GRAMMATECH

OWASP 2017 TOP 10 CATEGORIES | MAPPED TO CODESONAR® 6.2

TRUSTED LEADERS OF SOFTWARE ASSURANCE AND ADVANCED CYBER-SECURITY SOLUTIONS

WWW.GRAMMATECH.COM

INTRODUCTION

Since 2001, the Open Web Application Security Project (OWASP) has been providing a top ten list of the most critical coding and security flaws in Web development.

This list is popularly recognized as a security standard for all Web development.

For more information on OWASP:

https://owasp.org/

The following table shows the CodeSonar warning classes that are associated with OWASP categories.

Note close and broad mappings are identical, thus only one chart below to reflect both close and broad mapping.

C# and Java classes are tagged. All other classes are C/C++.

OWASP Category ID & Name		CodeSonar 6.2 Class Name
OWASP-2017:A1	Injection	Code Injection (C#) Code Injection (Java) Command Injection Command Injection (C#) Command Injection (Java) DLL Injection (C#) DLL Injection (Java) DOS Injection (C#) DOS Injection (Java) Fragment Injection (Java) LDAP Injection Reflection Injection (C#) Reflection Injection (Java) SQL Injection SQL Injection (C#) SQL Injection (Java) Tainted @Trusted Value (C#) Tainted @Trusted Value (Java) Tainted Bundle (C#) Tainted Bundle (Java) Tainted Control (C#) Tainted Control (Java) Tainted Data in Vulnerable Method (Java) Tainted Expression Evaluation (C#) Tainted Expression Evaluation (Java) Tainted HTTP Response (C#) Tainted HTTP Response (Java) Tainted Hardware Device Property (C#) Tainted Hardware Device Property (Java) Tainted LDAP Attribute (C#) Tainted LDAP Attribute (Java) Tainted Log (C#) Tainted Log (Java) Tainted Message (C#) Tainted Message (Java)

		Tainted Network Address (C#) Tainted Network Address (Java) Tainted Path (C#) Tainted Path (Java) Tainted Regular Expression (C#) Tainted Regular Expression (Java) Tainted Resource (C#) Tainted Resource (Java) Tainted Session (C#) Tainted Session (Java) Tainted URL (C#) Tainted URL (Java) Tainted XAML (C#) Tainted XAML (Java) Tainted XML (C#) Tainted XML (Java) Tainted Xpath (C#) Tainted Xpath (Java) Untrusted Process Creation Use of system
OWASP-2017:A2	Broken authentication	Anonymous LDAP Authentication (C#) Anonymous LDAP Authentication (Java) Certificate Added to Root Store (C#) Certificate Added to Root Store (Java) Cryptographic Algorithm with Risky Default Cipher (C#) Cryptographic Algorithm with Risky Default Cipher (Java) Cryptographic Algorithm with Weak Cipher (C#) Cryptographic Algorithm with Weak Cipher (Java) Cryptographic Algorithm with Weak Hash (C#) Cryptographic Algorithm with Weak Hash (Java) Hardcoded Password (C#) Hardcoded Password (Java) Hostname in Condition (C#) Hostname in Condition (Java) Inadequate Salt (C#) Inadequate Salt (Java) Insecure Key Derivation (C#) Insecure Key Derivation (Java) Missing Authentication Annotation (C#) Missing Authentication Annotation (Java) Password in Property File (C#) Password in Property File (Java) Plaintext Storage of Password Risky Cipher Algorithm (C#) Risky Cipher Algorithm (Java) Risky Cipher Field (C#) Risky Cipher Field (Java)

		Risky Cryptographic Algorithm (C#) Risky Cryptographic Algorithm (Java) Risky Cryptographic Field (C#) Risky Cryptographic Field (Java) Security Annotation Conflict (C#) Security Annotation Conflict (Java) Unsafe Base64 Encoding (C#) Unsafe Base64 Encoding (Java) Use of crypt Weak Cryptographic Value (C#) Weak Cryptographic Value (Java) Weak Cryptography Weak Hash Algorithm (C#) Weak Hash Algorithm (Java) Weak Hash Algorithm Field (C#) Weak Hash Algorithm Field (Java)
OWASP-2017:A3	Sensitive data exposure	Android Message Injection (Java) Android URL Injection (Java) Encryption without Padding Plaintext Storage of Password Redundant Condition Sensitive Data Cached (Java) Sensitive Data Written to External Storage (Java) Sensitive Data Written to Local File (Java) Tainted Write Use of crypt Weak Cryptography
OWASP-2017:A4	XML external entities	Possible XML External Entity Reference (C#) Possible XML External Entity Reference (Java) Use of XML_ExternalEntityParserCreate
OWASP-2017:A5	Broken access control	Disabled Input Validation (C#) Disabled Input Validation (Java) Fragment Injection (Java) Hardcoded Authentication Hardcoded Crypto Key Hardcoded Crypto Salt Method Disables Security Setting (C#) Method Disables Security Setting (Java) Missing Authentication Annotation (C#) Missing Authentication Annotation (Java) Missing isValidFragment Override (Java) Null Security Descriptor Plaintext Storage of Password Security Annotation Conflict (C#) Security Annotation Conflict (Java) Tainted Data in Vulnerable Method (Java) Tainted Filename

		Tainted Write Use of AddAccessAllowedAce Use of AddAccessDeniedAce Use of crypt Use of cuserid Use of getlogin Weak Cryptography
OWASP-2017:A6	Security misconfiguration	Encryption without Padding Hardcoded Authentication Hardcoded Crypto Key Hardcoded Crypto Salt Hardcoded DNS Name Memory Protection Removal
OWASP-2017:A7	Cross site scripting (XSS)	Cross Site Scripting (C#) Cross Site Scripting (Java) Tainted Write
OWASP-2017:A8	Insecure deserialization	Addition Overflow of Allocation Size Addition Overflow of Size Buffer Overrun Buffer Underrun Deserializable Class (C#) Deserializable Class (Java) Deserializing Non-Serializable Class (C#) Deserializing Non-Serializable Class (Java) Integer Overflow of Allocation Size Multiplication Overflow of Allocation Size Multiplication Overflow of Size Pointer Before Beginning of Object Pointer Past End of Object Subtraction Underflow of Allocation Size Subtraction Underflow of Size Tainted Buffer Access Type Overrun Type Underrun
OWASP-2017:A9	Using components with known vulnerabilities	Deprecated Cryptography Provider (C#) Deprecated Cryptography Provider (Java) Deprecated Transfer Protocol (C#) Deprecated Transfer Protocol (Java) Use of AddAccessAllowedAce Use of AddAccessDeniedAce Use of AfxLoadLibrary Use of CoLoadLibrary Use of CreateFile Use of CreateProcess Use of CreateThread Use of FormatMessage Use of GetTempFileName

		Use of LoadLibrary Use of LoadModule Use of MoveFile Use of OemToAnsi Use of OemToChar Use of crypt Use of gets Use of mkstemp Use of mktemp Use of rand Use of rand48 Function Use of random Use of tmpfile Use of tmpnam Weak Cryptography
OWASP-2017:A10	Insufficient logging and monitoring	Not Enough Assertions

GrammaTech is a leading global provider of application testing (AST) solutions used by the world's most security conscious organizations to detect, measure, analyze and resolve vulnerabilities for software they develop or use. The company is also a trusted cybersecurity and artificial intelligence research partner for the nation's civil, defense, and intelligence agencies.