SYNOPSYS®

Coverity Coverage for OWASP Top 10 (2017)

C#

Coverity Software Testing Platform version 2018.12			
Category	**CWE**	**Description**	**Coverity checker**
A1: Injection	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	HEADER_INJECTION, OS_CMD_INJECTION
	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	OS_CMD_INJECTION
	88	Argument Injection or Modification	HEADER_INJECTION, OS_CMD_INJECTION
	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
	91	XML Injection (aka Blind XPath Injection)	XML_INJECTION, XPATH_INJECTION
	943	Improper Neutralization of Special Elements in Data Query Logic	LDAP_INJECTION, SQLI, SQL_NOT_CONSTANT, XPATH_INJECTION
A2: Broken Authentication	287	Improper Authentication	CONFIG.CONNECTION_STRING_PASSWORD, HARDCODED_CREDENTIALS, MISSING_AUTHZ
A3: Sensitive Data Exposure	311	Missing Encryption of Sensitive Data	SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA
	312	Cleartext Storage of Sensitive Information	SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA
	319	Cleartext Transmission of Sensitive Information	SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA
	320	Key Management Errors	HARDCODED_CREDENTIALS
	326	Inadequate Encryption Strength	RISKY_CRYPTO
	327	Use of a Broken or Risky Cryptographic Algorithm	RISKY_CRYPTO, WEAK_PASSWORD_HASH
	328	Reversible One-Way Hash	RISKY_CRYPTO
	359	Exposure of Private Information ('Privacy Violation')	SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA

C# (cont.)

A4: XML External Entities (XXE)	611	Improper Restriction of XML External Entity Reference ('XXE')	XML_EXTERNAL_ENTITY
	776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	XML_EXTERNAL_ENTITY
A5: Broken Access Control	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	PATH_MANIPULATION
	284	Improper Access Control	CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.DEAD_AUTHORIZATION_RULE, HARDCODED_CREDENTIALS, MISSING_AUTHZ, RISKY_CRYPTO, SQLI, SQL_NOT_CONSTANT
	285	Improper Authorization	CONFIG.DEAD_AUTHORIZATION_RULE, MISSING_AUTHZ, SQLI, SQL_NOT_CONSTANT
	639	Authorization Bypass Through User-Controlled Key	SQLI, SQL_NOT_CONSTANT
A6: Security Misconfiguration	16	Configuration	CONFIG.ASP_VIEWSTATE_MAC, CONFIG.ENABLED_DEBUG_MODE
	209	Information Exposure Through an Error Message	SENSITIVE_DATA_LEAK
A7: Cross-Site Scripting (XSS)	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	XSS
A8: Insecure Deserialization	502	Deserialization of Untrusted Data	UNSAFE_DESERIALIZATION
A10: Insufficient Logging & Monitoring	223	Omission of Security-relevant Information	UNLOGGED_SECURITY_EXCEPTION
	778	Insufficient Logging	UNLOGGED_SECURITY_EXCEPTION

Java

Coverity Software Testing Platform version 2018.12			
Category	**CWE**	**Description**	**Coverity checker**
A1: Injection	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	EL_INJECTION, HEADER_INJECTION, OS_CMD_INJECTION
	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	OS_CMD_INJECTION, TAINTED_ENVIRONMENT_WITH_EXECUTION
	88	Argument Injection or Modification	HEADER_INJECTION, OS_CMD_INJECTION
	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	JSP_SQL_INJECTION, SQLI, SQL_NOT_CONSTANT
	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	LDAP_INJECTION

Java (cont.)

A1: Injection (cont.)	91	XML Injection (aka Blind XPath Injection)	XML_INJECTION, XPATH_INJECTION
	917	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	EL_INJECTION
	943	Improper Neutralization of Special Elements in Data Query Logic	JSP_SQL_INJECTION, LDAP_INJECTION, SQLI, SQL_NOT_CONSTANT, XPATH_INJECTION
A2: Broken Authentication	287	Improper Authentication	CONFIG.MISSING_JSF2_SECURITY_CONSTRAINT, CONFIG.SPRING_SECURITY_HARDCODED_CREDENTIALS, CONFIG.SPRING_SECURITY_REMEMBER_ME_HARDCODED_KEY, CONFIG.SPRING_SECURITY_SESSION_FIXATION, HARDCODED_CREDENTIALS, MISSING_AUTHZ, SESSION_FIXATION, WEAK_GUARD
	384	Session Fixation	CONFIG.SPRING_SECURITY_SESSION_FIXATION, SESSION_FIXATION
	613	Insufficient Session Expiration	CONFIG.UNSAFE_SESSION_TIMEOUT
A3: Sensitive Data Exposure	295	Improper Certificate Validation	BAD_CERT_VERIFICATION
	311	Missing Encryption of Sensitive Data	INSECURE_COOKIE, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA
	312	Cleartext Storage of Sensitive Information	SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA
	319	Cleartext Transmission of Sensitive Information	SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA
	320	Key Management Errors	HARDCODED_CREDENTIALS
	326	Inadequate Encryption Strength	RISKY_CRYPTO
	327	Use of a Broken or Risky Cryptographic Algorithm	RISKY_CRYPTO, WEAK_PASSWORD_HASH
	328	Reversible One-Way Hash	RISKY_CRYPTO
	359	Exposure of Private Information ('Privacy Violation')	SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA
A4: XML External Entities (XXE)	611	Improper Restriction of XML External Entity Reference ('XXE')	XML_EXTERNAL_ENTITY
	776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	XML_EXTERNAL_ENTITY
A5: Broken Access Control	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	JSP_DYNAMIC_INCLUDE, PATH_MANIPULATION

Java (cont.)

A5: Broken Access Control (cont.)	284	Improper Access Control	BAD_CERT_VERIFICATION, CONFIG.DWR_DEBUG_MODE, CONFIG.MISSING_JSF2_SECURITY_CONSTRAINT, CONFIG.SPRING_SECURITY_DEBUG_MODE, CONFIG.SPRING_SECURITY_HARDCODED_CREDENTIALS, CONFIG.SPRING_SECURITY_REMEMBER_ME_HARDCODED_KEY, CONFIG.SPRING_SECURITY_SESSION_FIXATION, CONFIG.STRUTS2_CONFIG_BROWSER_PLUGIN, CONFIG.STRUTS2_DYNAMIC_METHOD_INVOCATION, CONFIG.STRUTS2_ENABLED_DEV_MODE, HARDCODED_CREDENTIALS, IMPLICIT_INTENT, JSP_SQL_INJECTION, MISSING_AUTHZ, MISSING_PERMISSION_FOR_BROADCAST, MISSING_PERMISSION_ON_EXPORTED_COMPONENT, RISKY_CRYPTO, SENSITIVE_DATA_LEAK, SESSION_FIXATION, SQLI, SQL_NOT_CONSTANT, WEAK_GUARD
	285	Improper Authorization	CONFIG.DWR_DEBUG_MODE, CONFIG.MISSING_JSF2_SECURITY_CONSTRAINT, CONFIG.SPRING_SECURITY_DEBUG_MODE, CONFIG.STRUTS2_CONFIG_BROWSER_PLUGIN, CONFIG.STRUTS2_DYNAMIC_METHOD_INVOCATION, CONFIG.STRUTS2_ENABLED_DEV_MODE, IMPLICIT_INTENT, JSP_SQL_INJECTION, MISSING_AUTHZ, MISSING_PERMISSION_FOR_BROADCAST, MISSING_PERMISSION_ON_EXPORTED_COMPONENT, SENSITIVE_DATA_LEAK, SQLI, SQL_NOT_CONSTANT
	425	Direct Request ('Forced Browsing')	CONFIG.MISSING_JSF2_SECURITY_CONSTRAINT
	639	Authorization Bypass Through User-Controlled Key	JSP_SQL_INJECTION, SQLI, SQL_NOT_CONSTANT
A6: Security Misconfiguration	16	Configuration	CONFIG.DUPLICATE_SERVLET_DEFINITION, CONFIG.MISSING_GLOBAL_EXCEPTION_HANDLER
	209	Information Exposure Through an Error Message	SENSITIVE_DATA_LEAK
A7: Cross-Site Scripting (XSS)	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	XSS
A8: Insecure Deserialization	502	Deserialization of Untrusted Data	UNSAFE_DESERIALIZATION
A10: Insufficient Logging & Monitoring	223	Omission of Security-relevant Information	UNLOGGED_SECURITY_EXCEPTION
	778	Insufficient Logging	UNLOGGED_SECURITY_EXCEPTION

JavaScript

Coverity Software Testing Platform version 2018.12			
Category	**CWE**	**Description**	**Coverity checker**
A1: Injection	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	HEADER_INJECTION, OS_CMD_INJECTION
	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	OS_CMD_INJECTION
	88	Argument Injection or Modification	HEADER_INJECTION, OS_CMD_INJECTION
	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	SQLI
	943	Improper Neutralization of Special Elements in Data Query Logic	SQLI
A2: Broken Authentication	287	Improper Authentication	HARDCODED_CREDENTIALS, MISSING_AUTHZ
A3: Sensitive Data Exposure	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
	326	Inadequate Encryption Strength	RISKY_CRYPTO
	327	Use of a Broken or Risky Cryptographic Algorithm	INSECURE_SALT, RISKY_CRYPTO
	328	Reversible One-Way Hash	RISKY_CRYPTO
	359	Exposure of Private Information ('Privacy Violation')	SENSITIVE_DATA_LEAK
A4: XML External Entities (XXE)	611	Improper Restriction of XML External Entity Reference ('XXE')	XML_EXTERNAL_ENTITY
	776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	XML_EXTERNAL_ENTITY
A5: Broken Access Control	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	PATH_MANIPULATION
	284	Improper Access Control	HARDCODED_CREDENTIALS, MISSING_AUTHZ, SQLI, UNCHECKED_ORIGIN
	285	Improper Authorization	MISSING_AUTHZ, SQLI
	639	Authorization Bypass Through User-Controlled Key	SQLI

JavaScript (cont.)

A6: Security Misconfiguration	209	Information Exposure Through an Error Message	SENSITIVE_DATA_LEAK
A7: Cross-Site Scripting (XSS)	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	DOM_XSS, XSS, ANGULAR_BYPASS_SECURITY, ANGULAR_ELEMENT_REFERENCE
A8: Insecure Deserialization	502	Deserialization of Untrusted Data	UNSAFE_DESERIALIZATION
A10: Insufficient Logging & Monitoring	778	Insufficient logging	INSUFFICIENT_LOGGING

PHP

Coverity Software Testing Platform version 2018.12			
Category	**CWE**	**Description**	**Coverity checker**
A1: Injection	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	HEADER_INJECTION, OS_CMD_INJECTION
	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	OS_CMD_INJECTION
	88	Argument Injection or Modification	HEADER_INJECTION, OS_CMD_INJECTION
	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	SQLI
	943	Improper Neutralization of Special Elements in Data Query Logic	SQLI
A2: Broken Authentication	287	Improper Authentication	HARDCODED_CREDENTIALS, MISSING_AUTHZ
A3: Sensitive Data Exposure	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
	359	Exposure of Private Information ('Privacy Violation')	SENSITIVE_DATA_LEAK
A4: XML External Entities (XXE)	611	Improper Restriction of XML External Entity Reference ('XXE')	XML_EXTERNAL_ENTITY

PHP (cont.)

A5: Broken Access Control	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	PATH_MANIPULATION
	284	Improper Access Control	HARDCODED_CREDENTIALS, MISSING_AUTHZ, SQLI
	285	Improper Authorization	MISSING_AUTHZ, SQLI
	639	Authorization Bypass Through User-Controlled Key	SQLI
A6: Security Misconfiguration	209	Information Exposure Through an Error Message	SENSITIVE_DATA_LEAK
A7: Cross-Site Scripting (XSS)	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	XSS
A8: Insecure Deserialization	502	Deserialization of Untrusted Data	UNSAFE_DESERIALIZATION

Python

Coverity Software Testing Platform version 2018.12			
Category	**CWE**	**Description**	**Coverity checker**
A1: Injection	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 ('OS Command Injection')	OS_CMD_INJECTION
	88	Argument Injection or Modification	OS_CMD_INJECTION
	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	SQLI
	943	Improper Neutralization of Special Elements in Data Query Logic	SQLI
A2: Broken Authentication	287	Improper Authentication	HARDCODED_CREDENTIALS, MISSING_AUTHZ
A3: Sensitive Data Exposure	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
	359	Exposure of Private Information ('Privacy Violation')	SENSITIVE_DATA_LEAK
A4: XML External Entities (XXE)	611	Improper Restriction of XML External Entity Reference ('XXE')	XML_EXTERNAL_ENTITY

Python (cont.)

A5: Broken Access Control	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	PATH_MANIPULATION
	284	Improper Access Control	HARDCODED_CREDENTIALS, MISSING_AUTHZ, SQLI
	285	Improper Authorization	MISSING_AUTHZ, SQLI
	639	Authorization Bypass Through User-Controlled Key	SQLI
A6: Security Misconfiguration	209	Information Exposure Through an Error Message	SENSITIVE_DATA_LEAK
A7: Cross-Site Scripting (XSS)	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	XSS
A8: Insecure Deserialization	502	Deserialization of Untrusted Data	UNSAFE_DESERIALIZATION

Ruby

Coverity Software Testing Platform version 2018.12			
Category	**CWE**	**Description**	**Coverity checker**
A1: Injection	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	OS_CMD_INJECTION
	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	DYNAMIC_OBJECT_ATTRIBUTES, RUBY_VULNERABLE_LIBRARY, SQLI
A2: Broken Authentication	287	Improper Authentication	UNSAFE_BASIC_AUTH
A5: Broken Access Control	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	PATH_MANIPULATION, RUBY_VULNERABLE_LIBRARY
	639	Authorization Bypass Through User-Controlled Key	INSECURE_DIRECT_OBJECT_REFERENCE
A6: Security Misconfiguration	209	Information Exposure Through an Error Message	SENSITIVE_DATA_LEAK
A7: Cross-Site Scripting (XSS)	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	RUBY_VULNERABLE_LIBRARY, UNESCAPED_HTML, XSS
A8: Insecure Deserialization	502	Deserialization of Untrusted Data	RUBY_VULNERABLE_LIBRARY, UNSAFE_DESERIALIZATION

VB.NET

Coverity Software Testing Platform version 2018.12			
Category	**CWE**	**Description**	**Coverity checker**
A1: Injection	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
	943	Improper Neutralization of Special Elements in Data Query Logic	LDAP_INJECTION, SQLI, SQL_NOT_CONSTANT
A2: Broken Authentication	287	Improper Authentication	HARDCODED_CREDENTIALS, MISSING_AUTHZ
A3: Sensitive Data Exposure	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
	320	Key Management Errors	HARDCODED_CREDENTIALS
	326	Inadequate Encryption Strength	RISKY_CRYPTO
	327	Use of a Broken or Risky Cryptographic Algorithm	RISKY_CRYPTO, WEAK_PASSWORD_HASH
	328	Reversible One-Way Hash	RISKY_CRYPTO
	359	Exposure of Private Information ('Privacy Violation')	SENSITIVE_DATA_LEAK
A4: XML External Entities (XXE)	611	Improper Restriction of XML External Entity Reference ('XXE')	XML_EXTERNAL_ENTITY
	776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	XML_EXTERNAL_ENTITY
A5: Broken Access Control	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	PATH_MANIPULATION
	284	Improper Access Control	HARDCODED_CREDENTIALS, MISSING_AUTHZ, RISKY_CRYPTO, SQLI, SQL_NOT_CONSTANT
	285	Improper Authorization	MISSING_AUTHZ, SQLI, SQL_NOT_CONSTANT
	639	Authorization Bypass Through User-Controlled Key	SQLI, SQL_NOT_CONSTANT
A6: Security Misconfiguration	209	Information Exposure Through an Error Message	SENSITIVE_DATA_LEAK
A7: Cross-Site Scripting (XSS)	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	XSS
A8: Insecure Deserialization	502	Deserialization of Untrusted Data	UNSAFE_DESERIALIZATION
A10: Insufficient Logging & Monitoring	223	Omission of Security-relevant Information	UNLOGGED_SECURITY_EXCEPTION
	778	Insufficient Logging	UNLOGGED_SECURITY_EXCEPTION

THE SYNOPSYS DIFFERENCE

Synopsys helps development teams 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 optimize security and quality in DevSecOps and throughout the software development life cycle.

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

SYNOPSYS®

185 Berry Street, Suite 6500

San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193

International Sales: +1 415.321.5237

Email: software-integrity-sales@synopsys.com