Swift
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
20	Improper Input Validation	<ul style="list-style-type: none"> • REGEX_INJECTION • SCRIPT_CODE_INJECTION
89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	<ul style="list-style-type: none"> • SQLI
209	Information Exposure Through an Error Message	<ul style="list-style-type: none"> • SENSITIVE_DATA_LEAK
227	Improper Fulfillment of API Contract ('API Abuse')	<ul style="list-style-type: none"> • BAD_CERT_VERIFICATION
287	Improper Authentication	<ul style="list-style-type: none"> • WEAK_BIOMETRIC_AUTH
313	Cleartext Sensitive Data in a Database	<ul style="list-style-type: none"> • SENSITIVE_DATA_LEAK • UNENCRYPTED_SENSITIVE_DATA
314	Cleartext Storage in the Registry	<ul style="list-style-type: none"> • SENSITIVE_DATA_LEAK
315	Cleartext Storage of Sensitive Information in a Cookie	<ul style="list-style-type: none"> • SENSITIVE_DATA_LEAK • UNENCRYPTED_SENSITIVE_DATA
317	Cleartext Storage of Sensitive Information in GUI	<ul style="list-style-type: none"> • SENSITIVE_DATA_LEAK
319	Cleartext Transmission of Sensitive Information	<ul style="list-style-type: none"> • SENSITIVE_DATA_LEAK • INSECURE_MULTIPLE_PEER_CONNECTION • INSECURE_COMMUNICATION • CONFIG.ATS_INSECURE • UNENCRYPTED_SENSITIVE_DATA
327	Use of a Broken or Risky Cryptographic Algorithm	<ul style="list-style-type: none"> • RISKY_CRYPTO

Coverity Coverage for CWE: Swift
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
328	Reversible One-Way Hash	• RISKY_CRYPTO
391	Unchecked Error Condition	• UNEXPECTED_CONTROL_FLOW
398	Indicator of Poor Code Quality	• COPY_PASTE_ERROR • UNEXPECTED_CONTROL_FLOW • IDENTICAL_BRANCHES • PW.*
476	NULL Pointer Dereference	• FORWARD_NULL • REVERSE_NULL
480	Use of Incorrect Operator	• CONSTANT_EXPRESSION_RESULT
532	Information Exposure Through Log Files	• SENSITIVE_DATA_LEAK
561	Dead Code	• DEADCODE
569	Expression Issues	• CONSTANT_EXPRESSION_RESULT
710	Improper Adherence to Coding Standards	• PROPERTY_MIXUP
798	Use of Hard-coded Credentials	• HARDCODED_CREDENTIALS
829	Inclusion of Functionality from Untrusted Control Sphere	• CUSTOM_KEYBOARD_DATA_LEAK

VB.NET

Coverity Coverage for CWE: VB.NET
Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	• XSS
89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	• SQLI • SQL_NOT_CONSTANT
90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	• LDAP_INJECTION
209	Information Exposure Through an Error Message	• SENSITIVE_DATA_LEAK
223	Omission of Security-relevant Information	• UNLOGGED_SECURITY_EXCEPTION
285	Improper Authorization	• MISSING_AUTHZ • SQLI • SQL_NOT_CONSTANT
311	Missing Encryption of Sensitive Data	• SENSITIVE_DATA_LEAK
312	Cleartext Storage of Sensitive Information	• SENSITIVE_DATA_LEAK
319	Cleartext Transmission of Sensitive Information	• SENSITIVE_DATA_LEAK
321	Key Management Errors	• HARDCODED_CREDENTIALS

Coverity Coverage for CWE: VB.NET

Coverity Software Testing Platform version 2018.12

CWE	Name	Coverity checker
327	Use of a Broken or Risky Cryptographic Algorithm	<ul style="list-style-type: none"> • RISKY_CRYPT0 • WEAK_PASSWORD_HASH
328	Reversible One-Way Hash	<ul style="list-style-type: none"> • RISKY_CRYPT0
398	Indicator of Poor Code Quality	<ul style="list-style-type: none"> • COPY_PASTE_ERROR • UNEXPECTED_CONTROL_FLOW • IDENTICAL_BRANCHES
404	Improper Resource Shutdown or Release	<ul style="list-style-type: none"> • RESOURCE_LEAK
459	Incomplete Cleanup	<ul style="list-style-type: none"> • RESOURCE_LEAK
476	NULL Pointer Dereference	<ul style="list-style-type: none"> • FORWARD_NULL • REVERSE_INULL • NULL_RETURNS
502	Deserialization of Untrusted Data	<ul style="list-style-type: none"> • UNSAFE_DESERIALIZATION
561	Dead Code	<ul style="list-style-type: none"> • DEADCODE • UNREACHABLE
573	Improper Following of Specification by Caller	<ul style="list-style-type: none"> • CALL_SUPER
611	Improper Restriction of XML External Entity Reference ('XXE')	<ul style="list-style-type: none"> • XML_EXTERNAL_ENTITY
619	Dangling Database Cursor ('Cursor Injection')	<ul style="list-style-type: none"> • RESOURCE_LEAK
639	Authorization Bypass Through User-Controlled Key	<ul style="list-style-type: none"> • SQLI • SQL_NOT_CONSTANT
683	Function Call With Incorrect Order of Arguments	<ul style="list-style-type: none"> • SWAPPED_ARGUMENTS • RESOURCE_LEAK
690	Unchecked Return Value to NULL Pointer Dereference	<ul style="list-style-type: none"> • REVERSE_INULL
763	Release of Invalid Pointer or Reference	<ul style="list-style-type: none"> • RESOURCE_LEAK
772	Missing Release of Resource after Effective Lifetime	<ul style="list-style-type: none"> • RESOURCE_LEAK
776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	<ul style="list-style-type: none"> • XML_EXTERNAL_ENTITY
778	Insufficient Logging	<ul style="list-style-type: none"> • UNLOGGED_SECURITY_EXCEPTION

The Synopsys difference

Synopsys Software Integrity Group helps organizations build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations maximize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
 185 Berry Street, Suite 6500
 San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
 International Sales: +1 415.321.5237
 Email: sig-info@synopsys.com