

NOTE: The CWE column contains the CWE IDs and Cx IDs. If the value is < 10000, it represents a CWE ID and if the value is >10 000, it represents a Cx ID.

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Apex	Apex_Force_com_Critical_Security_Risk	Stored_XSS	79		Critical	
Apex	Apex_Force_com_Critical_Security_Risk	Reflected_XSS	79		High	
Apex	Apex_Force_com_Critical_Security_Risk	SOQL_SOSL_Injection	89		High	
Apex	Apex_Force_com_Code_Quality	Use_of_Hard_Coded_Cryptographic_Key	321		Medium	
Apex	Apex_Force_com_Critical_Security_Risk	Resource_Injection	99		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	Cookies_Scoping	0		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	CRUD_Delete	472	Updated	Medium	Medium
Apex	Apex_Force_com_Serious_Security_Risk	CSRF	352		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	CSRF_With_VF_Call	352		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	Dangerous_Methods	243		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	Dereferenced_Field	0		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	FLS_Create	285	Updated	Medium	Medium
Apex	Apex_Force_com_Serious_Security_Risk	FLS_Create_Partial	285		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	FLS_Read	285		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	FLS_Update	285		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	FLS_Update_Partial	285		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	Frame_Spoofing	79		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	HttpSplitting	113		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	inputText_Ignoring_FLS	0		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	Insecure_Endpoint	319		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	Secure_Cookie_Flag_Not_Set	614		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	Sharing	472		Medium	
Apex	Apex_Force_com_Serious_Security_Risk	URL_Redirection_Attack	601		Medium	
Apex	Apex_Low_Visibility	Privacy_Violation	359		Medium	
Apex	Apex_Force_com_Code_Quality	Bulkify_Apex_Methods_Using_Collections_In_Methods	0		Low	
Apex	Apex_Low_Visibility	Compromised_CDN	0		Low	
Apex	Apex_Low_Visibility	Escape_False_Warning	0		Low	
Apex	Apex_Low_Visibility	Hardcoded_Password	259		Low	
Apex	Apex_Low_Visibility	Parameter_Tampering	472		Low	
Apex	Apex_Low_Visibility	Password_misuse	0		Low	
Apex	Apex_Low_Visibility	Potential_Frame_Injection	0		Low	
Apex	Apex_Low_Visibility	Potential_URL_Redirection_Attack	601		Low	
Apex	Apex_Low_Visibility	Second_Order_SOQL_SOSL_Injection	89		Low	
Apex	Apex_Low_Visibility	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327		Low	
Apex	Apex_Low_Visibility	Verbose_Error_Reporting	209		Low	
Apex	Apex_Force_com_Code_Quality	Async_Future_Method_Inside_Loops	0		Information	
Apex	Apex_Force_com_Code_Quality	DML_Statements_Inside_Loops	0		Information	
Apex	Apex_Force_com_Code_Quality	Hardcoded_Messages	547		Information	
Apex	Apex_Force_com_Code_Quality	Hardcoding_Ids	0		Information	
Apex	Apex_Force_com_Code_Quality	Hardcoding_Of_Trigger_New	0		Information	
Apex	Apex_Force_com_Code_Quality	Hardcoding_Of_Trigger_Old	0		Information	
Apex	Apex_Force_com_Code_Quality	Hardcoding_References_To_Static_Resources	0		Information	
Apex	Apex_Force_com_Code_Quality	HTTP_Callouts	0		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Apex	Apex_Force_com_Code_Quality	Multiple_Forms_In_Visualforce_Page	0		Information	
Apex	Apex_Force_com_Code_Quality	Multiple_Trigger_On_same_sObject	0		Information	
Apex	Apex_Force_com_Code_Quality	Queries_With_No_Where_Or_Limit_Clause	0		Information	
Apex	Apex_Force_com_Code_Quality	SOSL_SOQL_Statments_Inside_Loops	0		Information	
Apex	Apex_Force_com_Code_Quality	Test_Assert_Without_Message	0		Information	
Apex	Apex_Force_com_Code_Quality	Test_Methods_With_No_Assert	0		Information	
Apex	Apex_Force_com_Code_Quality	Unused_Variable	563		Information	
Apex	Apex_Force_com_Code_Quality	Use_Of_Ajax_Toolkit	0		Information	
Apex	Apex_ISV_Quality_Rules	ActionPoller_Frequency_Check	0		Information	
Apex	Apex_ISV_Quality_Rules	Ajax_Toolkit_From_VF	0		Information	
Apex	Apex_ISV_Quality_Rules	Batch_Apex_exists	0		Information	
Apex	Apex_ISV_Quality_Rules	Batch_Apex_makes_outbound_call	0		Information	
Apex	Apex_ISV_Quality_Rules	DmlOptions_Set_To_False	0		Information	
Apex	Apex_ISV_Quality_Rules	Empty_Catch_Blocks	0		Information	
Apex	Apex_ISV_Quality_Rules	Empty_IfStmt	0		Information	
Apex	Apex_ISV_Quality_Rules	Empty_Methods	0		Information	
Apex	Apex_ISV_Quality_Rules	Empty_WhileStmt	0		Information	
Apex	Apex_ISV_Quality_Rules	Find_Exposed_Test_Data	0		Information	
Apex	Apex_ISV_Quality_Rules	Future_exists	0		Information	
Apex	Apex_ISV_Quality_Rules	Old_API_Version	0		Information	
Apex	Apex_ISV_Quality_Rules	Outbound_Email_Send	0		Information	
Apex	Apex_ISV_Quality_Rules	Report_with_no_Filter	0		Information	
Apex	Apex_ISV_Quality_Rules	SOQL_Dynamic_null_in_Where	0		Information	
Apex	Apex_ISV_Quality_Rules	SOQL_Formula_in_Where	0		Information	
Apex	Apex_ISV_Quality_Rules	SOQL_Hardcoded_null_in_Where	1067		Information	
Apex	Apex_ISV_Quality_Rules	SOQL_Relationship_in_Where	1067		Information	
Apex	Apex_ISV_Quality_Rules	SOQL_With_All_Fields	0		Information	
Apex	Apex_ISV_Quality_Rules	SOQL_with_All_Fields_in_Loop	0		Information	
Apex	Apex_ISV_Quality_Rules	SOSL_With_Where_Clause	0		Information	
Apex	Apex_ISV_Quality_Rules	Warn_About_Viewstate_Size_Limit	0		Information	
Apex	Apex_ISV_Quality_Rules	Workflow_sends_Emails	0		Information	
ASP	ASP_Critical_Risk	Code_Injection	94		Critical	
ASP	ASP_Critical_Risk	Command_Injection	77		Critical	
ASP	ASP_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
ASP	ASP_Critical_Risk	SQL_Injection	89		Critical	
ASP	ASP_Critical_Risk	Stored_Code_Injection	94		Critical	
ASP	ASP_Critical_Risk	Stored_XSS	79		Critical	
ASP	ASP_High_Risk	Connection_String_Injection	99		High	
ASP	ASP_High_Risk	Dangerous_File_Extension	434		High	
ASP	ASP_High_Risk	LDAP_Injection	90		High	
ASP	ASP_High_Risk	Path_Traversal	22		High	
ASP	ASP_High_Risk	Reflected_XSS	79		High	
ASP	ASP_Medium_Threat	CSRF	352		Medium	
ASP	ASP_Medium_Threat	DoS_by_Sleep	606		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
ASP	ASP_Medium_Threat	Hardcoded_password_in_Connection_String	547		Medium	
ASP	ASP_Medium_Threat	Improper_Locking	667		Medium	
ASP	ASP_Medium_Threat	Insufficiently_Protected_Credentials	522		Medium	
ASP	ASP_Medium_Threat	Open_Redirect	601		Medium	
ASP	ASP_Medium_Threat	Parameter_Tampering	472		Medium	
ASP	ASP_Medium_Threat	Privacy_Violation	359		Medium	
ASP	ASP_Medium_Threat	Resource_Injection	99		Medium	
ASP	ASP_Medium_Threat	SQL_Injection_Evasion_Attack	89		Medium	
ASP	ASP_Medium_Threat	Untrusted_Activex	618		Medium	
ASP	ASP_Medium_Threat	Use_of_Hard_coded_Cryptographic_Key	321		Medium	
ASP	ASP_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
ASP	ASP_Medium_Threat	XPath_Injection	643		Medium	
ASP	ASP_Low_Visibility	Client_Side_Only_Validation	602		Low	
ASP	ASP_Low_Visibility	Compromised_CDN	0		Low	
ASP	ASP_Low_Visibility	Impersonation_Issue	520		Low	
ASP	ASP_Low_Visibility	Improper_Exception_Handling	248		Low	
ASP	ASP_Low_Visibility	Improper_Resource_Shutdown_or_Release	404		Low	
ASP	ASP_Low_Visibility	Improper_Session_Management	201		Low	
ASP	ASP_Low_Visibility	Improper_Transaction_Handling	460		Low	
ASP	ASP_Low_Visibility	Information_Exposure_Through_an_Error_Message	209		Low	
ASP	ASP_Low_Visibility	Information_Leak_Through_Persistent_Cookies	539		Low	
ASP	ASP_Low_Visibility	Insecure_Randomness	338		Low	
ASP	ASP_Low_Visibility	Leaving_Temporary_Files	377		Low	
ASP	ASP_Low_Visibility	Log_Forging	117		Low	
ASP	ASP_Low_Visibility	Script_Poisoning	20		Low	
ASP	ASP_Low_Visibility	Server_Code_In_Client_Comment	615		Low	
ASP	ASP_Low_Visibility	Session_Clearing_Problems	613		Low	
ASP	ASP_Low_Visibility	Thread_Safety_Issue	567		Low	
ASP	ASP_Low_Visibility	Trust_Boundary_Violation_in_Session_Variables	501		Low	
ASP	ASP_Low_Visibility	URL_Canonicalization_Issue	647		Low	
ASP	ASP_Best_Coding_Practice	Aptca_Methods_Call_Non_Aptca_Methods	0		Information	
ASP	ASP_Best_Coding_Practice	Empty_Catch	390		Information	
ASP	ASP_Best_Coding_Practice	Hardcoded_Absolute_Path	426		Information	
ASP	ASP_Best_Coding_Practice	Hardcoded_Connection_String	798		Information	
ASP	ASP_Best_Coding_Practice	Just_One_of_Equals_and_Hash_code_Defined	581		Information	
ASP	ASP_Best_Coding_Practice	Missing_XML_Validation	112		Information	
ASP	ASP_Best_Coding_Practice	NULL_Argument_to_Equals	0		Information	
ASP	ASP_Best_Coding_Practice	Pages_Without_Global_Error_Handler	544		Information	
ASP	ASP_Best_Coding_Practice	PersistSecurityInfo_is_True	0		Information	
ASP	ASP_Best_Coding_Practice	Sockets_in_WebApp	246		Information	
ASP	ASP_Best_Coding_Practice	Threads_in_WebApp	383		Information	
ASP	ASP_Best_Coding_Practice	Unclosed_Objects	459		Information	
ASP	ASP_Best_Coding_Practice	Unvalidated_Arguments_Of_Public_Methods	0		Information	
ASP	ASP_Best_Coding_Practice	Use_of_System_Output_Stream	117		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
ASP	ASP_Best_Coding_Practice	Visible_Fields	0		Information	
Cobol	Cobol_Critical_Risk	Command_Injection	77		Critical	
Cobol	Cobol_Critical_Risk	Sql_Injection	89		Critical	
Cobol	Cobol_High_Risk	Module_Injection	94		High	
Cobol	Cobol_High_Risk	Path_Traversal	22		High	
Cobol	Cobol_High_Risk	Reflected_XSS	79		High	
Cobol	Cobol_Medium_Threat	Ignored_Error_Conditions	754		Medium	
Cobol	Cobol_Medium_Threat	Resource_Injection	99		Medium	
Cobol	Cobol_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
Cobol	Cobol_Low_Visibility	Compromised_CDN	0		Low	
Cobol	Cobol_Low_Visibility	Debug_Enabled	489		Low	
Cobol	Cobol_Low_Visibility	Dynamic_Module_Invocation	0		Low	
Cobol	Cobol_Low_Visibility	Information_Leak_Through_Comments	615		Low	
Cobol	Cobol_Best_Coding_Practices	Dynamic_SQL_Queries	89		Information	
Cobol	Cobol_Best_Coding_Practices	SQL_Select_Without_Where	0		Information	
Cobol	Cobol_Best_Coding_Practices	Use_of_Display	0		Information	
CPP	CPP_Buffer_Overflow	Buffer_Improper_Index_Access	129		Critical	
CPP	CPP_Buffer_Overflow	Buffer_Overflow_cin	120		Critical	
CPP	CPP_Buffer_Overflow	Buffer_Overflow_LongString	120		Critical	
CPP	CPP_Buffer_Overflow	Buffer_Overflow_Unbounded_Buffer	120		Critical	
CPP	CPP_Buffer_Overflow	Buffer_Overflow_Unbounded_Format	120		Critical	
CPP	CPP_Buffer_Overflow	Buffer_Overflow_Wrong_Buffer_Size	131	Updated	Critical	
CPP	CPP_Buffer_Overflow	Open_SSL_HeartBleed	120		Critical	
CPP	CPP_Critical_Risk	CGI_Stored_XSS	79		Critical	
CPP	CPP_Critical_Risk	Command_Injection	77		Critical	
CPP	CPP_Critical_Risk	SQL_Injection	89		Critical	
CPP	CPP_Stored_Vulnerabilities	Second_Order_SQL_Injection	89		Critical	
CPP	CPP_Stored_Vulnerabilities	Stored_Command_Injection	77		Critical	
CPP	CPP_Buffer_Overflow	Buffer_Overflow_AddressOfLocalVarReturned	562		High	
CPP	CPP_Buffer_Overflow	Buffer_Overflow_boundedcpy2	120		High	
CPP	CPP_Buffer_Overflow	Format_String_Attack	134		High	
CPP	CPP_Buffer_Overflow	Improper_Null_Termination	170		High	
CPP	CPP_Buffer_Overflow	Off_by_One_Error	193		High	
CPP	CPP_High_Risk	CGI_Reflected_XSS	79		High	
CPP	CPP_High_Risk	Connection_String_Injection	99		High	
CPP	CPP_High_Risk	Download_of_Code_Without_Integrity_Check	494		High	
CPP	CPP_High_Risk	LDAP_Injection	90		High	
CPP	CPP_High_Risk	Path_Traversal	22		High	
CPP	CPP_High_Risk	Process_Control	114		High	
CPP	CPP_High_Risk	Sensitive_Information_Exposure_in_Cleartext_Channel	319		High	
CPP	CPP_High_Risk	Use_After_Free	416	Updated	High	High
CPP	CPP_Insecure_Credential_Storage	Observable_Time_Discrepancy	208		High	
CPP	CPP_Stored_Vulnerabilities	Stored_Connection_String_Injection	99		High	
CPP	CPP_Stored_Vulnerabilities	Stored_LDAP_Injection	90		High	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
CPP	CPP_Stored_Vulnerabilities	Stored_Path_Traversal	22		High	
CPP	CPP_Buffer_Overflow	MultiByte_String_Length	135		Medium	
CPP	CPP_Insecure_Credential_Storage	Insecure_Scrypt_Parameters	522		Medium	
CPP	CPP_Insecure_Credential_Storage	Insufficient_BCrypt_Cost	522		Medium	
CPP	CPP_Insecure_Credential_Storage	Insufficient_Output_Length	522		Medium	
CPP	CPP_Insecure_Credential_Storage	PBKDF2_Insufficient_Iteration_Count	522		Medium	
CPP	CPP_Insecure_Credential_Storage	PBKDF2_Weak_Salt_Value	522		Medium	
CPP	CPP_Insecure_Credential_Storage	Scrypt_Weak_Salt_Value	522		Medium	
CPP	CPP_Insecure_Credential_Storage	Weak_Mechanism	522		Medium	
CPP	CPP_Integer_Overflow	Float_Overflow	190		Medium	
CPP	CPP_Integer_Overflow	Integer_Overflow	190		Medium	
CPP	CPP_Integer_Overflow	Type_Conversion_Error	681		Medium	
CPP	CPP_Medium_Threat	Dangerous_Functions	242	Updated	Medium	Medium
CPP	CPP_Medium_Threat	Divide_By_Zero	369		Medium	
CPP	CPP_Medium_Threat	DoS_by_Sleep	606		Medium	
CPP	CPP_Medium_Threat	Double_Free	415	Updated	Medium	Medium
CPP	CPP_Medium_Threat	Environment_Variable_Injection	15		Medium	
CPP	CPP_Medium_Threat	Hardcoded_password_in_Connection_String	547		Medium	
CPP	CPP_Medium_Threat	Improper_Container_Access	824	Updated	Medium	Medium
CPP	CPP_Medium_Threat	Improper_Resource_Access_Authorization	863		Medium	
CPP	CPP_Medium_Threat	Inadequate_Encryption_Strength	326		Medium	
CPP	CPP_Medium_Threat	Insufficiently_Protected_Credentials	522		Medium	
CPP	CPP_Medium_Threat	Memory_Leak	401	Updated	Medium	Medium
CPP	CPP_Medium_Threat	MemoryFree_on_StackVariable	590		Medium	
CPP	CPP_Medium_Threat	Parameter_Tampering	472		Medium	
CPP	CPP_Medium_Threat	Plaintext_Storage_Of_A_Password	256		Medium	
CPP	CPP_Medium_Threat	Pointer_Subtraction_Determines_Size	469		Medium	
CPP	CPP_Medium_Threat	Privacy_Violation	359		Medium	
CPP	CPP_Medium_Threat	Reliance_on_Reverse_DNS_Lookups_in_an_Action	350		Medium	
CPP	CPP_Medium_Threat	Resource_Injection	99		Medium	
CPP	CPP_Medium_Threat	Server_Information_Exposure	497		Medium	
CPP	CPP_Medium_Threat	Setting_Manipulation	15		Medium	
CPP	CPP_Medium_Threat	Uncontrolled_Recursion	674		Medium	
CPP	CPP_Medium_Threat	Use_of_a_One_Way_Hash_without_a_Salt	759		Medium	
CPP	CPP_Medium_Threat	Use_of_Hard_coded_Cryptographic_Key	321		Medium	
CPP	CPP_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
CPP	CPP_Medium_Threat	Use_of_Uninitialized_Variable	457		Medium	
CPP	CPP_Medium_Threat	Wrong_Memory_Allocation	131		Medium	
CPP	CPP_Stored_Vulnerabilities	Stored_DoS_by_Sleep	730		Medium	
CPP	CPP_Stored_Vulnerabilities	Stored_Environment_Variable_Injection	15		Medium	
CPP	CPP_Stored_Vulnerabilities	Stored_Parameter_Tampering	472		Medium	
CPP	CPP_Stored_Vulnerabilities	Stored_Process_Control	114		Medium	
CPP	CPP_Stored_Vulnerabilities	Stored_Resource_Injection	99		Medium	
CPP	CPP_Weak_Cryptography	Asymmetric_Encryption_Improper_Padding	326		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
CPP	CPP_Weak_Cryptography	Asymmetric_Encryption_Insufficient_Key_Size	326		Medium	
CPP	CPP_Weak_Cryptography	Asymmetric_Encryption_RSA_Low_Public_Exponent	326		Medium	
CPP	CPP_Weak_Cryptography	Encoding_Used_Instead_of_Encryption	326		Medium	
CPP	CPP_Weak_Cryptography	Hashing_Length_Extension_Attack	326		Medium	
CPP	CPP_Weak_Cryptography	Personal_Information_Without_Encryption	326		Medium	
CPP	CPP_Weak_Cryptography	Symmetric_Encryption_Insecure_Cipher_Mode	326		Medium	
CPP	CPP_Weak_Cryptography	Symmetric_Encryption_Insecure_Predictable_IV	326		Medium	
CPP	CPP_Weak_Cryptography	Symmetric_Encryption_Insecure_Predictable_Key	326		Medium	
CPP	CPP_Weak_Cryptography	Symmetric_Encryption_Insecure_Static_IV	326		Medium	
CPP	CPP_Weak_Cryptography	Symmetric_Encryption_Insecure_Static_Key	326		Medium	
CPP	CPP_Weak_Cryptography	Use_Of_Weak_Hashing_Primitive	326		Medium	
CPP	CPP_Low_Visibility	Arithmetic_Operation_On_Boolean	480		Low	
CPP	CPP_Low_Visibility	Compromised_CDN	0		Low	
CPP	CPP_Low_Visibility	Creation_of_chroot_Jail_without_Changing_Working_Directory	243		Low	
CPP	CPP_Low_Visibility	Deprecated_Functions_or_Properties	0		Low	
CPP	CPP_Low_Visibility	Heap_Inspection	244		Low	
CPP	CPP_Low_Visibility	Improper_Exception_Handling	248		Low	
CPP	CPP_Low_Visibility	Improper_Resource_Shutdown_or_Release	404		Low	
CPP	CPP_Low_Visibility	Improper_Transaction_Handling	460		Low	
CPP	CPP_Low_Visibility	Improperly_Locked_Memory	591		Low	
CPP	CPP_Low_Visibility	Inconsistent_Implementations	474		Low	
CPP	CPP_Low_Visibility	Incorrect_Permission_Assignment_For_File_System_Resources	732		Low	
CPP	CPP_Low_Visibility	Information_Exposure_Through_an_Error_Message	209		Low	
CPP	CPP_Low_Visibility	Information_Exposure_Through_Comments	615		Low	
CPP	CPP_Low_Visibility	Insecure_Temporary_File	377		Low	
CPP	CPP_Low_Visibility	Leaving_Temporary_Files	377		Low	
CPP	CPP_Low_Visibility	Log_Forging	117		Low	
CPP	CPP_Low_Visibility	NULL_Pointer_Dereference	476		Low	
CPP	CPP_Low_Visibility	Race_Condition_In_Cross_Functionality	362		Low	
CPP	CPP_Low_Visibility	TOCTOU	367		Low	
CPP	CPP_Low_Visibility	Unchecked_Array_Index	129		Low	
CPP	CPP_Low_Visibility	Unchecked_Return_Value	252		Low	
CPP	CPP_Low_Visibility	Undefined_Behavior	475		Low	
CPP	CPP_Low_Visibility	Unreleased_Resource_Leak	411		Low	
CPP	CPP_Low_Visibility	Use_Of_Deprecated_Class	477		Low	
CPP	CPP_Low_Visibility	Use_of_Insufficiently_Random_Values	338		Low	
CPP	CPP_Low_Visibility	Use_of_Obsolete_Functions	477		Low	
CPP	CPP_Low_Visibility	Use_of_Sizeof_On_a_Pointer_Type	467		Low	
CPP	CPP_Stored_Vulnerabilities	Stored_Log_Forging	117		Low	
CPP	CPP_Weak_Cryptography	Weak_Randomness_Biased_Random_Sample	338		Low	
CPP	CPP_Best_Coding_Practice	Buffer_Size_Literal	121		Information	
CPP	CPP_Best_Coding_Practice	Buffer_Size_Literal_Condition	121		Information	
CPP	CPP_Best_Coding_Practice	Buffer_Size_Literal_Overflow	121		Information	
CPP	CPP_Best_Coding_Practice	Dead_Code	561		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
CPP	CPP_Best_Coding_Practice	Declaration_Of_Catch_For_Generic_Exception	396		Information	
CPP	CPP_Best_Coding_Practice	Detection_of_Error_Condition_Without_Action	390		Information	
CPP	CPP_Best_Coding_Practice	Empty_Methods	0		Information	
CPP	CPP_Best_Coding_Practice	Exposure_of_Resource_to_Wrong_Sphere	493		Information	
CPP	CPP_Best_Coding_Practice	GOTO_Statement	0		Information	
CPP	CPP_Best_Coding_Practice	Hardcoded_Absolute_Path	426		Information	
CPP	CPP_Best_Coding_Practice	Magic_Numbers	0		Information	
CPP	CPP_Best_Coding_Practice	Methods_Without_ReturnType	0		Information	
CPP	CPP_Best_Coding_Practice	Non_Private_Static_Constructors	0		Information	
CPP	CPP_Best_Coding_Practice	Reliance_On_Untrusted_Inputs_In_Security_Decision	807		Information	
CPP	CPP_Best_Coding_Practice	Unused_Variable	563		Information	
CPP	CPP_Best_Coding_Practice	Unvalidated_Arguments_Of_Public_Methods	0		Information	
CPP	CPP_MISRA_C	R02_02_CPP_Comment_Style	0		Information	
CPP	CPP_MISRA_C	R02_03_Nested_Comments	0		Information	
CPP	CPP_MISRA_C	R02_04_Code_Commented_Out	0		Information	
CPP	CPP_MISRA_C	R03_04_Not_Explained_Pragma_Usage	0		Information	
CPP	CPP_MISRA_C	R04_01_Non_ISO_Escape_Sequences	0		Information	
CPP	CPP_MISRA_C	R04_02_Trigraphs	0		Information	
CPP	CPP_MISRA_C	R05_01_Identifiers_Length_Violation	0		Information	
CPP	CPP_MISRA_C	R05_02_Identifiers_Hiding_Outer_Scope_Identifiers	0		Information	
CPP	CPP_MISRA_C	R05_03_Typedef_Name_Reused	0		Information	
CPP	CPP_MISRA_C	R05_04_Tag_Name_Reused	0		Information	
CPP	CPP_MISRA_C	R05_05_Identifier_With_Static_Storage_Reused	0		Information	
CPP	CPP_MISRA_C	R05_07_Identifier_Name_Reused	0		Information	
CPP	CPP_MISRA_C	R06_01_Plain_Char_Type_Usage	0		Information	
CPP	CPP_MISRA_C	R06_02_Not_Plain_Char_Type_Usage	0		Information	
CPP	CPP_MISRA_C	R06_03_Non_Typedefd_Basic_Types	0		Information	
CPP	CPP_MISRA_C	R06_04_Bit_Fields_Type	0		Information	
CPP	CPP_MISRA_C	R06_05_Bit_Fields_Length	0		Information	
CPP	CPP_MISRA_C	R07_01_Non_Zero-Octal_Constant	0		Information	
CPP	CPP_MISRA_C	R08_03_Identical_Function_Decl_Def	0		Information	
CPP	CPP_MISRA_C	R08_05_Object_Function_In_Header_File	0		Information	
CPP	CPP_MISRA_C	R08_07_Block_Scope_Obj_If_Used_By_Single_Function	0		Information	
CPP	CPP_MISRA_C	R08_08_External_Objects_Declared_Once	0		Information	
CPP	CPP_MISRA_C	R09_03_Initializing_Non_First_And_Not_All_Members_In_Enum	0		Information	
CPP	CPP_MISRA_C	R10_06_U_Suffix_Not_Applied_To_Unsigned_Const	0		Information	
CPP	CPP_MISRA_C	R12_05_AND_OR_Operands_Not_As_Primary_Expressions	0		Information	
CPP	CPP_MISRA_C	R12_07_Bitwise_Operator_On_Signed_Type	0		Information	
CPP	CPP_MISRA_C	R12_09_Unary_Minus_Operator_On_Unsigned_Type	0		Information	
CPP	CPP_MISRA_C	R12_10_Comma_Operator_Used	0		Information	
CPP	CPP_MISRA_C	R12_12_Floating_Point_Bit_Underlying_Representation_Used	0		Information	
CPP	CPP_MISRA_C	R12_13_Using_Of_Incremental_And_Decremental_Operators	0		Information	
CPP	CPP_MISRA_C	R13_01_Assignment_Operators_In_Boolean_Expressions	0		Information	
CPP	CPP_MISRA_C	R13_03_Floating_Point_Equality_Or_Inequality	0		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
CPP	CPP_MISRA_C	R13_04_Floating_Points_Objects_In_For_Control	0		Information	
CPP	CPP_MISRA_C	R13_06_Loop_Iterator_Modified_In_Loop_Body	0		Information	
CPP	CPP_MISRA_C	R14_04_Use_Of_Goto	0		Information	
CPP	CPP_MISRA_C	R14_05_Use_Of_Continue	0		Information	
CPP	CPP_MISRA_C	R14_06_Multiple_Breaks_In_Iteration_Statement	0		Information	
CPP	CPP_MISRA_C	R14_07_Single_Point_Exit_At_Function_End	0		Information	
CPP	CPP_MISRA_C	R14_08_Not_Compound_Switch_Or_Iteration_Statement	0		Information	
CPP	CPP_MISRA_C	R14_09_Not_Compound_If_Or_Else	0		Information	
CPP	CPP_MISRA_C	R14_10_If_Else_If_Not_Ending_With_Else	0		Information	
CPP	CPP_MISRA_C	R15_01_Case_Not_Enclosed_By_Compound_Switch	0		Information	
CPP	CPP_MISRA_C	R15_02_Non_Empty_Switch_Clause_Without_Break	0		Information	
CPP	CPP_MISRA_C	R15_03_Non_Default_Final_Clause_In_Switch_Statement	0		Information	
CPP	CPP_MISRA_C	R15_05_No_Cases_in_Switch_Statement	0		Information	
CPP	CPP_MISRA_C	R16_01_Function_With_Variable_Number_Of_Arguments	0		Information	
CPP	CPP_MISRA_C	R16_02_Recursion_Exists	0		Information	
CPP	CPP_MISRA_C	R16_03_Function_Prototype_Without_Identifiers	0		Information	
CPP	CPP_MISRA_C	R16_04_Different_Identifiers_In_Function_Definition_And_Prototype	0		Information	
CPP	CPP_MISRA_C	R16_05_Function_Prototype_Declaration_Without_Parameters	0		Information	
CPP	CPP_MISRA_C	R16_06_Function_Invoke_Arg_Number_Not_Match_Function_Def_Number	0		Information	
CPP	CPP_MISRA_C	R16_07_Parameter_Pointer_To_Const_Where_Not_Modified	0		Information	
CPP	CPP_MISRA_C	R16_08_Non_Explicit_Return_Statement_In_Non_Void_Function	0		Information	
CPP	CPP_MISRA_C	R16_09_Using_Function_Identifier_Not_Call_Or_Pointer	0		Information	
CPP	CPP_MISRA_C	R18_04_Use_Of_Union	0		Information	
CPP	CPP_MISRA_C	R19_01_Non_Preprocessor_Command_Before_Include_In_File	0		Information	
CPP	CPP_MISRA_C	R19_02_Non_Standard_Chars_In_Header_File_Name	0		Information	
CPP	CPP_MISRA_C	R19_03_Include_Directive_In_Wrong_Format	0		Information	
CPP	CPP_MISRA_C	R19_05_Using_Define_Or_Undef_Directive_In_Block	0		Information	
CPP	CPP_MISRA_C	R19_06_Use_Of_Undef_Directive	0		Information	
CPP	CPP_MISRA_C	R19_12_Multiple_Pound_Or_Double_Pound_In_Same_Macro	0		Information	
CPP	CPP_MISRA_C	R19_13_Pound_Preprocessor_Operator_Is_Used	0		Information	
CPP	CPP_MISRA_C	R19_17_Preprocessor_If_And_Else_Operators_Reside_In_Different_Files	0		Information	
CPP	CPP_MISRA_C	R20_05_Using_Errno_Indicator_From_Errno_H	0		Information	
CPP	CPP_MISRA_C	R20_06_Using_Offsetof_Macro_From_Stddef_H	0		Information	
CPP	CPP_MISRA_C	R20_07_Using_Setjmp_Longjmp_Macros_From_Setjmp_H	0		Information	
CPP	CPP_MISRA_C	R20_08_Using_Signal_Handling_From_Signal_H	0		Information	
CPP	CPP_MISRA_C	R20_09_Using_Input_Output_From_Stdio_H	0		Information	
CPP	CPP_MISRA_C	R20_10_Using_Atof_Atoi_Atoll_Functions_From_Stdlib_H	0		Information	
CPP	CPP_MISRA_C	R20_11_Using_Abort_Exit_Getenv_System_Functions_From_Stdlib_H	0		Information	
CPP	CPP_MISRA_C	R20_12_Using_Time_Handling_From_Time_H	0		Information	
CPP	CPP_MISRA_C_2012	R01_04_Emergent_Features_Shall_Not_Be_Used	0		Information	
CPP	CPP_MISRA_C_2012	R02_X_Unused_Code	0		Information	
CPP	CPP_MISRA_C_2012	R03_X_Comments	0		Information	
CPP	CPP_MISRA_C_2012	R04_X_Character_Sets	0		Information	
CPP	CPP_MISRA_C_2012	R05_X_Identifier	0		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
CPP	CPP_MISRA_C_2012	R06_X_Bitfields	0		Information	
CPP	CPP_MISRA_C_2012	R07_01_Octal_Constants_Shall_Not_Used	0		Information	
CPP	CPP_MISRA_C_2012	R07_02_U_Or_u_Suffix_Shall_Be_Applied_To_All_Unsigned_Type_Integers	0		Information	
CPP	CPP_MISRA_C_2012	R07_03_Lowercase_l_Shall_Not_Used_In_A_Literal_Suffix	0		Information	
CPP	CPP_MISRA_C_2012	R07_04_String_Literal_Should_Be_Assigned_To_Pointer_To_Const_Char	0		Information	
CPP	CPP_MISRA_C_2012	R08_02_Function_Prototype_With_Named_Parameters	0		Information	
CPP	CPP_MISRA_C_2012	R08_03_Functions_Have_Same_Name	0		Information	
CPP	CPP_MISRA_C_2012	R08_04_Compatible_Declaration_Shall_Be_Visible	0		Information	
CPP	CPP_MISRA_C_2012	R08_05_External_Objects_Shall_Be_Declared_Once	0		Information	
CPP	CPP_MISRA_C_2012	R08_06_Single_External_Definition_Per_External_Identifier	0		Information	
CPP	CPP_MISRA_C_2012	R08_07_Function_And_Objects_Should_Not_Use_Extern_When_Referenced_In_One_File	0		Information	
CPP	CPP_MISRA_C_2012	R08_08_Static_Shall_Be_Used_In_All_Internal_Linkage_Declarations	0		Information	
CPP	CPP_MISRA_C_2012	R08_09_Identifiers_Should_Be_Defined_At_Block_Scope	0		Information	
CPP	CPP_MISRA_C_2012	R08_10_Inline_Function_Shall_Be_Declared_With_Static	0		Information	
CPP	CPP_MISRA_C_2012	R08_11_Extern_Array_Shall_Be_Declared_With_Determined_Size	0		Information	
CPP	CPP_MISRA_C_2012	R08_12_Value_Implicitly_Specified_Of_Enumeration_Constant_Shall_Be_Unique	0		Information	
CPP	CPP_MISRA_C_2012	R08_13_Pointer_Should_Point_Const	0		Information	
CPP	CPP_MISRA_C_2012	R08_14_Restrict_Type_Qualifier	0		Information	
CPP	CPP_MISRA_C_2012	R09_01_Value_Not_Read_Before_Being_Set	0		Information	
CPP	CPP_MISRA_C_2012	R09_02_to_03_Array_Initializer_Validation	0		Information	
CPP	CPP_MISRA_C_2012	R10_01_Operands_Shall_Not_Be_Of_An_Inappropriate_Essential_Type	0		Information	
CPP	CPP_MISRA_C_2012	R10_02_Char_Type_Shall_Not_Be_Used_Inappropriately_In_Operations	0		Information	
CPP	CPP_MISRA_C_2012	R10_03_Value_Of_An_Expression_Assigned_To_Inappropriate_Essential_Type	0		Information	
CPP	CPP_MISRA_C_2012	R10_04_Binary_Operator_Operands_With_Same_Type	0		Information	
CPP	CPP_MISRA_C_2012	R10_05_Value_Of_An_Expression_Cast_To_Inappropriate_Essential_Type	0		Information	
CPP	CPP_MISRA_C_2012	R10_06_to_08_Composite_Expressions	0		Information	
CPP	CPP_MISRA_C_2012	R11_X_Pointer_Type_Conversions	0		Information	
CPP	CPP_MISRA_C_2012	R12_01_Explicit_Operator_Precedence	0		Information	
CPP	CPP_MISRA_C_2012	R12_02_Right_Operand_Of_Shift_Operator_Out_Of_Range	0		Information	
CPP	CPP_MISRA_C_2012	R12_03_Comma_Operator_Shall_Not_Used	0		Information	
CPP	CPP_MISRA_C_2012	R12_04_Unsigned_Integer_Wrap_Around	0		Information	
CPP	CPP_MISRA_C_2012	R12_05_Sizeof_Operand_Not_Array_Of_Type	0		Information	
CPP	CPP_MISRA_C_2012	R13_X_Side_Effects	0		Information	
CPP	CPP_MISRA_C_2012	R14_X_Control_Statement_Expressions	0		Information	
CPP	CPP_MISRA_C_2012	R15_01_to_03_Goto_Usage_Constraints	0		Information	
CPP	CPP_MISRA_C_2012	R15_04_Iteration_Single_Exit_Point	0		Information	
CPP	CPP_MISRA_C_2012	R15_05_Function_Single_Exit_Point	0		Information	
CPP	CPP_MISRA_C_2012	R15_06_Statement_Body_Shall_Be_Compound	0		Information	
CPP	CPP_MISRA_C_2012	R15_07_If_Else_If_Constructs_Not_Ending_With_Else	0		Information	
CPP	CPP_MISRA_C_2012	R16_X_Switches	0		Information	
CPP	CPP_MISRA_C_2012	R17_01_StdArg_Shall_Not_Used	0		Information	
CPP	CPP_MISRA_C_2012	R17_02_No_Recursion	0		Information	
CPP	CPP_MISRA_C_2012	R17_03_Function_Shall_Not_Be_Declared_Implicitly	0		Information	
CPP	CPP_MISRA_C_2012	R17_04_Non_Void_Has_Valid_Return	0		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
CPP	CPP_MISRA_C_2012	R17_05_to_06_Functions_With_Array_Parameter	0		Information	
CPP	CPP_MISRA_C_2012	R17_07_Value_Returned_By_Non_Void_Function_Shall_Be_Used	0		Information	
CPP	CPP_MISRA_C_2012	R17_08_Function_Parameter_Should_Not_Be_Modified	0		Information	
CPP	CPP_MISRA_C_2012	R18_04_Pointer_Arithmetic	0		Information	
CPP	CPP_MISRA_C_2012	R18_05_Pointer_Nesting	0		Information	
CPP	CPP_MISRA_C_2012	R18_06_Automatic_Storage_Addresses_Shall_Not_Be_Copied	0		Information	
CPP	CPP_MISRA_C_2012	R18_07_to_08_Variable_Length_And_Flexible_Arrays	0		Information	
CPP	CPP_MISRA_C_2012	R19_X_Overlapping_Storage	0		Information	
CPP	CPP_MISRA_C_2012	R20_01_Include_Directive_Precedence	0		Information	
CPP	CPP_MISRA_C_2012	R20_02_Invalid_Include_Names	0		Information	
CPP	CPP_MISRA_C_2012	R20_03_Includes_In_Wrong_Format	0		Information	
CPP	CPP_MISRA_C_2012	R20_04_Macros_With_Keyword_Name	0		Information	
CPP	CPP_MISRA_C_2012	R20_05_Undef_Shall_Not_Be_Used	0		Information	
CPP	CPP_MISRA_C_2012	R20_10_to_12_Preprocessor_Concatenation_Operations	0		Information	
CPP	CPP_MISRA_C_2012	R20_13_Valid_PreProcessor_Directives	0		Information	
CPP	CPP_MISRA_C_2012	R20_14_Preprocessor_IF_Else_In_Same_File	0		Information	
CPP	CPP_MISRA_C_2012	R21_01_to_12_Usage_of_C_Standard_Library	0		Information	
CPP	CPP_MISRA_C_2012	R21_13_to_20_C_Standard_Library_Types	0		Information	
CPP	CPP_MISRA_C_2012	R22_X_Resources	0		Information	
CPP	CPP_MISRA_CPP	R00_01_03_Find_Unused_Variables	10775		Information	
CPP	CPP_MISRA_CPP	R00_01_05_Find_Unused_Typedefs	10776		Information	
CPP	CPP_MISRA_CPP	R00_01_10_Find_Unused_Defined_Functions	10777		Information	
CPP	CPP_MISRA_CPP	R00_01_11_Find_Unused_Parameters	10778		Information	
CPP	CPP_MISRA_CPP	R00_01_12_Find_Virtual_Unused_Parameters	10779		Information	
CPP	CPP_MISRA_CPP	R02_03_01_Trigraphs	0		Information	
CPP	CPP_MISRA_CPP	R02_05_01_Digraphs	10750		Information	
CPP	CPP_MISRA_CPP	R02_07_02_Code_Commented_Out	0		Information	
CPP	CPP_MISRA_CPP	R02_07_03_Code_CPP_Commented_Out	0		Information	
CPP	CPP_MISRA_CPP	R02_10_02_Identifiers_Hide_Outer_Scope_Identifiers	0		Information	
CPP	CPP_MISRA_CPP	R02_10_03_Typedef_Name_Reused	0		Information	
CPP	CPP_MISRA_CPP	R02_10_04_Class_Enum_Union_Names_Reused	0		Information	
CPP	CPP_MISRA_CPP	R02_10_05_Non_Member_Static_Name_Reuse	10751		Information	
CPP	CPP_MISRA_CPP	R02_13_01_Non_ISO_Escapes	0		Information	
CPP	CPP_MISRA_CPP	R02_13_02_Non_Zero-Octal_Constant	0		Information	
CPP	CPP_MISRA_CPP	R02_13_03_U_Suffix_Not_Applied_To_Unsigned_Hex-Oct	0		Information	
CPP	CPP_MISRA_CPP	R02_13_04_Literal_Suffix_Uppercase	10780		Information	
CPP	CPP_MISRA_CPP	R03_01_03_Find_Arrays_Without_Size	10781		Information	
CPP	CPP_MISRA_CPP	R03_02_01_Identical_Function_and_Object_Decl_Def	0		Information	
CPP	CPP_MISRA_CPP	R03_04_01_Obj_Defined_Outside_Minimal_Scope	0		Information	
CPP	CPP_MISRA_CPP	R03_09_02_Non_Typedef_Basic_Types	0		Information	
CPP	CPP_MISRA_CPP	R04_10_01_NULL_As_An_Integer_Value	0		Information	
CPP	CPP_MISRA_CPP	R04_10_02_Literal_Zero_As_Null_Pointer_Constant	0		Information	
CPP	CPP_MISRA_CPP	R05_00_07_Improper_Explicit_Floating_Integral_Conversion_Of_Expression	0		Information	
CPP	CPP_MISRA_CPP	R05_00_10_Bitwise_Operator_On_Unsigned_Char_Short_Types	0		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
CPP	CPP_MISRA_CPP	R05_00_11_Plain_Char_Type_Usage	0		Information	
CPP	CPP_MISRA_CPP	R05_00_12_Not_Plain_Char_Type_Usage	0		Information	
CPP	CPP_MISRA_CPP	R05_00_21_Bitwise_Operator_On_Signed_Type	0		Information	
CPP	CPP_MISRA_CPP	R05_02_01_AND_OR_Operands_Not_As_Postfix_Expressions	0		Information	
CPP	CPP_MISRA_CPP	R05_02_10_Using_Of_Incremental_And_Decrimental_Operators	0		Information	
CPP	CPP_MISRA_CPP	R05_02_11_Find_Special_Operator_Overloads	10782		Information	
CPP	CPP_MISRA_CPP	R05_03_02_Unary_Minus_Operator_On_Unsigned_Type	0		Information	
CPP	CPP_MISRA_CPP	R05_03_03_Overloading_Reference_Oper	10753		Information	
CPP	CPP_MISRA_CPP	R05_18_01_Comma_Operator_Used	0		Information	
CPP	CPP_MISRA_CPP	R06_02_01_Assignment_in_Sub_Expr	10754		Information	
CPP	CPP_MISRA_CPP	R06_02_02_FloatingPt_Equality_Inequality_Testing	10752		Information	
CPP	CPP_MISRA_CPP	R06_03_01_Not_Compound_Switch_Or_Iteration_Statement	0		Information	
CPP	CPP_MISRA_CPP	R06_04_01_Not_Compound_If_Or_Else	0		Information	
CPP	CPP_MISRA_CPP	R06_04_02_If_Else_If_Not_Ending_With_Else	0		Information	
CPP	CPP_MISRA_CPP	R06_04_04_Case_Not_Enclosed_By_Compound_Switch	0		Information	
CPP	CPP_MISRA_CPP	R06_04_05_Non_Empty_Switch_Clause_Without_Break_or_Throw	0		Information	
CPP	CPP_MISRA_CPP	R06_04_06_Non_Default_Final_Clause_In_Switch_Statement	0		Information	
CPP	CPP_MISRA_CPP	R06_04_07_Find_Switch_Condition_Bool	10783		Information	
CPP	CPP_MISRA_CPP	R06_05_01_Single_Non_Float_LC	0		Information	
CPP	CPP_MISRA_CPP	R06_05_02_Loop_Counter_Modify	10755		Information	
CPP	CPP_MISRA_CPP	R06_05_03_Change_Lc_In_St_And_Cond	10756		Information	
CPP	CPP_MISRA_CPP	R06_05_04_Incremental_Modified	10757		Information	
CPP	CPP_MISRA_CPP	R06_05_05_Lcv_Change_In_For_Stmt	10758		Information	
CPP	CPP_MISRA_CPP	R06_05_06_Bool_Lcv_Change	10759		Information	
CPP	CPP_MISRA_CPP	R06_06_02_Backward_Use_Of_Goto	0		Information	
CPP	CPP_MISRA_CPP	R06_06_03_Continue_In_Legal_For	10760		Information	
CPP	CPP_MISRA_CPP	R06_06_04_One_GoTo_Break_In_Iteration	0		Information	
CPP	CPP_MISRA_CPP	R06_06_05_Single_Point_Exit_At_Function_End	0		Information	
CPP	CPP_MISRA_CPP	R07_01_01_Declare_Const_if_not_Modified	10784		Information	
CPP	CPP_MISRA_CPP	R07_01_02_Declare_Ref_Const_if_not_Modified	10785		Information	
CPP	CPP_MISRA_CPP	R07_03_01_Definitions_in_Global_Namespace	10786		Information	
CPP	CPP_MISRA_CPP	R07_03_02_Find_non_Global_Mains	10787		Information	
CPP	CPP_MISRA_CPP	R07_03_03_Unnamed_NS_in_Headers	10788		Information	
CPP	CPP_MISRA_CPP	R07_03_04_Find_Using_Directives	10789		Information	
CPP	CPP_MISRA_CPP	R07_03_05_Multiple_Declarations_After_Using	10790		Information	
CPP	CPP_MISRA_CPP	R07_03_06_Find_Using_in_Headers	10791		Information	
CPP	CPP_MISRA_CPP	R07_05_02_Address_Assignment_out_of_Scope	10792		Information	
CPP	CPP_MISRA_CPP	R07_05_03_Return_Parameter_Passed_by_Ref	10793		Information	
CPP	CPP_MISRA_CPP	R07_05_04_Recursion_Exists	0		Information	
CPP	CPP_MISRA_CPP	R08_00_01_Find_Multiple_Declarators	10794		Information	
CPP	CPP_MISRA_CPP	R08_04_01_Function_With_Variable_Number_Of_Arguments	0		Information	
CPP	CPP_MISRA_CPP	R08_04_03_Explicit_Return_Throw	0		Information	
CPP	CPP_MISRA_CPP	R08_05_01_Uninitialized_Variable_Use	10761		Information	
CPP	CPP_MISRA_CPP	R09_05_01_Use_Of_Union	0		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
CPP	CPP_MISRA_CPP	R09_06_02_bool_Unsigned_Signed_Bit_Field	0		Information	
CPP	CPP_MISRA_CPP	R09_06_03_Enum_Bit_Fields	0		Information	
CPP	CPP_MISRA_CPP	R09_06_04_Bit_Fields_Length	0		Information	
CPP	CPP_MISRA_CPP	R10_01_01_Find_Virtual_Base_Classes	10795		Information	
CPP	CPP_MISRA_CPP	R10_03_02_Find_Override_Without_Virtual	10796		Information	
CPP	CPP_MISRA_CPP	R10_03_03_Redeclare_Function_as_Pure	10797		Information	
CPP	CPP_MISRA_CPP	R12_01_03_Find_non_Explicit_Constructor	10798		Information	
CPP	CPP_MISRA_CPP	R15_00_02_Throw_Pointers	10762		Information	
CPP	CPP_MISRA_CPP	R15_00_03_Goto_Label_Inside_TryCatch	10763		Information	
CPP	CPP_MISRA_CPP	R15_01_02_No_Explicit_Null_Throw	10764		Information	
CPP	CPP_MISRA_CPP	R15_01_03_Empty_Throw_Outside_Catch	10765		Information	
CPP	CPP_MISRA_CPP	R15_03_02_Catch_All_In_Main	10766		Information	
CPP	CPP_MISRA_CPP	R15_03_03_Accessing_Non_Static_Mem_In_Ctr_Dtr	10767		Information	
CPP	CPP_MISRA_CPP	R15_03_07_Catch_All_Final	10768		Information	
CPP	CPP_MISRA_CPP	R15_05_01_Statements_Outside_TryCatch_Dtr	10769		Information	
CPP	CPP_MISRA_CPP	R16_00_02_Define_Only_in_Global_Namespace	10770		Information	
CPP	CPP_MISRA_CPP	R16_00_03_Use_Of_Undef_Directive	0		Information	
CPP	CPP_MISRA_CPP	R16_00_04_Function_Like_Macros_Shall_Not_Be_Defined	10771		Information	
CPP	CPP_MISRA_CPP	R16_00_05_No_Tokens_In_Func_Like_Macro	10772		Information	
CPP	CPP_MISRA_CPP	R16_00_07_Undefined_Macro_Identifiers	10799		Information	
CPP	CPP_MISRA_CPP	R16_00_08_Sharp_Before_Preprocessing-Token	10773		Information	
CPP	CPP_MISRA_CPP	R16_01_01_Defined_Standart_Forms	10774		Information	
CPP	CPP_MISRA_CPP	R16_01_02_Preprocessor_If_And_Else_Operators_Reside_In_Different_Files	0		Information	
CPP	CPP_MISRA_CPP	R16_02_06_Include_Directive_In_Wrong_Format	0		Information	
CPP	CPP_MISRA_CPP	R16_03_02_Pound_Preprocessor_Operator_Is_Used	0		Information	
CPP	CPP_MISRA_CPP	R17_00_01_Standard_Library_Redefined_Or_Undefined	0		Information	
CPP	CPP_MISRA_CPP	R17_00_02_Standard_Library_Macros_Reuse	0		Information	
CPP	CPP_MISRA_CPP	R17_00_03_Standard_Library_Functions_Override	0		Information	
CPP	CPP_MISRA_CPP	R18_00_04_Ctime	0		Information	
CPP	CPP_MISRA_CPP	R18_00_05_Unbounded_Functions_Of_Library_CString	0		Information	
CPP	CPP_MISRA_CPP	R18_04_01_Dynamic_Heap_Memory_Allocation	0		Information	
CPP	CPP_MISRA_CPP	R18_07_01_Csignal	0		Information	
CSharp	CSharp_Critical_Risk	Code_Injection	94		Critical	
CSharp	CSharp_Critical_Risk	Command_Injection	77		Critical	
CSharp	CSharp_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
CSharp	CSharp_Critical_Risk	SQL_Injection	89		Critical	
CSharp	CSharp_Critical_Risk	Stored_Code_Injection	94		Critical	
CSharp	CSharp_Critical_Risk	Stored_Command_Injection	77		Critical	
CSharp	CSharp_Critical_Risk	Stored_XSS	79		Critical	
CSharp	CSharp_High_Risk	Buffer_Overflow	120		High	
CSharp	CSharp_High_Risk	CGI_XSS	79		High	
CSharp	CSharp_High_Risk	Connection_String_Injection	99		High	
CSharp	CSharp_High_Risk	Dangerous_File_Extension	434		High	
CSharp	CSharp_High_Risk	Deserialization_of_Untrusted_Data	502		High	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
CSharp	CSharp_High_Risk	Deserialization_of_Untrusted_Data_MSMQ	502		High	
CSharp	CSharp_High_Risk	Improper_Restriction_of_XXE_Ref	611		High	
CSharp	CSharp_High_Risk	JWT_No_Signature_Verification	347		High	
CSharp	CSharp_High_Risk	LDAP_Injection	90		High	
CSharp	CSharp_High_Risk	Path_Traversal	22		High	
CSharp	CSharp_High_Risk	Reflected_XSS	79		High	
CSharp	CSharp_High_Risk	SSRF	918		High	
CSharp	CSharp_High_Risk	Stored_LDAP_Injection	90		High	
CSharp	CSharp_High_Risk	Stored_Path_Traversal	22		High	
CSharp	CSharp_High_Risk	Unsafe_Reflection	470		High	
CSharp	CSharp_Windows_Phone	Insecure_Data_Storage	312		High	
CSharp	CSharp_Windows_Phone	Insufficient_Application_Layer_Protect	319		High	
CSharp	CSharp_Medium_Threat	Command_Argument_Injection	88		Medium	
CSharp	CSharp_Medium_Threat	Cookie_Injection	20		Medium	
CSharp	CSharp_Medium_Threat	CSRF	352		Medium	
CSharp	CSharp_Medium_Threat	Data_Filter_Injection	943		Medium	
CSharp	CSharp_Medium_Threat	DoS_by_Sleep	606		Medium	
CSharp	CSharp_Medium_Threat	Excessive_Data_Exposure	201		Medium	
CSharp	CSharp_Medium_Threat	Hardcoded_password_in_Connection_String	547		Medium	
CSharp	CSharp_Medium_Threat	HttpOnly_Cookie_Flag_Not_Set	1004	Updated	Medium	Medium
CSharp	CSharp_Medium_Threat	Impersonation_Issue	520		Medium	
CSharp	CSharp_Medium_Threat	Improper_Locking	667		Medium	
CSharp	CSharp_Medium_Threat	Insufficient_Connection_String_Encryption	522		Medium	
CSharp	CSharp_Medium_Threat	Insufficiently_Protected_Credentials	522		Medium	
CSharp	CSharp_Medium_Threat	JWT_Sensitive_Information_Exposure	201		Medium	
CSharp	CSharp_Medium_Threat	JWT_Use_Of_Hardcoded_Secret	321		Medium	
CSharp	CSharp_Medium_Threat	Missing_Column_Encryption	312		Medium	
CSharp	CSharp_Medium_Threat	Missing_Function_Level_Authorization	862		Medium	
CSharp	CSharp_Medium_Threat	Missing_HSTS_Header	346		Medium	
CSharp	CSharp_Medium_Threat	Missing_Object_Level_Authorization	862		Medium	
CSharp	CSharp_Medium_Threat	MVC_View_Injection	74		Medium	
CSharp	CSharp_Medium_Threat	No_Request_Validation	20		Medium	
CSharp	CSharp_Medium_Threat	Open_Redirect	601		Medium	
CSharp	CSharp_Medium_Threat	Parameter_Tampering	472		Medium	
CSharp	CSharp_Medium_Threat	Password_In_Comment	615		Medium	
CSharp	CSharp_Medium_Threat	Privacy_Violation	359		Medium	
CSharp	CSharp_Medium_Threat	ReDoS_By_Regex_Injection	1333		Medium	
CSharp	CSharp_Medium_Threat	ReDoS_In_Code	1333		Medium	
CSharp	CSharp_Medium_Threat	ReDoS_In_Validation	1333		Medium	
CSharp	CSharp_Medium_Threat	Reliance_on_Reverse_DNS_Lookups_in_an_Action	350		Medium	
CSharp	CSharp_Medium_Threat	Resource_Injection	99		Medium	
CSharp	CSharp_Medium_Threat	Secure_Cookie_Flag_Not_Set	614	Updated	Medium	Medium
CSharp	CSharp_Medium_Threat	Session_Fixation	384		Medium	
CSharp	CSharp_Medium_Threat	SQL_Injection_Evasion_Attack	89		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
CSharp	CSharp_Medium_Threat	SSL_Verification_Bypass	599		Medium	
CSharp	CSharp_Medium_Threat	Stored_Command_Argument_Injection	88		Medium	
CSharp	CSharp_Medium_Threat	Stored_XPath_Injection	643		Medium	
CSharp	CSharp_Medium_Threat	Unsafe_Object_Binding	915		Medium	
CSharp	CSharp_Medium_Threat	Use_Of_Broken_Or_Risky_Cryptographic_Algorithm	327		Medium	
CSharp	CSharp_Medium_Threat	Use_of_Cryptographically_Weak_PRNG	338		Medium	
CSharp	CSharp_Medium_Threat	Use_of_Hard_coded_Cryptographic_Key	321		Medium	
CSharp	CSharp_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
CSharp	CSharp_Medium_Threat	Value_Shadowing	233		Medium	
CSharp	CSharp_Medium_Threat	XPath_Injection	643		Medium	
CSharp	CSharp_WebConfig	CookieLess_Authentication	642		Medium	
CSharp	CSharp_WebConfig	CookieLess_Session_State	0		Medium	
CSharp	CSharp_WebConfig	Elmah_Enabled	213		Medium	
CSharp	CSharp_WebConfig	HardcodedCredentials	798		Medium	
CSharp	CSharp_WebConfig	HttpOnly_Cookie_Flag_Not_Set_In_Config	1004	Updated	Medium	Medium
CSharp	CSharp_WebConfig	RequireSSL	614		Medium	
CSharp	CSharp_WebConfig	TraceEnabled	749		Medium	
CSharp	CSharp_Windows_Phone	Client_Side_Injection	89		Medium	
CSharp	CSharp_Windows_Phone	Hard_Coded_Cryptography_Key	321		Medium	
CSharp	CSharp_Windows_Phone	Poor_Authorization_and_Authentication	306		Medium	
CSharp	CSharp_Low_Visibility	Client_Side_Only_Validation	602		Low	
CSharp	CSharp_Low_Visibility	Compromised_CDN	0		Low	
CSharp	CSharp_Low_Visibility	Heap_Inspection	244		Low	
CSharp	CSharp_Low_Visibility	Improper_Encoding_Of_Output	116		Low	
CSharp	CSharp_Low_Visibility	Improper_Exception_Handling	248		Low	
CSharp	CSharp_Low_Visibility	Improper_Resource_Shutdown_or_Release	404		Low	
CSharp	CSharp_Low_Visibility	Improper_Session_Management	201		Low	
CSharp	CSharp_Low_Visibility	Improper_Transaction_Handling	460		Low	
CSharp	CSharp_Low_Visibility	Inappropriate_Encoding_for_Output_Context	838		Low	
CSharp	CSharp_Low_Visibility	Information_Exposure_Through_an_Error_Message	209		Low	
CSharp	CSharp_Low_Visibility	Information_Exposure_via_Headers	200		Low	
CSharp	CSharp_Low_Visibility	Information_Leak_Through_Persistent_Cookies	539		Low	
CSharp	CSharp_Low_Visibility	Insufficient_DB_Connection_Encryption	522		Low	
CSharp	CSharp_Low_Visibility	JWT_Excessive_Expiration_Time	613		Low	
CSharp	CSharp_Low_Visibility	JWT_Lack_Of_Expiration_Time	613		Low	
CSharp	CSharp_Low_Visibility	JWT_No_Expiration_Time_Validation	613		Low	
CSharp	CSharp_Low_Visibility	Leaving_Temporary_Files	377		Low	
CSharp	CSharp_Low_Visibility	Log_Forging	117		Low	
CSharp	CSharp_Low_Visibility	Missing_Content_Security_Policy	346		Low	
CSharp	CSharp_Low_Visibility	Off_By_One_Error	193		Low	
CSharp	CSharp_Low_Visibility	Overtly_Permissive_Cross_Origin_Resource_Sharing_Policy	346		Low	
CSharp	CSharp_Low_Visibility	Permissive_Content_Security_Policy	346		Low	
CSharp	CSharp_Low_Visibility	Persistent_Connection_String	257		Low	
CSharp	CSharp_Low_Visibility	Race_Condition_within_a_Thread	366		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
CSharp	CSharp_Low_Visibility	Session_Clearing_Problems	613		Low	
CSharp	CSharp_Low_Visibility	Thread_Safety_Issue	567		Low	
CSharp	CSharp_Low_Visibility	Trust_Boundary_Violation_in_Session_Variables	501		Low	
CSharp	CSharp_Low_Visibility	Unencrypted_Web_Config_File	312		Low	
CSharp	CSharp_Low_Visibility	URL_Canonicalization_Issue	647		Low	
CSharp	CSharp_Low_Visibility	Use_of_Insufficiently_Random_Values	338		Low	
CSharp	CSharp_Low_Visibility	Use_of_RSA_Algorithm_without_OAEP	780		Low	
CSharp	CSharp_WebConfig	CustomError	12		Low	
CSharp	CSharp_WebConfig	DebugEnabled	11		Low	
CSharp	CSharp_WebConfig	Directory_Browse	548		Low	
CSharp	CSharp_WebConfig	Missing_Framing_Policy	1021		Low	
CSharp	CSharp_WebConfig	NonUniqueFormName	694		Low	
CSharp	CSharp_WebConfig	Password_in_Configuration_File	260		Low	
CSharp	CSharp_WebConfig	SlidingExpiration	613		Low	
CSharp	CSharp_Windows_Phone	Side_Channel_Data_Leakage	922		Low	
CSharp	CSharp_Best_Coding_Practice	Aptca_Methods_Call_Non_Aptca_Methods	0		Information	
CSharp	CSharp_Best_Coding_Practice	Catch_NullPointerException	395		Information	
CSharp	CSharp_Best_Coding_Practice	Declaration_Of_Catch_For_Generic_Exception	396		Information	
CSharp	CSharp_Best_Coding_Practice	Deprecated_Methods	0		Information	
CSharp	CSharp_Best_Coding_Practice	Detection_of_Error_Condition_Without_Action	390		Information	
CSharp	CSharp_Best_Coding_Practice	Direct_Use_of_Sockets	246		Information	
CSharp	CSharp_Best_Coding_Practice	Dynamic_SQL_Queries	89		Information	
CSharp	CSharp_Best_Coding_Practice	Exposure_of_Resource_to_Wrong_Sphere	493		Information	
CSharp	CSharp_Best_Coding_Practice	GetLastWin32Error_Is_Not_Called_After_Pinvoke	0		Information	
CSharp	CSharp_Best_Coding_Practice	Hardcoded_Absolute_Path	426		Information	
CSharp	CSharp_Best_Coding_Practice	Hardcoded_Connection_String	798		Information	
CSharp	CSharp_Best_Coding_Practice	Insufficient_Logging_of_Database_Actions	778		Information	
CSharp	CSharp_Best_Coding_Practice	Insufficient_Logging_of_Exceptions	778		Information	
CSharp	CSharp_Best_Coding_Practice	Insufficient_Logging_of_Sensitive_Operations	778		Information	
CSharp	CSharp_Best_Coding_Practice	Just_One_of_Equals_and_Hash_code_Defined	581		Information	
CSharp	CSharp_Best_Coding_Practice	Leftover_Debug_Code	489		Information	
CSharp	CSharp_Best_Coding_Practice	Magic_Numbers	0		Information	
CSharp	CSharp_Best_Coding_Practice	Missing_XML_Validation	112		Information	
CSharp	CSharp_Best_Coding_Practice	Non_Private_Static_Constructors	0		Information	
CSharp	CSharp_Best_Coding_Practice	NULL_Argument_to_Equals	0		Information	
CSharp	CSharp_Best_Coding_Practice	Pages_Without_Global_Error_Handler	544		Information	
CSharp	CSharp_Best_Coding_Practice	PersistSecurityInfo_is_True	0		Information	
CSharp	CSharp_Best_Coding_Practice	Suspicious_Endpoints	923		Information	
CSharp	CSharp_Best_Coding_Practice	Threads_in_WebApp	383		Information	
CSharp	CSharp_Best_Coding_Practice	Unchecked_Error_Condition	0		Information	
CSharp	CSharp_Best_Coding_Practice	Unclosed_Objects	459		Information	
CSharp	CSharp_Best_Coding_Practice	Undocumented_API	0		Information	
CSharp	CSharp_Best_Coding_Practice	Unsafe_Bidi_Unicode_Data	94		Information	
CSharp	CSharp_Best_Coding_Practice	Unsafe_Homoglyphs_Unicode_Data	94		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
CSharp	CSharp_Best_Coding_Practice	Unvalidated_Arguments_Of_Public_Methods	0		Information	
CSharp	CSharp_Best_Coding_Practice	Use_of_System_Output_Stream	117		Information	
CSharp	CSharp_Best_Coding_Practice	Use_Of_Uninitialized_Variables	457		Information	
CSharp	CSharp_Best_Coding_Practice	Using_Of_Index_Instead_Of_Key	1285		Information	
CSharp	CSharp_Best_Coding_Practice	Visible_Pointers	0		Information	
CSharp	CSharp_Windows_Phone	Unused_Permission	250		Information	
Dart	Dart_Mobile_High_Risk	Absolute_Path_Traversal	36		High	
Dart	Dart_Mobile_High_Risk	Resource_Updated_By_URL_Data	939		High	
Dart	Dart_Mobile_High_Risk	Sensitive_Information_Exposure_in_Cleartext_Channel	319		High	
Dart	Dart_Mobile_High_Risk	Unencrypted_Sensitive_Information_in_Publicly_Accessible_Cloud_Storage	922		High	
Dart	Dart_Mobile_High_Risk	Unsafe_Reflection	470	Updated	High	High
Dart	Dart_Mobile_High_Risk	Use_of_Hardcoded_Cryptographic_Key_in_Client	321		High	
Dart	Dart_Mobile_High_Risk	WebView_JavaScript_Injection_from_URL_Scheme	79		High	
Dart	Dart_Mobile_Medium_Threat	Autocorrection_Keystroke_Logging	359		Medium	
Dart	Dart_Mobile_Medium_Threat	Broken_or_Risky_Encryption_Algorithm	327		Medium	
Dart	Dart_Mobile_Medium_Threat	Broken_or_Risky_Hashing_Function	327		Medium	
Dart	Dart_Mobile_Medium_Threat	Communication_Over_HTTP	319		Medium	
Dart	Dart_Mobile_Medium_Threat	Encoding_Used_Instead_of_Encryption	326		Medium	
Dart	Dart_Mobile_Medium_Threat	Hardcoded_Password_In_Gradle	259		Medium	
Dart	Dart_Mobile_Medium_Threat	Implicit_Intent_With_Read_Write_Permissions	276		Medium	
Dart	Dart_Mobile_Medium_Threat	Improper_Certificate_Validation	295		Medium	
Dart	Dart_Mobile_Medium_Threat	Information_Exposure_Through_Query_String	598		Medium	
Dart	Dart_Mobile_Medium_Threat	Insecure_Asymmetric_Cryptographic_Algorithm_Parameters	326		Medium	
Dart	Dart_Mobile_Medium_Threat	Insecure_HTTP_Connections_Enabled	319		Medium	
Dart	Dart_Mobile_Medium_Threat	Insecure_WebSocket_Connection	1385		Medium	
Dart	Dart_Mobile_Medium_Threat	Insufficiently_Secure_Password_Storage_Algorithm_Parameters	522		Medium	
Dart	Dart_Mobile_Medium_Threat	Pasteboard_Leakage	922		Medium	
Dart	Dart_Mobile_Medium_Threat	Poor_Authorization_and_Authentication	306		Medium	
Dart	Dart_Mobile_Medium_Threat	Public_Storage_SQL_Injection	89		Medium	
Dart	Dart_Mobile_Medium_Threat	Public_Storage_WebView_JavaScript_Injection	79		Medium	
Dart	Dart_Mobile_Medium_Threat	Sensitive_Information_Through_URL_Scheme	319		Medium	
Dart	Dart_Mobile_Medium_Threat	SQL_Injection_from_URL_Scheme_or_Intent	89		Medium	
Dart	Dart_Mobile_Medium_Threat	Third_Party_Keyboards_On_Sensitive_Field	829		Medium	
Dart	Dart_Mobile_Medium_Threat	Unencrypted_Sensitive_Information_in_External_Storage	922		Medium	
Dart	Dart_Mobile_Medium_Threat	Use_of_Cryptographically_Weak_PRNG	338		Medium	
Dart	Dart_Mobile_Medium_Threat	Use_of_Hardcoded_Cryptographic_IV	547		Medium	
Dart	Dart_Mobile_Medium_Threat	Use_of_Hardcoded_Salt	760		Medium	
Dart	Dart_Mobile_Medium_Threat	Use_Of_Implicit_Intent_For_Sensitive_Communication	927		Medium	
Dart	Dart_Mobile_Medium_Threat	WebView_Cache_Information_Leak	524		Medium	
Dart	Dart_Mobile_Low_Visibility	App_Transport_Security_Disabled	319		Low	
Dart	Dart_Mobile_Low_Visibility	Compromised_CDN	0		Low	
Dart	Dart_Mobile_Low_Visibility	Encrypted_Sensitive_Information_in_Publicly_Accessible_Cloud_Storage	922		Low	
Dart	Dart_Mobile_Low_Visibility	Improper_Resource_Shutdown_or_Release	404		Low	
Dart	Dart_Mobile_Low_Visibility	Insecure_Android_SDK_Version	1104		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Dart	Dart_Mobile_Low_Visibility	Missing_Device_Lock_Verification	829		Low	
Dart	Dart_Mobile_Low_Visibility	Missing_Root_Or_Jailbreak_Check	250		Low	
Dart	Dart_Mobile_Low_Visibility	No_Installer_Verification_Implemented	829		Low	
Dart	Dart_Mobile_Low_Visibility	Private_Storage_SQL_Injection	89		Low	
Dart	Dart_Mobile_Low_Visibility	Private_Storage_WebView_JavaScript_Injection	79		Low	
Dart	Dart_Mobile_Low_Visibility	Relative_Path_Traversal	23		Low	
Dart	Dart_Mobile_Low_Visibility	Secret_Stored_Outside_of_Keychain	922		Low	
Dart	Dart_Mobile_Low_Visibility	Self_SQL_Injection	89		Low	
Dart	Dart_Mobile_Low_Visibility	Self_WebView_JavaScript_Injection	79		Low	
Dart	Dart_Mobile_Low_Visibility	Unencrypted_Sensitive_Information_in_Internal_Storage	922		Low	
Dart	Dart_Mobile_Low_Visibility	Unencrypted_Sensitive_Information_in_Temporary_File	377		Low	
Dart	Dart_Mobile_Low_Visibility	Use_of_Native_Language	695		Low	
Dart	Dart_Mobile_Low_Visibility	User_Information_in_Publicly_Accessible_Storage	922		Low	
Dart	Dart_Mobile_Best_Coding_Practice	Deprecated_Functions_or_Properties	477		Information	
Dart	Dart_Mobile_Best_Coding_Practice	Encrypted_Sensitive_Information_in_External_Storage	0		Information	
Dart	Dart_Mobile_Best_Coding_Practice	Missing_Certificate_Pinning	295		Information	
Dart	Dart_Mobile_Best_Coding_Practice	Unused_Permission	250		Information	
Dart	Dart_Mobile_Best_Coding_Practice	Use_of_Non_Cryptographic_Random	338		Information	
Go	Go_AWS_Lambda	DynamoDB_NoSQL_Injection	943		Critical	
Go	Go_Critical_Risk	Arbitrary_File_Write	669	New	Critical	
Go	Go_Critical_Risk	CGI_Stored_XSS	79	New	Critical	
Go	Go_Critical_Risk	Command_Injection	77		Critical	
Go	Go_Critical_Risk	NoSQL_Injection	943	New	Critical	
Go	Go_Critical_Risk	Second_Order_NoSQL_Injection	943	New	Critical	
Go	Go_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
Go	Go_Critical_Risk	SQL_Injection	89		Critical	
Go	Go_Critical_Risk	Stored_Command_Injection	77		Critical	
Go	Go_Critical_Risk	Stored_XSS_All_Clients	79		Critical	
Go	Go_AWS_Lambda	AWS_Credentials_Leak	522		High	
Go	Go_High_Risk	Absolute_Path_Traversal	36		High	
Go	Go_High_Risk	CGI_Reflected_XSS	79	Updated	High	
Go	Go_High_Risk	Connection_String_Injection	99		High	
Go	Go_High_Risk	JWT_No_Signature_Verification	347	Updated	High	High
Go	Go_High_Risk	Observable_Timing_Discrepancy	208	New	High	
Go	Go_High_Risk	Plain_Text_Transport_Layer_in_Server	319		High	
Go	Go_High_Risk	Reflected_XSS	79		High	
Go	Go_High_Risk	Relative_Path_Traversal	23		High	
Go	Go_High_Risk	Sensitive_Information_Exposure_in_Cleartext_Channel	319	Updated	High	High
Go	Go_High_Risk	SSRF	918	Updated	High	High
Go	Go_High_Risk	Unsafe_Archive_Unpacking	22	New	High	
Go	Go_High_Risk	Unsafe_Reflection	470		High	
Go	Go_AWS_Lambda	Hardcoded_AWS_Credentials	798		Medium	
Go	Go_AWS_Lambda	Permission_Manipulation_In_S3	281		Medium	
Go	Go_AWS_Lambda	Unrestricted_Read_S3	639		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Go	Go_AWS_Lambda	Unrestricted_Write_S3	639		Medium	
Go	Go_AWS_Lambda	Use_of_Hardcoded_Cryptographic_Key_On_Server	321		Medium	
Go	Go_Insecure_Credential_Storage	Insecure_Credential_Storage_Mechanism	522	Updated	Medium	Medium
Go	Go_Insecure_Credential_Storage	Insecure_Script_Parameters	522		Medium	
Go	Go_Insecure_Credential_Storage	Insufficient_Bcrypt_Cost	522		Medium	
Go	Go_Insecure_Credential_Storage	Insufficient_Output_Length	522		Medium	
Go	Go_Insecure_Credential_Storage	PBKDF2_Insufficient_Iteration_Count	522		Medium	
Go	Go_Insecure_Credential_Storage	PBKDF2_Weak_Salt_Value	522		Medium	
Go	Go_Insecure_Credential_Storage	Script_Weak_Salt_Value	522		Medium	
Go	Go_Medium_Threat	Broken_or_Risky_Encryption_Algorithm	327	Updated	Medium	Medium
Go	Go_Medium_Threat	Broken_or_Risky_Hashing_Function	327		Medium	
Go	Go_Medium_Threat	Command_Argument_Injection	88		Medium	
Go	Go_Medium_Threat	DoS_By_Sleep	606	New	Medium	
Go	Go_Medium_Threat	Email_Content_Forgery	116		Medium	
Go	Go_Medium_Threat	Empty_Password_In_Connection_String	521		Medium	
Go	Go_Medium_Threat	Hardcoded_Cryptographic_IV	547	New	Medium	
Go	Go_Medium_Threat	Hardcoded_Cryptographic_Key	321	New	Medium	
Go	Go_Medium_Threat	Hardcoded_Password_in_Connection_String	547		Medium	
Go	Go_Medium_Threat	Hardcoded_Salt	760	New	Medium	
Go	Go_Medium_Threat	HttpOnly_Cookie_Flag_Not_Set_In_Config	1004		Medium	
Go	Go_Medium_Threat	Insecure_Asymmetric_Cryptographic_Algorithm_Parameters	326	New	Medium	
Go	Go_Medium_Threat	Insecure_Value_of_the_SameSite_Cookie_Attribute_in_Code	1275		Medium	
Go	Go_Medium_Threat	Insufficiently_Secure_Password_Storage_Algorithm_Parameters	522	New	Medium	
Go	Go_Medium_Threat	JWT_Lack_Of_Expiration_Time	613	New	Medium	
Go	Go_Medium_Threat	JWT_Use_Of_Hardcoded_Secret	321	New	Medium	
Go	Go_Medium_Threat	JWT_Use_of_None_Algorithm	287	New	Medium	
Go	Go_Medium_Threat	Missing_HSTS_Header	346		Medium	
Go	Go_Medium_Threat	Open_Redirect	601	Updated	Medium	Medium
Go	Go_Medium_Threat	Parameter_Tampering	472	Updated	Medium	Medium
Go	Go_Medium_Threat	Password_In_Comment	615		Medium	
Go	Go_Medium_Threat	PCI_Data_Exposure	312	New	Medium	
Go	Go_Medium_Threat	Privacy_Violation	359	Updated	Medium	Medium
Go	Go_Medium_Threat	Secret_Leak	312	New	Medium	
Go	Go_Medium_Threat	Secure_Cookie_Flag_Not_Set_In_Config	614		Medium	
Go	Go_Medium_Threat	Server_Information_Exposure	497	New	Medium	
Go	Go_Medium_Threat	SSL_Verification_Bypass	599		Medium	
Go	Go_Medium_Threat	Stored_Absolute_Path_Traversal	36		Medium	
Go	Go_Medium_Threat	Stored_Command_Argument_Injection	88		Medium	
Go	Go_Medium_Threat	Stored_Relative_Path_Traversal	23		Medium	
Go	Go_Medium_Threat	Trust_Proxy_On	348		Medium	
Go	Go_Medium_Threat	Unchecked_Input_for_Loop_Condition	606	New	Medium	
Go	Go_Medium_Threat	Unrestricted_File_Size_Upload	434	New	Medium	
Go	Go_Medium_Threat	Unsafe_Object_Binding	915		Medium	
Go	Go_Medium_Threat	Use_of_Cryptographically_Weak_PRNG	338	Updated	Medium	Medium

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Go	Go_Medium_Threat	Use_of_Hardcoded_Password	259		Medium	
Go	Go_Medium_Threat	Use_Of_Hardcoded_Password_in_Config	260		Medium	
Go	Go_Medium_Threat	Use_of_Native_Language	695	New	Medium	
Go	Go_Medium_Threat	Use_Of_Unsafe_Package	242		Medium	
Go	Go_AWS_Lambda	Race_Condition_Global_Scope	1108		Low	
Go	Go_AWS_Lambda	Unrestricted_Delete_S3	639		Low	
Go	Go_AWS_Lambda	User_Based_SDK_Configurations	15		Low	
Go	Go_Low_Visibility	Compromised_CDN	0		Low	
Go	Go_Low_Visibility	Dangerous_File_Extension	434	New	Low	
Go	Go_Low_Visibility	Deprecated_Functions_or_Properties	477		Low	
Go	Go_Low_Visibility	Divide_By_Zero	369		Low	
Go	Go_Low_Visibility	Environment_Variable_Injection	15	New	Low	
Go	Go_Low_Visibility	Improper_Error_Handling	248		Low	
Go	Go_Low_Visibility	Incorrect_Reflect_Value_Comparison	595		Low	
Go	Go_Low_Visibility	Integer_Overflow	190		Low	
Go	Go_Low_Visibility	Integer_Underflow	191	New	Low	
Go	Go_Low_Visibility	JWT_Excessive_Expiration_Time	613	New	Low	
Go	Go_Low_Visibility	JWT_No_Claims_Directives_Validation	304	Updated	Low	Low
Go	Go_Low_Visibility	Leaving_Temporary_File	377	Updated	Low	Low
Go	Go_Low_Visibility	Log_Forging	117		Low	
Go	Go_Low_Visibility	Missing_Content_Security_Policy	346		Low	
Go	Go_Low_Visibility	Missing_Password_Field_Masking	549	New	Low	
Go	Go_Low_Visibility	Overly_Permissive_Cross-Origin_Resource_Sharing_Policy	346		Low	
Go	Go_Low_Visibility	PCI_Data_Exposure_in_Error_Messages	209	New	Low	
Go	Go_Low_Visibility	PCI_Data_Exposure_in_Files	312	New	Low	
Go	Go_Low_Visibility	PCI_Data_Exposure_in_JWT	312	New	Low	
Go	Go_Low_Visibility	PCI_Data_Exposure_in_Logs	532	New	Low	
Go	Go_Low_Visibility	PCI_Data_Exposure_in_URL	312	New	Low	
Go	Go_Low_Visibility	Permissive_Content_Security_Policy	346		Low	
Go	Go_Low_Visibility	Privacy_Violation_in_Error_Messages	209	New	Low	
Go	Go_Low_Visibility	Privacy_Violation_in_Files	312	New	Low	
Go	Go_Low_Visibility	Privacy_Violation_in_JWT	312	New	Low	
Go	Go_Low_Visibility	Privacy_Violation_in_Logs	532	New	Low	
Go	Go_Low_Visibility	Privacy_Violation_in_URL	312	New	Low	
Go	Go_Low_Visibility	Race_Condition_Concurrent_Instances	366		Low	
Go	Go_Low_Visibility	Race_Condition_In_Cross_Functionality	362		Low	
Go	Go_Low_Visibility	Secret_Leak_in_Error_Messages	209	New	Low	
Go	Go_Low_Visibility	Secret_Leak_in_Files	312	New	Low	
Go	Go_Low_Visibility	Secret_Leak_in_JWT	312	New	Low	
Go	Go_Low_Visibility	Secret_Leak_in_Logs	532	New	Low	
Go	Go_Low_Visibility	Secret_Leak_in_URL	312	New	Low	
Go	Go_Low_Visibility	Server_Information_Exposure_In_Error_Messages	209	New	Low	
Go	Go_Low_Visibility	Server_Information_Exposure_via_Misconfiguration	312	New	Low	
Go	Go_Low_Visibility	Stored_Environment_Variable_Injection	15	New	Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Go	Go_Low_Visibility	Uncontrolled_Format_String	134	New	Low	
Go	Go_Low_Visibility	Use_of_Non_Cryptographic_Random	338	New	Low	
Go	Go_Best_Coding_Practice	Outdated_Encryption_Algorithm	326	New	Information	
Go	Go_Best_Coding_Practice	Outdated_Hashing_Function	328		Information	
Groovy	Groovy_Critical_Risk	CGI_Stored_XSS	79		Critical	
Groovy	Groovy_Critical_Risk	Code_Injection	94		Critical	
Groovy	Groovy_Critical_Risk	Command_Injection	77		Critical	
Groovy	Groovy_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
Groovy	Groovy_Critical_Risk	SQL_Injection	89		Critical	
Groovy	Groovy_Critical_Risk	Stored_Command_Injection	77		Critical	
Groovy	Groovy_Critical_Risk	Stored_XSS	79		Critical	
Groovy	Groovy_Stored	Stored_Code_Injection	94		Critical	
Groovy	Groovy_High_Risk	Absolute_Path_Traversal	36		High	
Groovy	Groovy_High_Risk	CGI_Reflected_XSS	79		High	
Groovy	Groovy_High_Risk	Cleartext_Submission_of_Sensitive_Information	319		High	
Groovy	Groovy_High_Risk	Connection_String_Injection	99		High	
Groovy	Groovy_High_Risk	Dangerous_File_Inclusion	829		High	
Groovy	Groovy_High_Risk	Improper_Build_Of_Sql_Mapping	89		High	
Groovy	Groovy_High_Risk	LDAP_Injection	90		High	
Groovy	Groovy_High_Risk	Reflected_XSS	79		High	
Groovy	Groovy_High_Risk	Relative_Path_Traversal	23		High	
Groovy	Groovy_High_Risk	Stored_LDAP_Injection	90		High	
Groovy	Groovy_Medium_Threat	Authorization_Bypass_Through_User_Controlled_SQL_PrimaryKey	566		Medium	
Groovy	Groovy_Medium_Threat	CSRF	352		Medium	
Groovy	Groovy_Medium_Threat	DB_Control_of_System_or_Config_Setting	15		Medium	
Groovy	Groovy_Medium_Threat	Direct_Use_of_Unsafe_JNI	111		Medium	
Groovy	Groovy_Medium_Threat	DoS_by_Sleep	606		Medium	
Groovy	Groovy_Medium_Threat	Empty_Password_In_Connection_String	521		Medium	
Groovy	Groovy_Medium_Threat	External_Control_of_Critical_State_Data	642		Medium	
Groovy	Groovy_Medium_Threat	External_Control_of_System_or_Config_Setting	15		Medium	
Groovy	Groovy_Medium_Threat	Hardcoded_password_in_Connection_String	547		Medium	
Groovy	Groovy_Medium_Threat	HttpOnly_Cookie_Flag_Not_Set	1004		Medium	
Groovy	Groovy_Medium_Threat	HttpOnlyCookies_In_Config	1004		Medium	
Groovy	Groovy_Medium_Threat	Improper_Locking	667		Medium	
Groovy	Groovy_Medium_Threat	Insufficiently_Protected_Credentials	522		Medium	
Groovy	Groovy_Medium_Threat	Not_Using_a_Random_IV_with_CBC_Mode	329		Medium	
Groovy	Groovy_Medium_Threat	Open_Redirect	601		Medium	
Groovy	Groovy_Medium_Threat	Parameter_Tampering	472		Medium	
Groovy	Groovy_Medium_Threat	Plaintext_Storage_of_a_Password	256		Medium	
Groovy	Groovy_Medium_Threat	Privacy_Violation	359		Medium	
Groovy	Groovy_Medium_Threat	Process_Control	114		Medium	
Groovy	Groovy_Medium_Threat	ReDoS_From_Regex_Injection	1333		Medium	
Groovy	Groovy_Medium_Threat	ReDoS_In_Match	1333		Medium	
Groovy	Groovy_Medium_Threat	ReDoS_In_Pattern	1333		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Groovy	Groovy_Medium_Threat	ReDoS_In_Replace	1333		Medium	
Groovy	Groovy_Medium_Threat	Reliance_on_Cookies_without_Validation	565		Medium	
Groovy	Groovy_Medium_Threat	Reliance_on_Reverse_DNS_Lookups_in_an_Action	350		Medium	
Groovy	Groovy_Medium_Threat	Resource_Injection	99		Medium	
Groovy	Groovy_Medium_Threat	Reversible_One_Way_Hash	328		Medium	
Groovy	Groovy_Medium_Threat	Secure_Cookie_Flag_Not_Set	614		Medium	
Groovy	Groovy_Medium_Threat	Session_Fixation	384		Medium	
Groovy	Groovy_Medium_Threat	Spring_ModelView_Injection	94		Medium	
Groovy	Groovy_Medium_Threat	SQL_Injection_Evasion_Attack	89		Medium	
Groovy	Groovy_Medium_Threat	Stored_Absolute_Path_Traversal	36		Medium	
Groovy	Groovy_Medium_Threat	Stored_Relative_Path_Traversal	23		Medium	
Groovy	Groovy_Medium_Threat	Unchecked_Input_for_Loop_Condition	606		Medium	
Groovy	Groovy_Medium_Threat	Uncontrolled_Memory_Allocation	789		Medium	
Groovy	Groovy_Medium_Threat	Unvalidated_Forwards	601		Medium	
Groovy	Groovy_Medium_Threat	Use_of_a_One_Way_Hash_with_a_Predictable_Salt	760		Medium	
Groovy	Groovy_Medium_Threat	Use_of_a_One_Way_Hash_without_a_Salt	759		Medium	
Groovy	Groovy_Medium_Threat	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327		Medium	
Groovy	Groovy_Medium_Threat	Use_of_Cryptographically_Weak_PRNG	338		Medium	
Groovy	Groovy_Medium_Threat	Use_of_Hard_coded_Cryptographic_Key	321		Medium	
Groovy	Groovy_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
Groovy	Groovy_Medium_Threat	Use_of_Native_Language	695		Medium	
Groovy	Groovy_Medium_Threat	Using_Referer_Field_for_Authentication	293		Medium	
Groovy	Groovy_Medium_Threat	XPath_Injection	643		Medium	
Groovy	Groovy_Stored	Stored_Open_Redirect	601		Medium	
Groovy	Groovy_Stored	Stored_XPath_Injection	643		Medium	
Groovy	Groovy_Low_Visibility	Compromised_CDN	0		Low	
Groovy	Groovy_Low_Visibility	Creation_of_Temp_File_in_Dir_with_Incorrect_Permissions	379		Low	
Groovy	Groovy_Low_Visibility	Creation_of_Temp_File_With_Insecure_Permissions	378		Low	
Groovy	Groovy_Low_Visibility	Data_Leak_Between_Sessions	362		Low	
Groovy	Groovy_Low_Visibility	Divide_By_Zero	369		Low	
Groovy	Groovy_Low_Visibility	ESAPI_Same_Password_Repeats_Twice	521		Low	
Groovy	Groovy_Low_Visibility	Escape_False	116		Low	
Groovy	Groovy_Low_Visibility	Heap_Inspection	244		Low	
Groovy	Groovy_Low_Visibility	Improper_Exception_Handling	248		Low	
Groovy	Groovy_Low_Visibility	Improper_Resource_Locking	413		Low	
Groovy	Groovy_Low_Visibility	Improper_Resource_Shutdown_or_Release	404		Low	
Groovy	Groovy_Low_Visibility	Improper_Session_Management	201		Low	
Groovy	Groovy_Low_Visibility	Improper_Transaction_Handling	460		Low	
Groovy	Groovy_Low_Visibility	Information_Exposure_Through_an_Error_Message	209		Low	
Groovy	Groovy_Low_Visibility	Information_Exposure_Through_Debug_Log	532		Low	
Groovy	Groovy_Low_Visibility	Information_Exposure_Through_Server_Log	532		Low	
Groovy	Groovy_Low_Visibility	Information_Leak_Through_Comments	615		Low	
Groovy	Groovy_Low_Visibility	Information_Leak_Through_Persistent_Cookies	539		Low	
Groovy	Groovy_Low_Visibility	Information_Leak_Through_Shell_Error_Message	535		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Groovy	Groovy_Low_Visibility	Insufficient_Session_Expiration	613		Low	
Groovy	Groovy_Low_Visibility	Integer_Overflow	190		Low	
Groovy	Groovy_Low_Visibility	Integer_Underflow	191		Low	
Groovy	Groovy_Low_Visibility	Leaving_Temporary_File	377		Low	
Groovy	Groovy_Low_Visibility	Log_Forging	117		Low	
Groovy	Groovy_Low_Visibility	Logic_Time_Bomb	511		Low	
Groovy	Groovy_Low_Visibility	Missing_Password_Field_Masking	549		Low	
Groovy	Groovy_Low_Visibility	Object_Hijack	491		Low	
Groovy	Groovy_Low_Visibility	Off_by_One_Error	193		Low	
Groovy	Groovy_Low_Visibility	Public_Static_Final_References_Mutable_Object	607		Low	
Groovy	Groovy_Low_Visibility	Race_Condition	362		Low	
Groovy	Groovy_Low_Visibility	Race_Condition_Format_Flaw	362		Low	
Groovy	Groovy_Low_Visibility	Same_Seed_in_PRNG	336		Low	
Groovy	Groovy_Low_Visibility	Serializable_Class_Containing_Sensitive_Data	499		Low	
Groovy	Groovy_Low_Visibility	Server_Information_Exposure	497		Low	
Groovy	Groovy_Low_Visibility	Spring_defaultHtmlEscape_Not_True	116		Low	
Groovy	Groovy_Low_Visibility	TOCTOU	367		Low	
Groovy	Groovy_Low_Visibility	Trust_Boundary_Violation_in_Session_Variables	501		Low	
Groovy	Groovy_Low_Visibility	Uncaught_Exception	248		Low	
Groovy	Groovy_Low_Visibility	Uncontrolled_Format_String	134		Low	
Groovy	Groovy_Low_Visibility	Unsynchronized_Access_To_Shared_Data	567		Low	
Groovy	Groovy_Low_Visibility	Use_of_Hard_coded_Security_Constants	547		Low	
Groovy	Groovy_Low_Visibility	Use_of_Insufficiently_Random_Values	338		Low	
Groovy	Groovy_Low_Visibility	Use_of_RSA_Algorithm_without_OAEP	780		Low	
Groovy	Groovy_Low_Visibility	XSS_Evasion_Attack_via_Replace	182		Low	
Groovy	Groovy_Stored	Stored_Boundary_Violation	646		Low	
Groovy	Groovy_Best_Coding_Practice	Assign_Collection	0		Information	
Groovy	Groovy_Best_Coding_Practice	Assigning_instead_of_Comparing	481		Information	
Groovy	Groovy_Best_Coding_Practice	Comparing_instead_of_Assigning	482		Information	
Groovy	Groovy_Best_Coding_Practice	Declaration_Of_Catch_For_Generic_Exception	396		Information	
Groovy	Groovy_Best_Coding_Practice	Declaration_of_Throws_for_Generic_Exception	397		Information	
Groovy	Groovy_Best_Coding_Practice	Deprecated_Functions_or_Properties	477		Information	
Groovy	Groovy_Best_Coding_Practice	Dynamic_SQL_Queries	89		Information	
Groovy	Groovy_Best_Coding_Practice	Empty_Methods	0		Information	
Groovy	Groovy_Best_Coding_Practice	Explicit_Calls_To_Methods	0		Information	
Groovy	Groovy_Best_Coding_Practice	Explicit_Instantiation	0		Information	
Groovy	Groovy_Best_Coding_Practice	Exposure_of_Resource_to_Wrong_Sphere	493		Information	
Groovy	Groovy_Best_Coding_Practice	Getter_Method_Could_Be_Property	0		Information	
Groovy	Groovy_Best_Coding_Practice	GOTO_Statement	0		Information	
Groovy	Groovy_Best_Coding_Practice	Hardcoded_Absolute_Path	426		Information	
Groovy	Groovy_Best_Coding_Practice	Hardcoded_Connection_String	798		Information	
Groovy	Groovy_Best_Coding_Practice	Incorrect_Block_Delimitation	483		Information	
Groovy	Groovy_Best_Coding_Practice	Input_Path_Not_Canonicalized	73		Information	
Groovy	Groovy_Best_Coding_Practice	Just_One_of_Equals_and_Hash_code_Defined	581		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Groovy	Groovy_Best_Coding_Practice	Missing_Default_Case_In_Switch_Statement	478		Information	
Groovy	Groovy_Best_Coding_Practice	Omitted_Break_Statement_In_Switch	484		Information	
Groovy	Groovy_Best_Coding_Practice	Potential_Usage_of_Vulnerable_Log4J	502		Information	
Groovy	Groovy_Best_Coding_Practice	Public_Static_Field_Not_Marked_Final	500		Information	
Groovy	Groovy_Best_Coding_Practice	Return_Inside_Finally_Block	584		Information	
Groovy	Groovy_Best_Coding_Practice	Use_Collect_Many	0		Information	
Groovy	Groovy_Best_Coding_Practice	Use_Collect_Nested	0		Information	
Groovy	Groovy_Best_Coding_Practice	Use_of_System_exit	382		Information	
Groovy	Groovy_Best_Coding_Practice	Use_of_Wrong_Operator_in_String_Comparison	597		Information	
Java	Java_AWS_Lambda	DynamoDB_NoSQL_Injection	943		Critical	
Java	Java_Critical_Risk	CGI_Stored_XSS	79		Critical	
Java	Java_Critical_Risk	Code_Injection	94		Critical	
Java	Java_Critical_Risk	Command_Injection	77		Critical	
Java	Java_Critical_Risk	Expression_Language_Injection_EL	917		Critical	
Java	Java_Critical_Risk	Expression_Language_Injection_MVEL	917		Critical	
Java	Java_Critical_Risk	Expression_Language_Injection_OGNL	917		Critical	
Java	Java_Critical_Risk	Expression_Language_Injection_SPEL	917		Critical	
Java	Java_Critical_Risk	JSF_Local_File_Inclusion	98		Critical	
Java	Java_Critical_Risk	NoSQL_Injection	943		Critical	
Java	Java_Critical_Risk	Second_Order_NoSQL_Injection	943		Critical	
Java	Java_Critical_Risk	Second_Order_SQL_Injection	89	Updated	Critical	
Java	Java_Critical_Risk	SQL_Injection	89		Critical	
Java	Java_Critical_Risk	Stored_Command_Injection	77		Critical	
Java	Java_Critical_Risk	Stored_XSS	79		Critical	
Java	Java_Critical_Risk	Unsafe_JNDI_Lookup	20		Critical	
Java	Java_Spring	Spring_View_SPEL_Injection	917		Critical	
Java	Java_Stored	Stored_Code_Injection	94		Critical	
Java	Java_Android	Insecure_WebView_Usage	829		High	
Java	Java_Android	Insufficient_Sensitive_Application_Layer	319		High	
Java	Java_AWS_Lambda	AWS_Credentials_Leak	522		High	
Java	Java_GWT	GWT_DOM_XSS	79		High	
Java	Java_GWT	GWT_Reflected_XSS	79		High	
Java	Java_High_Risk	Absolute_Path_Traversal	36		High	
Java	Java_High_Risk	CGI_Reflected_XSS	79		High	
Java	Java_High_Risk	Cleartext_Submission_of_Sensitive_Information	319		High	
Java	Java_High_Risk	Connection_String_Injection	99		High	
Java	Java_High_Risk	Dangerous_File_Inclusion	829		High	
Java	Java_High_Risk	Deserialization_of_Untrusted_Data	502		High	
Java	Java_High_Risk	Deserialization_of_Untrusted_Data_in_JMS	502		High	
Java	Java_High_Risk	Download_of_Code_Without_Integrity_Check	494		High	
Java	Java_High_Risk	Improper_Build_Of_Sql_Mapping	89		High	
Java	Java_High_Risk	Improper_Restriction_of_Stored_XXE_Ref	611		High	
Java	Java_High_Risk	Improper_Restriction_of_XXE_Ref	611		High	
Java	Java_High_Risk	JWT_No_Signature_Verification	347		High	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Java	Java_High_Risk	JWT_Use_Of_None_Algorithm	287		High	
Java	Java_High_Risk	LDAP_Injection	90		High	
Java	Java_High_Risk	Reflected_XSS	79		High	
Java	Java_High_Risk	Relative_Path_Traversal	23		High	
Java	Java_High_Risk	SSRF	918	Updated	High	High
Java	Java_High_Risk	Stored_LDAP_Injection	90		High	
Java	Java_High_Risk	Unsafe_Reflection	470		High	
Java	Java_Spring	Spring_Observable_Time_Discrepancy	208		High	
Java	Java_Android	Client_Side_Injection	89		Medium	
Java	Java_Android	Copy_Paste_Buffer_Caching	922		Medium	
Java	Java_Android	Exported_Content_Provider_Without_Protective_Permissions	276		Medium	
Java	Java_Android	Exported_Service_Without_Protective_Permissions	276		Medium	
Java	Java_Android	Hardcoded_Password_In_Gradle	259		Medium	
Java	Java_Android	Implicit_Intent_With_Read_Write_Permissions	276		Medium	
Java	Java_Android	Improper_Certificate_Validation	295		Medium	
Java	Java_Android	Improper_Verification_Of_Intent_By_Broadcast_Receiver	925		Medium	
Java	Java_Android	Insecure_HTTP_Connections_Enabled	319		Medium	
Java	Java_Android	Insufficient_Application_Layer_Protect	319		Medium	
Java	Java_Android	Poor_Authorization_and_Authentication	306		Medium	
Java	Java_Android	Screen_Caching	524		Medium	
Java	Java_Android	Side_Channel_Data_Leakage	922		Medium	
Java	Java_Android	Use_Of_Implicit_Intent_For_Sensitive_Communication	927		Medium	
Java	Java_Android	Weak_Encryption	326		Medium	
Java	Java_Android	WebView_Cache_Information_Leak	524		Medium	
Java	Java_AWS_Lambda	Hardcoded_AWS_Credentials	798		Medium	
Java	Java_AWS_Lambda	Permission_Manipulation_in_S3	281		Medium	
Java	Java_AWS_Lambda	Unrestricted_Delete_S3	639		Medium	
Java	Java_AWS_Lambda	Unrestricted_Read_S3	639		Medium	
Java	Java_AWS_Lambda	Unrestricted_Write_S3	639		Medium	
Java	Java_AWS_Lambda	Use_of_Hardcoded_Cryptographic_Key_On_Server	321		Medium	
Java	Java_Medium_Threat	Authorization_Bypass_Through_User_Controlled_SQL_PrimaryKey	566		Medium	
Java	Java_Medium_Threat	Client_State_Saving_Method_JSF	642		Medium	
Java	Java_Medium_Threat	Command_Argument_Injection	88		Medium	
Java	Java_Medium_Threat	CSRF	352		Medium	
Java	Java_Medium_Threat	Dangerous_File_Size_Upload	434		Medium	
Java	Java_Medium_Threat	DB_Control_of_System_or_Config_Setting	15		Medium	
Java	Java_Medium_Threat	DoS_by_Sleep	606		Medium	
Java	Java_Medium_Threat	Empty_Password_In_Connection_String	521		Medium	
Java	Java_Medium_Threat	Environment_Variable_Injection	15		Medium	
Java	Java_Medium_Threat	Excessive_Data_Exposure	201		Medium	
Java	Java_Medium_Threat	External_Control_of_Critical_State_Data	642		Medium	
Java	Java_Medium_Threat	External_Control_of_System_or_Config_Setting	15		Medium	
Java	Java_Medium_Threat	Frameable_Login_Page	829		Medium	
Java	Java_Medium_Threat	Hardcoded_password_in_Connection_String	547		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Java	Java_Medium_Threat	HttpOnly_Cookie_Flag_Not_Set	1004		Medium	
Java	Java_Medium_Threat	HttpOnly_Cookie_Flag_Not_Set_In_Config	1004		Medium	
Java	Java_Medium_Threat	Improper_Locking	667		Medium	
Java	Java_Medium_Threat	Information_Exposure_Through_Query_String	598		Medium	
Java	Java_Medium_Threat	Insufficiently_Protected_Credentials	522		Medium	
Java	Java_Medium_Threat	JSF_CSRF	352		Medium	
Java	Java_Medium_Threat	JSF_Managed_Bean_PII_Leak	359		Medium	
Java	Java_Medium_Threat	JWT_Sensitive_Information_Exposure	201		Medium	
Java	Java_Medium_Threat	JWT_Use_Of_Hardcoded_Secret	321		Medium	
Java	Java_Medium_Threat	Misconfigured_Deserialization_Filter	0		Medium	
Java	Java_Medium_Threat	Missing_HSTS_Header	346		Medium	
Java	Java_Medium_Threat	Not_Using_a_Random_IV_with_CBC_Mode	329		Medium	
Java	Java_Medium_Threat	Open_Redirect	601	Updated	Medium	Medium
Java	Java_Medium_Threat	Parameter_Tampering	472		Medium	
Java	Java_Medium_Threat	Password_In_Comment	615		Medium	
Java	Java_Medium_Threat	Plaintext_Storage_of_a_Password	256		Medium	
Java	Java_Medium_Threat	Privacy_Violation	359		Medium	
Java	Java_Medium_Threat	Process_Control	114		Medium	
Java	Java_Medium_Threat	ReDoS_From_Regex_Injection	1333		Medium	
Java	Java_Medium_Threat	ReDoS_In_Match	1333		Medium	
Java	Java_Medium_Threat	ReDoS_In_Pattern	1333		Medium	
Java	Java_Medium_Threat	ReDoS_In_Replace	1333		Medium	
Java	Java_Medium_Threat	Reliance_on_Cookies_without_Validation	565		Medium	
Java	Java_Medium_Threat	Reliance_on_Reverse_DNS_Lookups_in_an_Action	350		Medium	
Java	Java_Medium_Threat	Resource_Injection	99		Medium	
Java	Java_Medium_Threat	Reversible_One_Way_Hash	328		Medium	
Java	Java_Medium_Threat	Secure_Cookie_Flag_Not_Set	614		Medium	
Java	Java_Medium_Threat	Session_Fixation	384		Medium	
Java	Java_Medium_Threat	SQL_Injection_Evasion_Attack	89		Medium	
Java	Java_Medium_Threat	SSL_Verification_Bypass	599	Updated	Medium	Medium
Java	Java_Medium_Threat	Stored_Absolute_Path_Traversal	36		Medium	
Java	Java_Medium_Threat	Stored_Command_Argument_Injection	88		Medium	
Java	Java_Medium_Threat	Stored_Environment_Variable_Injection	15		Medium	
Java	Java_Medium_Threat	Stored_Relative_Path_Traversal	23		Medium	
Java	Java_Medium_Threat	Unchecked_Input_for_Loop_Condition	606		Medium	
Java	Java_Medium_Threat	Uncontrolled_Memory_Allocation	789		Medium	
Java	Java_Medium_Threat	Unsafe_Object_Binding	915		Medium	
Java	Java_Medium_Threat	Unvalidated_Forwards	601		Medium	
Java	Java_Medium_Threat	Use_of_a_One_Way_Hash_with_a_Predictable_Salt	760		Medium	
Java	Java_Medium_Threat	Use_of_a_One_Way_Hash_without_a_Salt	759		Medium	
Java	Java_Medium_Threat	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327		Medium	
Java	Java_Medium_Threat	Use_of_Cryptographically_Weak_PRNG	338		Medium	
Java	Java_Medium_Threat	Use_of_Hard_coded_Cryptographic_Key	321		Medium	
Java	Java_Medium_Threat	Use_Of_Hardcoded_Password	259	Updated	Medium	Medium

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Java	Java_Medium_Threat	Use_Of_Hardcoded_Password_In_Config	260	Updated	Medium	Medium
Java	Java_Medium_Threat	Use_of_Native_Language	695	Updated	Medium	Medium
Java	Java_Medium_Threat	Using_Referer_Field_for_Authentication	293		Medium	
Java	Java_Medium_Threat	XPath_Injection	643		Medium	
Java	Java_Medium_Threat	XQuery_Injection	652		Medium	
Java	Java_Spring	Spring_Argon2_Insecure_Parameters	522		Medium	
Java	Java_Spring	Spring_BCrypt_Insecure_Parameters	522		Medium	
Java	Java_Spring	Spring_CSRF	352		Medium	
Java	Java_Spring	Spring_Missing_Function_Level_Authorization	862		Medium	
Java	Java_Spring	Spring_Missing_HSTS_Header	346		Medium	
Java	Java_Spring	Spring_Missing_Object_Level_Authorization	862		Medium	
Java	Java_Spring	Spring_ModelView_Injection	94		Medium	
Java	Java_Spring	Spring_Scrypt_Insecure_Parameters	522		Medium	
Java	Java_Spring	Spring_Use_of_Broken_or_Risky_Cryptographic_Primitive	327		Medium	
Java	Java_Spring	Spring_Use_Of_Hardcoded_Password	259		Medium	
Java	Java_Stored	Stored_Open_Redirect	601		Medium	
Java	Java_Stored	Stored_XPath_Injection	643		Medium	
Java	Java_Struts	Struts_Form_Does_Not_Extend_Validation_Class	104		Medium	
Java	Java_Struts	Struts_Incomplete_Validate_Method_Definition	103		Medium	
Java	Java_Struts	Struts_Validation_Turned_Off	109		Medium	
Java	Java_Android	Allowed_Backup	530		Low	
Java	Java_Android	Android_Improper_Resource_Shutdown_or_Release	404		Low	
Java	Java_Android	Client_ReDoS_From_Regex_Injection	1333		Low	
Java	Java_Android	Debuggable_App	489		Low	
Java	Java_Android	Information_Leak_Through_Response_Caching	524		Low	
Java	Java_Android	Insecure_Android_SDK_Version	1104		Low	
Java	Java_Android	Insecure_Data_Storage	312		Low	
Java	Java_Android	Insecure_Data_Storage_Usage	312		Low	
Java	Java_Android	Keyboard_Cache_Information_Leak	524		Low	
Java	Java_Android	Missing_Device_Lock_Verification	829		Low	
Java	Java_Android	Missing_Rooted_Device_Check	250		Low	
Java	Java_Android	No_Installer_Verification_Implemented	829		Low	
Java	Java_Android	Non_Encrypted_Data_Storage	922		Low	
Java	Java_Android	Passing_Non_Encrypted_Data_Between_Activities	319		Low	
Java	Java_Android	ProGuard_Obfuscation_Not_In_Use	540		Low	
Java	Java_Android	Reuse_Of_Cryptographic_Key	521		Low	
Java	Java_Android	Unsafe_Permission_Check	732		Low	
Java	Java_Android	Use_of_Native_Language	695		Low	
Java	Java_Android	Use_of_WebView_AddJavascriptInterface	749	Updated	Low	Low
Java	Java_AWS_Lambda	Race_Condition_Global_Scope	1108		Low	
Java	Java_AWS_Lambda	User_Based_SDK_Configurations	15		Low	
Java	Java_Low_Visibility	Citrus_Developer_Mode_Enabled	0		Low	
Java	Java_Low_Visibility	Compromised_CDN	0		Low	
Java	Java_Low_Visibility	Cookie_Overly_Broad_Path	539		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Java	Java_Low_Visibility	Creation_of_Temp_File_in_Dir_with_Incorrect_Permissions	379		Low	
Java	Java_Low_Visibility	Creation_of_Temp_File_With_Insecure_Permissions	378		Low	
Java	Java_Low_Visibility	Divide_By_Zero	369		Low	
Java	Java_Low_Visibility	ESAPI_Same_Password_Repeats_Twice	521		Low	
Java	Java_Low_Visibility	Escape_False	116		Low	
Java	Java_Low_Visibility	File_Permissions_World_Readable	732		Low	
Java	Java_Low_Visibility	Heap_Inspection	244		Low	
Java	Java_Low_Visibility	Improper_Exception_Handling	248		Low	
Java	Java_Low_Visibility	Improper_Resource_Locking	413		Low	
Java	Java_Low_Visibility	Improper_Resource_Shutdown_or_Release	404		Low	
Java	Java_Low_Visibility	Improper_Transaction_Handling	460		Low	
Java	Java_Low_Visibility	Incorrect_Permission_Assignment_For_File_System_Resources	732	Updated	Low	Low
Java	Java_Low_Visibility	Information_Exposure_Through_an_Error_Message	209		Low	
Java	Java_Low_Visibility	Information_Exposure_Through_Debug_Log	532		Low	
Java	Java_Low_Visibility	Information_Exposure_Through_Server_Log	532		Low	
Java	Java_Low_Visibility	Information_Leak_Through_Comments	615		Low	
Java	Java_Low_Visibility	Information_Leak_Through_Persistent_Cookies	539		Low	
Java	Java_Low_Visibility	Information_Leak_Through_Shell_Error_Message	535		Low	
Java	Java_Low_Visibility	Insufficient_Session_Expiration	613		Low	
Java	Java_Low_Visibility	Integer_Overflow	190		Low	
Java	Java_Low_Visibility	Integer_Underflow	191		Low	
Java	Java_Low_Visibility	JWT_Excessive_Expiration_Time	613		Low	
Java	Java_Low_Visibility	JWT_Lack_Of_Expiration_Time	613		Low	
Java	Java_Low_Visibility	Leaving_Temporary_File	377		Low	
Java	Java_Low_Visibility	Log_Forging	117		Low	
Java	Java_Low_Visibility	Logic_Time_Bomb	511		Low	
Java	Java_Low_Visibility	Missing_Content_Security_Policy	346		Low	
Java	Java_Low_Visibility	Missing_Framing_Policy	1021		Low	
Java	Java_Low_Visibility	Missing_Password_Field_Masking	549		Low	
Java	Java_Low_Visibility	Object_Hijack	491		Low	
Java	Java_Low_Visibility	Off_by_One_Error	193		Low	
Java	Java_Low_Visibility	Overly_Permissive_Cross-Origin_Resource_Sharing_Policy	346		Low	
Java	Java_Low_Visibility	Permissive_Content_Security_Policy	346		Low	
Java	Java_Low_Visibility	Portability_Flaw_Locale_Dependent_Comparison	474		Low	
Java	Java_Low_Visibility	Private_Array_Returned_From_A_Public_Method	495		Low	
Java	Java_Low_Visibility	Public_Data_Assigned_to_Private_Array	496		Low	
Java	Java_Low_Visibility	Public_Static_Final_References_Mutable_Object	607		Low	
Java	Java_Low_Visibility	Race_Condition	362		Low	
Java	Java_Low_Visibility	Race_Condition_Format_Flaw	362		Low	
Java	Java_Low_Visibility	Same_Seed_in_PRNG	336		Low	
Java	Java_Low_Visibility	Serializable_Class_Containing_Sensitive_Data	499		Low	
Java	Java_Low_Visibility	Server_Information_Exposure	497		Low	
Java	Java_Low_Visibility	Stored_Log_Forging	117		Low	
Java	Java_Low_Visibility	TOCTOU	367		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Java	Java_Low_Visibility	TruffleHog_HighEntropy_Strings	798		Low	
Java	Java_Low_Visibility	TruffleHog_Regex_Matches	798		Low	
Java	Java_Low_Visibility	Trust_Boundary_Violation_in_Session_Variables	501		Low	
Java	Java_Low_Visibility	Uncaught_Exception	248		Low	
Java	Java_Low_Visibility	Uncontrolled_Format_String	134		Low	
Java	Java_Low_Visibility	Unsynchronized_Access_To_Shared_Data	567		Low	
Java	Java_Low_Visibility	Use_of_Hard_coded_Security_Constants	547		Low	
Java	Java_Low_Visibility	Use_of_RSA_Algorithm_without_OAEP	780		Low	
Java	Java_Low_Visibility	XSS_Evasion_Attack_via_Replace	182		Low	
Java	Java_Spring	Spring_defaultHtmlEscape_Not_True	116		Low	
Java	Java_Spring	Spring_Missing_Content_Security_Policy	346		Low	
Java	Java_Spring	Spring_Missing_Framing_Policy	1021		Low	
Java	Java_Spring	Spring_Overly_Permissive_Cross_Origin_Resource_Sharing_Policy	346	Updated	Low	Low
Java	Java_Spring	Spring_Permissive_Content_Security_Policy	346		Low	
Java	Java_Stored	Stored_Boundary_Violation	646		Low	
Java	Java_Struts	Struts_Duplicate_Config_Files	694		Low	
Java	Java_Struts	Struts_Duplicate_Form_Bean	694		Low	
Java	Java_Struts	Struts_Duplicate_Validation_Files	694		Low	
Java	Java_Struts	Struts_Duplicate_Validation_Forms	102		Low	
Java	Java_Struts	Struts_Form_Field_Without_Validator	105		Low	
Java	Java_Struts	Struts_Mapping_to_Missing_Form_Bean	457		Low	
Java	Java_Struts	Struts_Non_Private_Field_In_ActionForm_Class	608		Low	
Java	Java_Struts	Struts_Thread_Safety_Violation_In_Action_Class	362		Low	
Java	Java_Struts	Struts_Unused_Validation_Form	306		Low	
Java	Java_Struts	Struts_Unvalidated_Action_Form	108		Low	
Java	Java_Struts	Struts_Validator_Without_Form_Field	110		Low	
Java	Java_Struts	Struts2_Action_Field_Without_Validator	108		Low	
Java	Java_Struts	Struts2_Duplicate_Action_Field_Validators	102		Low	
Java	Java_Struts	Struts2_Duplicate_Validators	102		Low	
Java	Java_Android	Exposure_Of_Resource_To_Other_Applications	0		Information	
Java	Java_Android	General_Android_Find_Request_Permissions	0		Information	
Java	Java_Android	Missing_Certificate_Pinning	295		Information	
Java	Java_Android	Unused_Permission	250		Information	
Java	Java_Best_Coding_Practice	Access_Specifier_Manipulation	0		Information	
Java	Java_Best_Coding_Practice	Array_Declared_Public_Final_and_Static	582		Information	
Java	Java_Best_Coding_Practice	Assigning_instead_of_Comparing	481		Information	
Java	Java_Best_Coding_Practice	Call_to_Thread_run	572		Information	
Java	Java_Best_Coding_Practice	Catch_NullPointerException	395		Information	
Java	Java_Best_Coding_Practice	clone_Method_Without_super_clone	580		Information	
Java	Java_Best_Coding_Practice	Comparing_instead_of_Assigning	482		Information	
Java	Java_Best_Coding_Practice	Comparison_of_Classes_By_Name	486		Information	
Java	Java_Best_Coding_Practice	Confusing_Naming	0		Information	
Java	Java_Best_Coding_Practice	Critical_Public_Variable_Without_Final_Modifier	493		Information	
Java	Java_Best_Coding_Practice	Dead_Code	561		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Java	Java_Best_Coding_Practice	Declaration_Of_Catch_For_Generic_Exception	396		Information	
Java	Java_Best_Coding_Practice	Declaration_of_Throws_for_Generic_Exception	397		Information	
Java	Java_Best_Coding_Practice	Detection_of_Error_Condition_Without_Action	390		Information	
Java	Java_Best_Coding_Practice	Direct_Use_of_Sockets	246		Information	
Java	Java_Best_Coding_Practice	Direct_Use_of_Threads	383		Information	
Java	Java_Best_Coding_Practice	Dynamic_File_Inclusion	829		Information	
Java	Java_Best_Coding_Practice	Dynamic_Set_Of_Null_SecurityManager	0		Information	
Java	Java_Best_Coding_Practice	Dynamic_SQL_Queries	89		Information	
Java	Java_Best_Coding_Practice	Empty_Methods	0		Information	
Java	Java_Best_Coding_Practice	Empty_Synchronized_Block	585		Information	
Java	Java_Best_Coding_Practice	Empty_TryBlocks	390		Information	
Java	Java_Best_Coding_Practice	ESAPI_Banned_API	676	Updated	Information	Information
Java	Java_Best_Coding_Practice	Explicit_Call_to_Finalize	586		Information	
Java	Java_Best_Coding_Practice	Exposure_of_Resource_to_Wrong_Sphere	493		Information	
Java	Java_Best_Coding_Practice	Expression_is_Always_False	570		Information	
Java	Java_Best_Coding_Practice	Expression_is_Always_True	571		Information	
Java	Java_Best_Coding_Practice	Failure_to_Catch_All_Exceptions_in_Servlet	600		Information	
Java	Java_Best_Coding_Practice	finalize_Method_Declared_Public	583		Information	
Java	Java_Best_Coding_Practice	finalize_Method_Without_super_finalize	568		Information	
Java	Java_Best_Coding_Practice	GOTO_Statement	0		Information	
Java	Java_Best_Coding_Practice	Hardcoded_Absolute_Path	426	Updated	Information	Information
Java	Java_Best_Coding_Practice	Hardcoded_Connection_String	798		Information	
Java	Java_Best_Coding_Practice	Improper_Initialization	0		Information	
Java	Java_Best_Coding_Practice	Incorrect_Block_Delimitation	483	Updated	Information	Information
Java	Java_Best_Coding_Practice	Incorrect_Conversion_between_Numeric_Types	681		Information	
Java	Java_Best_Coding_Practice	Input_Path_Not_Canonicalized	73	Updated	Information	Information
Java	Java_Best_Coding_Practice	Insufficient_Logging_of_Database_Actions	778		Information	
Java	Java_Best_Coding_Practice	Insufficient_Logging_of_Exceptions	778		Information	
Java	Java_Best_Coding_Practice	Just_One_of_Equals_and_Hash_code_Defined	581		Information	
Java	Java_Best_Coding_Practice	Leftover_Debug_Code	489	Updated	Information	Information
Java	Java_Best_Coding_Practice	Missing_Default_Case_In_Switch_Statement	478		Information	
Java	Java_Best_Coding_Practice	Missing_XML_Validation	112		Information	
Java	Java_Best_Coding_Practice	Non_serializable_Object_Stored_in_Session	579		Information	
Java	Java_Best_Coding_Practice	Not_Static_Final_Logger	0		Information	
Java	Java_Best_Coding_Practice	Omitted_Break_Statement_In_Switch	484		Information	
Java	Java_Best_Coding_Practice	Pages_Without_Global_Error_Handler	544		Information	
Java	Java_Best_Coding_Practice	Portability_Flaw_In_File_Separator	474		Information	
Java	Java_Best_Coding_Practice	Potential_SpringShell	0		Information	
Java	Java_Best_Coding_Practice	Potential_Usage_of_Vulnerable_Log4J	502		Information	
Java	Java_Best_Coding_Practice	Potentially_Serializable_Class_With_Sensitive_Data	499	Updated	Information	Information
Java	Java_Best_Coding_Practice	Public_Static_Field_Not_Marked_Final	500		Information	
Java	Java_Best_Coding_Practice	Redirect_Without_Exit	698		Information	
Java	Java_Best_Coding_Practice	Reliance_On_Untrusted_Inputs_In_Security_Decision	807		Information	
Java	Java_Best_Coding_Practice	Return_Inside_Finally_Block	584		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Java	Java_Best_Coding_Practice	Suspicious_Endpoints	923		Information	
Java	Java_Best_Coding_Practice	Unchecked_Error_Condition	0		Information	
Java	Java_Best_Coding_Practice	Unclosed_Objects	459		Information	
Java	Java_Best_Coding_Practice	Uncontrolled_Recursion	674		Information	
Java	Java_Best_Coding_Practice	Undocumented_API	0		Information	
Java	Java_Best_Coding_Practice	Unsafe_BiDi_Unicode_Data	94		Information	
Java	Java_Best_Coding_Practice	Unsafe_Homoglyphs_Unicode_Data	94		Information	
Java	Java_Best_Coding_Practice	Unused_Variable	563	Updated	Information	Information
Java	Java_Best_Coding_Practice	Use_of_Inner_Class_Containing_Sensitive_Data	492		Information	
Java	Java_Best_Coding_Practice	Use_of_Non_Cryptographic_Random	338		Information	
Java	Java_Best_Coding_Practice	Use_of_Obsolete_Functions	477		Information	
Java	Java_Best_Coding_Practice	Use_of_System_exit	382		Information	
Java	Java_Best_Coding_Practice	Use_of_System_Output_Stream	117		Information	
Java	Java_Best_Coding_Practice	Use_of_Wrong_Operator_in_String_Comparison	597		Information	
Java	Java_Struts	Struts_Missing_Form_Bean_Name	563		Information	
Java	Java_Struts	Struts_Missing_Form_Bean_Type	563		Information	
Java	Java_Struts	Struts_Missing_Forward_Name	693		Information	
Java	Java_Struts	Struts_Unused_Action_Form	563		Information	
Java	Java_Struts	Struts_Use_of_Relative_Path_in_Config	0		Information	
Java	Java_Struts	Struts2_Undeclared_Validator	105		Information	
Java	Java_Struts	Struts2_Validation_File_Without_Action	306		Information	
Java	Java_Struts	Struts2_Validator_Without_Action_Field	110		Information	
JavaScript	JavaScript_AWS_Lambda	DynamoDB_NoSQL_Injection	943		Critical	
JavaScript	Javascript_Lightning	Lightning_Stored_XSS	79		Critical	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Code_Injection	94		Critical	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Command_Injection	77		Critical	
JavaScript	JavaScript_Server_Side_Vulnerabilities	MongoDB_NoSQL_Injection	89		Critical	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Second_Order_SQL_Injection	89		Critical	
JavaScript	JavaScript_Server_Side_Vulnerabilities	SQL_Injection	89		Critical	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Stored_Code_Injection	94		Critical	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Stored_XSS	79		Critical	
JavaScript	JavaScript_XS	XS_Code_Injection	94		Critical	
JavaScript	JavaScript_XS	XS_Second_Order_SQL_Injection	89		Critical	
JavaScript	JavaScript_XS	XS_SQL_Injection	89		Critical	
JavaScript	JavaScript_XS	XS_Stored_Code_Injection	94		Critical	
JavaScript	JavaScript_XS	XS_Stored_XSS	79		Critical	
JavaScript	JavaScript_Angular	Angular_Client_DOM_XSS	79		High	
JavaScript	JavaScript_Angular	Angular_Client_Stored_DOM_XSS	79		High	
JavaScript	JavaScript_Cordova	Cordova_Code_Injection	94		High	
JavaScript	JavaScript_High_Risk	Client_DOM_Code_Injection	94		High	
JavaScript	JavaScript_High_Risk	Client_DOM_Code_Injection_from AJAX	0		High	
JavaScript	JavaScript_High_Risk	Client_DOM_Stored_Code_Injection	94		High	
JavaScript	JavaScript_High_Risk	Client_DOM_Stored_XSS	79		High	
JavaScript	JavaScript_High_Risk	Client_DOM_XSS	79		High	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
JavaScript	JavaScript_High_Risk	Client_DOM_XSS_from AJAX	79		High	
JavaScript	JavaScript_High_Risk	Client_Dynamic_File_Inclusion	829		High	
JavaScript	JavaScript_High_Risk	Client_Resource_Injection	99		High	
JavaScript	JavaScript_High_Risk	Deserialization_of_Untrusted_Data	502		High	
JavaScript	JavaScript_High_Risk	Improper_Restriction_of_XXE_Ref	611		High	
JavaScript	JavaScript_High_Risk	Prototype_Pollution	1321		High	
JavaScript	JavaScript_Jelly	Jelly_Injection	94		High	
JavaScript	JavaScript_Jelly	Jelly_XSS	79		High	
JavaScript	Javascript_Kony	Kony_Code_Injection	94		High	
JavaScript	Javascript_Kony	Kony_Stored_Code_Injection	94		High	
JavaScript	Javascript_Lightning	Lightning_DOM_XSS	79		High	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Absolute_Path_Traversal	36		High	
JavaScript	JavaScript_Server_Side_Vulnerabilities	JWT_No_Signature_Verification	347		High	
JavaScript	JavaScript_Server_Side_Vulnerabilities	JWT_Use_Of_None_Algorithm	287		High	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Reflected_XSS	79		High	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Relative_Path_Traversal	23		High	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Sensitive_Information_Exposure_in_Cleartext_Channel	319		High	
JavaScript	JavaScript_Server_Side_Vulnerabilities	SSRF	918		High	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Stored_Path_Traversal	22		High	
JavaScript	JavaScript_Vue	Vue_DOM_XSS	79		High	
JavaScript	JavaScript_XS	XS_Reflected_XSS	79		High	
JavaScript	JavaScript_AWS_Lambda	Permission_Manipulation_in_S3	281		Medium	
JavaScript	JavaScript_AWS_Lambda	Unrestricted_Delete_S3	639		Medium	
JavaScript	JavaScript_AWS_Lambda	Unrestricted_Read_S3	639		Medium	
JavaScript	JavaScript_AWS_Lambda	Unrestricted_Write_S3	639		Medium	
JavaScript	JavaScript_Cordova	Cordova_File_Disclosure	538		Medium	
JavaScript	JavaScript_Cordova	Cordova_File_Manipulation	552		Medium	
JavaScript	JavaScript_Cordova	Cordova_Open_Redirect	601		Medium	
JavaScript	JavaScript_Cordova	Cordova_Privacy_Violation	359		Medium	
JavaScript	Javascript_Kony	Kony_Hardcoded_EncryptionKey	321		Medium	
JavaScript	Javascript_Kony	Kony_Information_Leakage	319		Medium	
JavaScript	Javascript_Kony	Kony_URL_Injection	601		Medium	
JavaScript	Javascript_Kony	Kony_Use_WeakEncryption	326		Medium	
JavaScript	Javascript_Kony	Kony_Use_WeakHash	328		Medium	
JavaScript	JavaScript_Medium_Threat	AngularJS_SCE_Disabled	116		Medium	
JavaScript	JavaScript_Medium_Threat	Client_Cookies_Inspection	315		Medium	
JavaScript	JavaScript_Medium_Threat	Client_CSS_Injection	83		Medium	
JavaScript	JavaScript_Medium_Threat	Client_DOM_Cookie_Poisoning	472		Medium	
JavaScript	JavaScript_Medium_Threat	Client_DOM_Open_Redirect	601		Medium	
JavaScript	JavaScript_Medium_Threat	Client_Empty_Password	259		Medium	
JavaScript	JavaScript_Medium_Threat	Client_HTML5_Insecure_Storage	312		Medium	
JavaScript	JavaScript_Medium_Threat	Client_HTML5_Store_Sensitive_data_In_Web_Storage	312		Medium	
JavaScript	JavaScript_Medium_Threat	Client_Password_In_Comment	615		Medium	
JavaScript	JavaScript_Medium_Threat	Client_Potential_Code_Injection	94		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
JavaScript	JavaScript_Medium_Threat	Client_Weak_Cryptographic_Hash	327		Medium	
JavaScript	JavaScript_Medium_Threat	Client_XPATH_Injection	643		Medium	
JavaScript	JavaScript_Medium_Threat	Insecure_Value_of_the_SameSite_Cookie_Attribute	1275		Medium	
JavaScript	JavaScript_Medium_Threat	Insufficiently_Protected_Credentials	522		Medium	
JavaScript	JavaScript_Medium_Threat	JWT_Sensitive_Information_Exposure	201		Medium	
JavaScript	JavaScript_Medium_Threat	JWT_Use_Of_Hardcoded_Secret	321		Medium	
JavaScript	JavaScript_Medium_Threat	Missing_HSTS_Header	346		Medium	
JavaScript	JavaScript_Medium_Threat	Not_Using_a_Random_IV	329		Medium	
JavaScript	JavaScript_Medium_Threat	PCI_Data_Exposure	312		Medium	
JavaScript	JavaScript_Medium_Threat	PCI_Data_Exposure_in_JWT	312		Medium	
JavaScript	JavaScript_Medium_Threat	Secret_Leak	312		Medium	
JavaScript	JavaScript_Medium_Threat	Unchecked_Input_For_Loop_Condition	606		Medium	
JavaScript	JavaScript_ReactNative	Clipboard_Information_Leakage	312		Medium	
JavaScript	JavaScript_ReactNative	Insecure_Text_Entry	549		Medium	
JavaScript	JavaScript_ReactNative	Insufficient_Transport_Layer_Security	319		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Cleartext_Storage_Of_Sensitive_Information	312		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Cookie_Poisoning	472		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	CSRF	352		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Dangerous_File_Size_Upload	434		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Excessive_Data_Exposure	201		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Hardcoded_password_in_Connection_String	547		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	HttpOnly_Cookie_Flag_Not_Set	1004	Updated	Medium	Medium
JavaScript	JavaScript_Server_Side_Vulnerabilities	Insecure_Storage_of_Sensitive_Data	922		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Open_Redirect	601		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Parameter_Tampering	472		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Password_Weak_Encryption	261		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Plaintext_Storage_of_a_Password	256		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Poor_Database_Access_Control	862		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Privacy_Violation	359		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	ReDoS_From_Regex_Injection	1333		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Server_DoS_by_Sleep	606		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	SSL_Verification_Bypass	599		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Unchecked_Input_for_Loop_Condition	606		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Unsafe_Object_Binding	915		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Use_Of_Hardcoded_Password	259		Medium	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Use_Of_HTTP_Sensitive_Data_Exposure	319		Medium	
JavaScript	JavaScript_XS	XS_CSRF	352		Medium	
JavaScript	JavaScript_XS	XS_Email_Content_Forgery	113		Medium	
JavaScript	JavaScript_XS	XS_Open_Redirect	601		Medium	
JavaScript	JavaScript_XS	XS_Parameter_Tampering	472		Medium	
JavaScript	JavaScript_XS	XS_Sensitive_Information_Exposure_in_Cleartext_Channel	319		Medium	
JavaScript	JavaScript_Visualforce_Remoting	VF_Remoting_Client_Potential_Code_Injection	94		Medium	
JavaScript	JavaScript_Visualforce_Remoting	VF_Remoting_Client_Potential_XSS	79		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
JavaScript	JavaScript_Angular	Angular_Usage_of_Unsafe_DOM_Sanitizer	116		Low	
JavaScript	JavaScript_AWS_Lambda	Race_Condition_Global_Scope	1108		Low	
JavaScript	JavaScript_AWS_Lambda	User_Based_SDK_Configurations	15		Low	
JavaScript	JavaScript_Cordova	Cordova_Insufficient_Domain_Whitelist	942		Low	
JavaScript	JavaScript_Cordova	Cordova_Missing_Content_Security_Policy	346		Low	
JavaScript	JavaScript_Cordova	Cordova_Permissive_Content_Security_Policy	346		Low	
JavaScript	JavaScript_Kony	Kony_Path_Injection	73		Low	
JavaScript	JavaScript_Kony	Kony_Second_Order_SQL_Injection	89		Low	
JavaScript	JavaScript_Kony	Kony_SQL_Injection	89		Low	
JavaScript	JavaScript_Kony	Kony_Unsecure_Browser_Configuration	15		Low	
JavaScript	JavaScript_Low_Visibility	Client_Cross_Session_Contamination	488		Low	
JavaScript	JavaScript_Low_Visibility	Client_Dangerous_File_Inclusion	829		Low	
JavaScript	JavaScript_Low_Visibility	Client_DoS_By_Sleep	606		Low	
JavaScript	JavaScript_Low_Visibility	Client_HTML5_Information_Exposure	941		Low	
JavaScript	JavaScript_Low_Visibility	Client_Insecure_Randomness	338		Low	
JavaScript	JavaScript_Low_Visibility	Client_JQuery_Deprecated_Symbols	477		Low	
JavaScript	JavaScript_Low_Visibility	Client_Null_Password	259		Low	
JavaScript	JavaScript_Low_Visibility	Client_Overly_Permissive_Message_Posting	201		Low	
JavaScript	JavaScript_Low_Visibility	Client_Potential_DOM_Open_Redirect	601		Low	
JavaScript	JavaScript_Low_Visibility	Client_ReDoS_From_Regex_Injection	1333		Low	
JavaScript	JavaScript_Low_Visibility	Client_ReDoS_In_Match	1333		Low	
JavaScript	JavaScript_Low_Visibility	Client_ReDoS_In_RegExp	1333		Low	
JavaScript	JavaScript_Low_Visibility	Client_ReDoS_In_Replace	1333		Low	
JavaScript	JavaScript_Low_Visibility	Client_Regex_Injection	1333		Low	
JavaScript	JavaScript_Low_Visibility	Client_Server_Empty_Password	259		Low	
JavaScript	JavaScript_Low_Visibility	Client_Use_Of_Iframe_Sandbox_with_Dangerous_Values	829		Low	
JavaScript	JavaScript_Low_Visibility	Client_Use_Of_Iframe_Without_Sandbox	829		Low	
JavaScript	JavaScript_Low_Visibility	Client_Weak_Encryption	327		Low	
JavaScript	JavaScript_Low_Visibility	Client_Weak_Password_Authentication	798		Low	
JavaScript	JavaScript_Low_Visibility	Compromised_CDN	0		Low	
JavaScript	JavaScript_Low_Visibility	CSV_Injection	1236		Low	
JavaScript	JavaScript_Low_Visibility	Deprecated_Modules_or_Libraries	477		Low	
JavaScript	JavaScript_Low_Visibility	Information_Exposure_Through_Query_Strings	522		Low	
JavaScript	JavaScript_Low_Visibility	Missing_Framing_Policy	1021		Low	
JavaScript	JavaScript_Low_Visibility	Overly_Permissive_Cross-Origin_Resource_Sharing_Policy	346		Low	
JavaScript	JavaScript_Low_Visibility	PCI_Data_Exposure_in_Error_Messages	209		Low	
JavaScript	JavaScript_Low_Visibility	PCI_Data_Exposure_in_Files	312		Low	
JavaScript	JavaScript_Low_Visibility	PCI_Data_Exposure_in_Logs	532		Low	
JavaScript	JavaScript_Low_Visibility	PCI_Data_Exposure_in_URL	312		Low	
JavaScript	JavaScript_Low_Visibility	Permissive_Content_Security_Policy	346		Low	
JavaScript	JavaScript_Low_Visibility	Potential_Clickjacking_on_Legacy_Browsers	79		Low	
JavaScript	JavaScript_Low_Visibility	Privacy_Violation_in_Error_Messages	209		Low	
JavaScript	JavaScript_Low_Visibility	Privacy_Violation_in_Files	312		Low	
JavaScript	JavaScript_Low_Visibility	Privacy_Violation_in_JWT	312		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
JavaScript	JavaScript_Low_Visibility	Privacy_Violation_in_Logs	532		Low	
JavaScript	JavaScript_Low_Visibility	Privacy_Violation_in_URL	312		Low	
JavaScript	JavaScript_Low_Visibility	React_Deprecated	477		Low	
JavaScript	JavaScript_Low_Visibility	Secret_Leak_in_Error_Messages	209		Low	
JavaScript	JavaScript_Low_Visibility	Secret_Leak_in_Files	312		Low	
JavaScript	JavaScript_Low_Visibility	Secret_Leak_in_Logs	532		Low	
JavaScript	JavaScript_Low_Visibility	Secret_Leak_in_URL	312		Low	
JavaScript	JavaScript_Low_Visibility	Unsafe_Use_Of_Target_blank	1022		Low	
JavaScript	JavaScript_Low_Visibility	Use_Of_Controlled_Input_On_Sensitive_Field	0		Low	
JavaScript	JavaScript_ReactNative	Missing_Root_Or_Jailbreak_Check	250		Low	
JavaScript	JavaScript_ReactNative	Unencrypted_Sensitive_Data_Storage	922		Low	
JavaScript	JavaScript_SAPUI5	Client_Manual_CSRF_Token_Handling	352		Low	
JavaScript	JavaScript_SAPUI5	SAPUI5_Deprecated_Symbols	1104		Low	
JavaScript	JavaScript_SAPUI5	SAPUI5_Potential_Malicious_File_Upload	434		Low	
JavaScript	JavaScript_SAPUI5	SAPUI5_Use_Of_Hardcoded_URL	200		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Divide_By_Zero	369		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Information_Exposure_Through_an_Error_Message	209		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Information_Exposure_Through_Directory_Listing	548		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Information_Exposure_Through-Headers	200		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Information_Exposure_Through_Log_Files	532		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	JWT_Excessive_Expiration_Time	613		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	JWT_Lack_Of_Expiration_Time	613		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	JWT_No_Expiration_Time_Validation	613		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	JWT_No_NotBefore_Validation	304		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Log_Forging	117		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Missing_CSP_Header	346		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Null_Password	252		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Use_of_Deprecated_or_Obsolete_Functions	477		Low	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Use_of_Insufficiently_Random_Values	338		Low	
JavaScript	JavaScript_XS	XS_Log_Injection	117		Low	
JavaScript	JavaScript_XS	XS_Overly_Permissive_CORS	749		Low	
JavaScript	JavaScript_XS	XS_Potentially_Vulnerable_To_Clickjacking	79		Low	
JavaScript	JavaScript_XS	XS_Use_Of_Hardcoded_URL	798		Low	
JavaScript	JavaScript_Best_Coding_Practice	Angular_Deprecated_API	477		Information	
JavaScript	JavaScript_Best_Coding_Practice	Avoid_the_Use_of_FinalizationRegistry	0		Information	
JavaScript	JavaScript_Best_Coding_Practice	Avoid_the_Use_of_WeakRef	0		Information	
JavaScript	JavaScript_Best_Coding_Practice	Client_HTML5_Easy_To_Guess_Database_Name	0		Information	
JavaScript	JavaScript_Best_Coding_Practice	Client_Negative_Content_Length	0		Information	
JavaScript	JavaScript_Best_Coding_Practice	Client_Potential_XSS	79		Information	
JavaScript	JavaScript_Best_Coding_Practice	Client_Untrusted_Activex	618		Information	
JavaScript	JavaScript_Best_Coding_Practice	Hardcoded_Absolute_Path	426		Information	
JavaScript	JavaScript_Best_Coding_Practice	React_Multiple_Classes_With_Same_Name	694		Information	
JavaScript	JavaScript_Best_Coding_Practice	Use_Of_Multiple_Mixins	0		Information	
JavaScript	Javascript_Kony	Kony_Deprecated_Functions	477		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
JavaScript	Javascript_Lightning	Lightning_Aura_Attribute_With_Object_Type	0		Information	
JavaScript	Javascript_Lightning	Lightning_Component_Bad_Naming	0		Information	
JavaScript	Javascript_Lightning	Lightning_Data_Retrieval_Without_Wire_Decorator	0		Information	
JavaScript	Javascript_Lightning	Lightning_Dynamic_Href_In_Anchor_Tag	0		Information	
JavaScript	Javascript_Lightning	Lightning_Use_of_Aura_Component	0		Information	
JavaScript	Javascript_Lightning	Lightning_Use_of_LWC_Event_Bubbling	0		Information	
JavaScript	Javascript_Lightning	Lightning_Use_of_Same_Controller_Method_In_Different_Components	0		Information	
JavaScript	JavaScript_SAPUI5	Client_Manual_XHR_Handling	474		Information	
JavaScript	JavaScript_SAPUI5	SAPUI5_Custom_OData_Model	474		Information	
JavaScript	JavaScript_SAPUI5	SAPUI5_OData_Call_Without_Batch_Mode	474		Information	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Comparing_instead_of_Assigning	482		Information	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Dynamic_File_Inclusion	829		Information	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Expression_is_Always_False	570		Information	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Expression_is_Always_True	571		Information	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Missing_Default_Case_In_Switch_Statement	478		Information	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Omitted_Break_Statement_In_Switch	484		Information	
JavaScript	JavaScript_Server_Side_Vulnerabilities	Uncontrolled_Format_String	134		Information	
JavaScript	JavaScript_Vue	Declaration_of_Multiple_Vue_Components_per_File	0		Information	
JavaScript	JavaScript_Vue	Declaration_of_Vue_Component_Data_as_Property	0		Information	
JavaScript	JavaScript_Vue	Inconsistent_Component_Top_Level_Elements_Ordering	0		Information	
JavaScript	JavaScript_Vue	Inconsistent_use_of_Directive_Shorthands	0		Information	
JavaScript	JavaScript_Vue	Use_of_Implicit_Types_on_Vue_Component_Props	0		Information	
JavaScript	JavaScript_Vue	Use_of_Single_Word_Named_Vue_Components	0		Information	
JavaScript	JavaScript_Vue	Use_of_vif_and_vfor_On_Same_Element	0		Information	
Kotlin	Kotlin_Critical_Risk	Code_Injection	94		Critical	
Kotlin	Kotlin_Critical_Risk	Command_Injection	77		Critical	
Kotlin	Kotlin_Critical_Risk	Expression_Language_Injection_MVEL	917		Critical	
Kotlin	Kotlin_Critical_Risk	Expression_Language_Injection_SPEL	917		Critical	
Kotlin	Kotlin_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
Kotlin	Kotlin_Critical_Risk	SQL_Injection	89		Critical	
Kotlin	Kotlin_Critical_Risk	Stored_Command_Injection	77		Critical	
Kotlin	Kotlin_Critical_Risk	Stored_XSS	79		Critical	
Kotlin	Kotlin_Spring	Spring_View_Manipulation	917		Critical	
Kotlin	Kotlin_Android	Insecure_WebView_Usage	829		High	
Kotlin	Kotlin_Android	Sensitive_Information_Exposure_in_Cleartext_Channel	319		High	
Kotlin	Kotlin_High_Risk	Cleartext_Submission_of_Sensitive_Information	319		High	
Kotlin	Kotlin_High_Risk	Connection_String_Injection	99		High	
Kotlin	Kotlin_High_Risk	Deserialization_of_Untrusted_Data	502		High	
Kotlin	Kotlin_High_Risk	JWT_No_Signature_Verification	347		High	
Kotlin	Kotlin_High_Risk	JWT_Use_Of_None_Algorithm	287		High	
Kotlin	Kotlin_High_Risk	LDAP_Injection	90		High	
Kotlin	Kotlin_High_Risk	Reflected_XSS	79		High	
Kotlin	Kotlin_High_Risk	SSRF	918		High	
Kotlin	Kotlin_High_Risk	Stored_LDAP_Injection	90		High	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Kotlin	Kotlin_High_Risk	Unsafe_Reflection	470		High	
Kotlin	Kotlin_Android	Client_Side_Injection	89		Medium	
Kotlin	Kotlin_Android	Communication_Over_HTTP	319		Medium	
Kotlin	Kotlin_Android	Copy_Paste_Buffer_Caching	922		Medium	
Kotlin	Kotlin_Android	Exported_Content_Provider_Without_Protective_Permissions	276		Medium	
Kotlin	Kotlin_Android	Exported_Service_Without_Protective_Permissions	276		Medium	
Kotlin	Kotlin_Android	Hardcoded_Password_In_Gradle	259		Medium	
Kotlin	Kotlin_Android	Implicit_Intent_With_Read_Write_Permissions	276		Medium	
Kotlin	Kotlin_Android	Improper_Certificate_Validation	295		Medium	
Kotlin	Kotlin_Android	Improper_Verification_Of_Intent_By_Broadcast_Receiver	925		Medium	
Kotlin	Kotlin_Android	Insecure_HTTP_Connections_Enabled	319		Medium	
Kotlin	Kotlin_Android	Privacy_Violation	359		Medium	
Kotlin	Kotlin_Android	Screen_Caching	524		Medium	
Kotlin	Kotlin_Android	Use_Of_Implicit_Intent_For_Sensitive_Communication	927		Medium	
Kotlin	Kotlin_Android	WebView_Cache_Information_Leak	524		Medium	
Kotlin	Kotlin_Medium_Threat	Command_Argument_Injection	88		Medium	
Kotlin	Kotlin_Medium_Threat	DoS_by_Sleep	606		Medium	
Kotlin	Kotlin_Medium_Threat	Excessive_Data_Exposure	201		Medium	
Kotlin	Kotlin_Medium_Threat	Frameable_Login_Page	829		Medium	
Kotlin	Kotlin_Medium_Threat	Hardcoded_password_in_Connection_String	547		Medium	
Kotlin	Kotlin_Medium_Threat	HttpOnly_Cookie_Flag_Not_Set	1004		Medium	
Kotlin	Kotlin_Medium_Threat	Improper_Locking	667		Medium	
Kotlin	Kotlin_Medium_Threat	JWT_Sensitive_Information_Exposure	201		Medium	
Kotlin	Kotlin_Medium_Threat	JWT_Use_Of_Hardcoded_Secret	321		Medium	
Kotlin	Kotlin_Medium_Threat	Missing_HSTS_Header	346		Medium	
Kotlin	Kotlin_Medium_Threat	Parameter_Tampering	472		Medium	
Kotlin	Kotlin_Medium_Threat	Password_In_Comment	615		Medium	
Kotlin	Kotlin_Medium_Threat	Plaintext_Storage_of_a_Password	256		Medium	
Kotlin	Kotlin_Medium_Threat	Privacy_Violation	359		Medium	
Kotlin	Kotlin_Medium_Threat	Reliance_on_Cookies_without_Validation	565		Medium	
Kotlin	Kotlin_Medium_Threat	Resource_Injection	99		Medium	
Kotlin	Kotlin_Medium_Threat	Secure_Cookie_Flag_Not_Set	614		Medium	
Kotlin	Kotlin_Medium_Threat	Stored_Command_Argument_Injection	88		Medium	
Kotlin	Kotlin_Medium_Threat	Unchecked_Input_for_Loop_Condition	606		Medium	
Kotlin	Kotlin_Medium_Threat	Unsafe_Object_Binding	915		Medium	
Kotlin	Kotlin_Medium_Threat	Use_of_a_One_Way_Hash_with_a_Predictable_Salt	760		Medium	
Kotlin	Kotlin_Medium_Threat	Use_of_a_One_Way_Hash_without_a_Salt	759		Medium	
Kotlin	Kotlin_Medium_Threat	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327		Medium	
Kotlin	Kotlin_Medium_Threat	Use_of_Cryptographically_Weak_PRNG	338		Medium	
Kotlin	Kotlin_Medium_Threat	Use_of_Hardcoded_Cryptographic_Key	321		Medium	
Kotlin	Kotlin_Medium_Threat	Use_of_Hardcoded_Password	259		Medium	
Kotlin	Kotlin_Medium_Threat	Use_of_Unsafe_JNI	111		Medium	
Kotlin	Kotlin_Medium_Threat	XPath_Injection	643		Medium	
Kotlin	Kotlin_Spring	Spring_ModelView_Injection	94		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Kotlin	Kotlin_Android	Allowed_Backup	530		Low	
Kotlin	Kotlin_Android	Client_ReDoS_From_Regex_Injection	1333		Low	
Kotlin	Kotlin_Android	Debuggable_App	489		Low	
Kotlin	Kotlin_Android	DeviceId_Authentication	259		Low	
Kotlin	Kotlin_Android	Insecure_Android_SDK_Version	1104		Low	
Kotlin	Kotlin_Android	Insecure_Sensitive_Data_Storage	295		Low	
Kotlin	Kotlin_Android	Missing_Rooted_Device_Check	250		Low	
Kotlin	Kotlin_Android	Non_Encrypted_Data_Storage	922		Low	
Kotlin	Kotlin_Android	Passing_Non_Encrypted_Data_Between_Activities	319		Low	
Kotlin	Kotlin_Android	ProGuard_Obfuscation_Not_In_Use	540		Low	
Kotlin	Kotlin_Android	Reuse_of_Cryptographic_Key	521		Low	
Kotlin	Kotlin_Android	Unsafe_Permission_Check	732		Low	
Kotlin	Kotlin_Android	Use_of_WebView_AddJavascriptInterface	749		Low	
Kotlin	Kotlin_Low_Visibility	Compromised_CDN	0		Low	
Kotlin	Kotlin_Low_Visibility	Deprecated_Functions_or_Properties	477	Updated	Low	Low
Kotlin	Kotlin_Low_Visibility	JWT_Excessive_Expiration_Time	613		Low	
Kotlin	Kotlin_Low_Visibility	JWT_Lack_Of_Expiration_Time	613		Low	
Kotlin	Kotlin_Low_Visibility	Same_Seed_in_PRNG	336		Low	
Kotlin	Kotlin_Low_Visibility	Use_of_RSA_Algorithm_without_OAEP	780		Low	
Kotlin	Kotlin_Android	Insecure_Cipher_Mode	326		Information	
Kotlin	Kotlin_Android	Unused_Permission	250		Information	
Kotlin	Kotlin_Android	Webview_DOM_XSS	79		Information	
Kotlin	Kotlin_Best_Coding_Practice	Potential_Usage_of_Vulnerable_Log4J	502		Information	
Kotlin	Kotlin_Best_Coding_Practice	Use_of_Non_Cryptographic_Random	338		Information	
Lua	Lua_Critical_Risk	Arbitrary_File_Write	669		Critical	
Lua	Lua_Critical_Risk	Code_Injection	94		Critical	
Lua	Lua_Critical_Risk	Command_Injection	77		Critical	
Lua	Lua_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
Lua	Lua_Critical_Risk	SQL_Injection	89		Critical	
Lua	Lua_Critical_Risk	Stored_Code_Injection	94		Critical	
Lua	Lua_Critical_Risk	Stored_Command_Injection	77		Critical	
Lua	Lua_Critical_Risk	Stored_XSS	79		Critical	
Lua	Lua_High_Risk	Absolute_Path_Traversal	36		High	
Lua	Lua_High_Risk	Connection_String_Injection	99		High	
Lua	Lua_High_Risk	Dangerous_File_Inclusion	829		High	
Lua	Lua_High_Risk	Deserialization_of_Untrusted_Data	502		High	
Lua	Lua_High_Risk	JWT_No_Signature_Verification	347		High	
Lua	Lua_High_Risk	Reflected_XSS	79		High	
Lua	Lua_High_Risk	Relative_Path_Traversal	23		High	
Lua	Lua_High_Risk	SSRF	918		High	
Lua	Lua_Medium_Threat	Broken_or_Risky_Encryption_Algorithm	327		Medium	
Lua	Lua_Medium_Threat	Broken_or_Risky_Hashing_Function	327		Medium	
Lua	Lua_Medium_Threat	Command_Argument_Injection	88		Medium	
Lua	Lua_Medium_Threat	CSRF	352		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Lua	Lua_Medium_Threat	DoS_by_Sleep	606		Medium	
Lua	Lua_Medium_Threat	DoS_from_Evil_Regex	1333		Medium	
Lua	Lua_Medium_Threat	DoS_from_RegEx_Injection	1333		Medium	
Lua	Lua_Medium_Threat	Empty_password_in_Connection_String	521		Medium	
Lua	Lua_Medium_Threat	Encoding_Used_Instead_of_Encryption	326		Medium	
Lua	Lua_Medium_Threat	Excessive_Data_Exposure	201		Medium	
Lua	Lua_Medium_Threat	Hardcoded_AWS_Credentials	798		Medium	
Lua	Lua_Medium_Threat	Hardcoded_Cryptographic_IV	326		Medium	
Lua	Lua_Medium_Threat	Hardcoded_Cryptographic_Key	321		Medium	
Lua	Lua_Medium_Threat	Hardcoded_password_in_Connection_String	547		Medium	
Lua	Lua_Medium_Threat	Hardcoded_Salt	760		Medium	
Lua	Lua_Medium_Threat	Hashing_Length_Extension_Attack	326		Medium	
Lua	Lua_Medium_Threat	HttpOnly_Cookie_Flag_Not_Set	1004		Medium	
Lua	Lua_Medium_Threat	Insecure_Asymmetric_Cryptographic_Algorithm_Parameters	326		Medium	
Lua	Lua_Medium_Threat	Insecure_Value_of_the_SameSite_Cookie_Attribute	1275		Medium	
Lua	Lua_Medium_Threat	Insufficiently_Secure_Password_Storage_Algorithm_Parameters	522		Medium	
Lua	Lua_Medium_Threat	JWT_Use_Of_Hardcoded_Secret	321		Medium	
Lua	Lua_Medium_Threat	Misconfigured_HSTS_Header	346		Medium	
Lua	Lua_Medium_Threat	Missing_HSTS_Header	346		Medium	
Lua	Lua_Medium_Threat	Open_Redirect	601		Medium	
Lua	Lua_Medium_Threat	Parameter_Tampering	472		Medium	
Lua	Lua_Medium_Threat	Password_In_Comment	615		Medium	
Lua	Lua_Medium_Threat	Plaintext_Storage_of_a_Password	256		Medium	
Lua	Lua_Medium_Threat	Privacy_Violation	359		Medium	
Lua	Lua_Medium_Threat	Reliance_on_Reverse_DNS_Lookups_in_an_Action	350		Medium	
Lua	Lua_Medium_Threat	Resource_Injection	99		Medium	
Lua	Lua_Medium_Threat	Secret_Leak	312		Medium	
Lua	Lua_Medium_Threat	Secret_Leak_in_JWT	312		Medium	
Lua	Lua_Medium_Threat	Secure_Cookie_Flag_Not_Set	614		Medium	
Lua	Lua_Medium_Threat	Sensitive_Information_Exposure_in_Cleartext_Channel	319		Medium	
Lua	Lua_Medium_Threat	Session_Fixation	384		Medium	
Lua	Lua_Medium_Threat	SSL_Verification_Bypass	599		Medium	
Lua	Lua_Medium_Threat	Stored_Absolute_Path_Traversal	36		Medium	
Lua	Lua_Medium_Threat	Stored_Command_Argument_Injection	88		Medium	
Lua	Lua_Medium_Threat	Stored_Dangerous_File_Inclusion	829		Medium	
Lua	Lua_Medium_Threat	Stored_Relative_Path_Traversal	23		Medium	
Lua	Lua_Medium_Threat	Unchecked_Input_for_Loop_Condition	606		Medium	
Lua	Lua_Medium_Threat	Uncontrolled_Memory_Allocation	789		Medium	
Lua	Lua_Medium_Threat	Unrestricted_Read_S3	639		Medium	
Lua	Lua_Medium_Threat	Use_of_Cryptographically_Weak_PRNG	338		Medium	
Lua	Lua_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
Lua	Lua_Medium_Threat	Use_Of_Hardcoded_Password_In_Config	260		Medium	
Lua	Lua_Medium_Threat	Using_Referer_Field_for_Authentication	293		Medium	
Lua	Lua_Low_Visibility	Compromised_CDN	0		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Lua	Lua_Low_Visibility	Cookie_Overly_Broad_Path	539		Low	
Lua	Lua_Low_Visibility	Dangerous_File_Extension	434		Low	
Lua	Lua_Low_Visibility	Exposure_of_System_Data	497		Low	
Lua	Lua_Low_Visibility	Heap_Inspection	244		Low	
Lua	Lua_Low_Visibility	Improper_Exception_Handling	248		Low	
Lua	Lua_Low_Visibility	Improper_Resource_Shutdown_or_Release	404		Low	
Lua	Lua_Low_Visibility	Information_Exposure_Through_Server_Log	532		Low	
Lua	Lua_Low_Visibility	Insufficient_Session_Expiration	613		Low	
Lua	Lua_Low_Visibility	JWT_Excessive_Expiration_Time	613		Low	
Lua	Lua_Low_Visibility	JWT_Lack_of_Expiration_Time	613		Low	
Lua	Lua_Low_Visibility	JWT_No_Expiration_Time_Validation	613		Low	
Lua	Lua_Low_Visibility	JWT_No_NotBefore_Validation	304		Low	
Lua	Lua_Low_Visibility	Leaving_Temporary_File	377		Low	
Lua	Lua_Low_Visibility	Log_Forging	117		Low	
Lua	Lua_Low_Visibility	Missing_Content_Security_Policy	346		Low	
Lua	Lua_Low_Visibility	Missing_Framing_Policy	1021		Low	
Lua	Lua_Low_Visibility	Missing_Password_Field_Masking	549		Low	
Lua	Lua_Low_Visibility	Null_Pointer_Dereference	476		Low	
Lua	Lua_Low_Visibility	Overly_Permissive_Cross_Origin_Resource_Sharing_Policy	346		Low	
Lua	Lua_Low_Visibility	Path_Traversal_Evasion_Attack_via_Replace	36		Low	
Lua	Lua_Low_Visibility	PCI_Data_Exposure	312		Low	
Lua	Lua_Low_Visibility	PCI_Data_Exposure_in_Error_Messages	209		Low	
Lua	Lua_Low_Visibility	PCI_Data_Exposure_in_Files	312		Low	
Lua	Lua_Low_Visibility	PCI_Data_Exposure_in_JWT	312		Low	
Lua	Lua_Low_Visibility	PCI_Data_Exposure_in_Logs	532		Low	
Lua	Lua_Low_Visibility	PCI_Data_Exposure_in_URL	312		Low	
Lua	Lua_Low_Visibility	Permissive_Content_Security_Policy	346		Low	
Lua	Lua_Low_Visibility	Privacy_Violation_in_Error_Messages	209		Low	
Lua	Lua_Low_Visibility	Privacy_Violation_in_Files	312		Low	
Lua	Lua_Low_Visibility	Privacy_Violation_in_JWT	312		Low	
Lua	Lua_Low_Visibility	Privacy_Violation_in_Logs	532		Low	
Lua	Lua_Low_Visibility	Privacy_Violation_in_URL	312		Low	
Lua	Lua_Low_Visibility	Race_Condition	362		Low	
Lua	Lua_Low_Visibility	Secret_Leak_in_Error_Messages	209		Low	
Lua	Lua_Low_Visibility	Secret_Leak_in_Files	312		Low	
Lua	Lua_Low_Visibility	Secret_Leak_in_Logs	532		Low	
Lua	Lua_Low_Visibility	Secret_Leak_in_URL	312		Low	
Lua	Lua_Low_Visibility	Server_Information_Exposure	497		Low	
Lua	Lua_Low_Visibility	Server_Information_Exposure_via_Misconfiguration	312		Low	
Lua	Lua_Low_Visibility	Trust_Boundary_Violation_in_Session_Variables	501		Low	
Lua	Lua_Low_Visibility	Uncontrolled_Format_String	134		Low	
Lua	Lua_Low_Visibility	XSS_Evasion_Attack_via_Replace	182		Low	
Lua	Lua_Best_Coding_Practice	Use_of_Evil_Regex	0		Information	
Lua	Lua_Best_Coding_Practice	Use_of_Native_Language	695		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Lua	Lua_Best_Coding_Practice	Use_of_Non_Cryptographic_Random	338		Information	
Markup	Markup_High_Risk	Secrets_Exposure	0		High	
Objc	ObjectiveC_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
Objc	ObjectiveC_Critical_Risk	SQL_Injection	89		Critical	
Objc	ObjectiveC_Critical_Risk	Stored_XSS	79		Critical	
Objc	Apple_Secure_Coding_Guide	Buffer_Size_Literal_Overflow	121		High	
Objc	Apple_Secure_Coding_Guide	NSPredicate_Injection_Via_Deserialization	502		High	
Objc	Apple_Secure_Coding_Guide	Unsecure_Deserialization	502		High	
Objc	ObjectiveC_High_Risk	Format_String_Attack	134		High	
Objc	ObjectiveC_High_Risk	Insufficient_Transport_Layer_Input	319		High	
Objc	ObjectiveC_High_Risk	Insufficient_Transport_Layer_Output	319		High	
Objc	ObjectiveC_High_Risk	Reflected_XSS_All_Clients	79		High	
Objc	ObjectiveC_High_Risk	Unsafe_Reflection	470		High	
Objc	ObjectiveC_High_Risk	Use_of_Hardcoded_Cryptographic_Key	321		High	
Objc	Apple_Secure_Coding_Guide	Improper_Implementation_of_NSSecureCoding	502		Medium	
Objc	Apple_Secure_Coding_Guide	NSPredicate_Injection	134		Medium	
Objc	ObjectiveC_Medium_Threat	Autocorrection_Keystroke_Logging	359		Medium	
Objc	ObjectiveC_Medium_Threat	Cut_And_Paste_Leakage	922		Medium	
Objc	ObjectiveC_Medium_Threat	Improper_Certificate_Validation	295		Medium	
Objc	ObjectiveC_Medium_Threat	Information_Exposure_Through_Extension	359		Medium	
Objc	ObjectiveC_Medium_Threat	Information_Exposure_Through_Query_String	598		Medium	
Objc	ObjectiveC_Medium_Threat	Insecure_Data_Storage	312		Medium	
Objc	ObjectiveC_Medium_Threat	Password_In_Comment	615		Medium	
Objc	ObjectiveC_Medium_Threat	Plain_Text_Transport_Layer	319		Medium	
Objc	ObjectiveC_Medium_Threat	Poor_Authorization_and_Authentication	306		Medium	
Objc	ObjectiveC_Medium_Threat	ReDoS_From_Regex_Injection	1333		Medium	
Objc	ObjectiveC_Medium_Threat	Screen_Caching	524		Medium	
Objc	ObjectiveC_Medium_Threat	Third_Party_Keyboard_Enabled	829		Medium	
Objc	ObjectiveC_Medium_Threat	Third_Party_Keyboards_On_Sensitive_Field	829		Medium	
Objc	ObjectiveC_Medium_Threat	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327		Medium	
Objc	ObjectiveC_Medium_Threat	Use_of_Hardcoded_Password	259		Medium	
Objc	Apple_Secure_Coding_Guide	Jailbreak_File_Referenced_By_Name	379		Low	
Objc	Apple_Secure_Coding_Guide	Jailbreak_Unchecked_File_Operation_Result_Code	252		Low	
Objc	Apple_Secure_Coding_Guide	Path_Manipulation	73		Low	
Objc	Apple_Secure_Coding_Guide	Signed_Memory_Arithmetic	190		Low	
Objc	Apple_Secure_Coding_Guide	Unscrubbed_Secret	226		Low	
Objc	Apple_Secure_Coding_Guide	URL_Injection	74		Low	
Objc	ObjectiveC_Low_Visibility	Allowed_Backup	530		Low	
Objc	ObjectiveC_Low_Visibility	App_Transport_Security_Disabled	319		Low	
Objc	ObjectiveC_Low_Visibility	Compromised_CDN	0		Low	
Objc	ObjectiveC_Low_Visibility	Empty_Password	521		Low	
Objc	ObjectiveC_Low_Visibility	Functions_Apple_Recommends_To_Avoid	477		Low	
Objc	ObjectiveC_Low_Visibility	Improper_Resource_Shutdown_or_Release	404		Low	
Objc	ObjectiveC_Low_Visibility	Information_Exposure_Through_an_Error_Message	209		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Objc	ObjectiveC_Low_Visibility	Information_Leak_Through_Response_Caching	524		Low	
Objc	ObjectiveC_Low_Visibility	Insufficient_Encryption_Key_Size	326		Low	
Objc	ObjectiveC_Low_Visibility	iOS_Improper_Resource_Release_Shutdown	404		Low	
Objc	ObjectiveC_Low_Visibility	Log_Forging	117		Low	
Objc	ObjectiveC_Low_Visibility	Memory_Leak	401		Low	
Objc	ObjectiveC_Low_Visibility	Missing_Device_Lock_Verification	829		Low	
Objc	ObjectiveC_Low_Visibility	Missing_Jailbreak_Check	250		Low	
Objc	ObjectiveC_Low_Visibility	Null_Password	252		Low	
Objc	ObjectiveC_Low_Visibility	Path_Traversal	22		Low	
Objc	ObjectiveC_Low_Visibility	Sensitive_Data_In_Temp_Folders	377		Low	
Objc	ObjectiveC_Low_Visibility	Use_of_Insufficiently_Random_Values	338		Low	
Objc	ObjectiveC_Low_Visibility	Use_of_Obsolete_Functions	477		Low	
Objc	ObjectiveC_Low_Visibility	XML_External_Entity	611		Low	
Objc	Apple_Secure_Coding_Guide	Buffer_Size_Literal	121		Information	
Objc	Apple_Secure_Coding_Guide	Buffer_Size_Literal_Condition	121		Information	
Objc	Apple_Secure_Coding_Guide	UDP_Protocol_Used	0		Information	
Objc	Apple_Secure_Coding_Guide	Unchecked_CString_Conversion	252		Information	
Objc	ObjectiveC_Best_Coding_Practice	Dead_Code	561		Information	
Objc	ObjectiveC_Best_Coding_Practice	Dynamic_SQL_Queries	89		Information	
Objc	ObjectiveC_Best_Coding_Practice	Empty_Methods	0		Information	
Objc	ObjectiveC_Best_Coding_Practice	Expression_is_Always_False	570		Information	
Objc	ObjectiveC_Best_Coding_Practice	Expression_is_Always_True	571		Information	
Objc	ObjectiveC_Best_Coding_Practice	Incorrect_Initialization	456		Information	
Objc	ObjectiveC_Best_Coding_Practice	Missing_Certificate_Pinning	295		Information	
Objc	ObjectiveC_Best_Coding_Practice	Missing_Colon_In_Selector	483		Information	
Objc	ObjectiveC_Best_Coding_Practice	Unchecked_Return_Value	252		Information	
Perl	Perl_Critical_Risk	Code_Injection	94		Critical	
Perl	Perl_Critical_Risk	Command_Injection	77		Critical	
Perl	Perl_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
Perl	Perl_Critical_Risk	SQL_Injection	89		Critical	
Perl	Perl_Critical_Risk	Stored_Code_Injection	94		Critical	
Perl	Perl_Critical_Risk	Stored_Command_Injection	77		Critical	
Perl	Perl_Critical_Risk	Stored_XSS	79		Critical	
Perl	Perl_High_Risk	Connection_String_Injection	99		High	
Perl	Perl_High_Risk	Dangerous_File_Inclusion	829		High	
Perl	Perl_High_Risk	Improper_Restriction_of_XXE_Ref	611		High	
Perl	Perl_High_Risk	LDAP_Injection	90		High	
Perl	Perl_High_Risk	Path_Traversal	22		High	
Perl	Perl_High_Risk	Reflected_XSS	79		High	
Perl	Perl_High_Risk	Stored_LDAP_Injection	90		High	
Perl	Perl_High_Risk	Stored_Path_Traversal	22		High	
Perl	Perl_High_Risk	Unprotected_Transport_of_Credentials	523		High	
Perl	Perl_Medium_Threat	CSRF	352		Medium	
Perl	Perl_Medium_Threat	DoS_by_Sleep	606		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Perl	Perl_Medium_Threat	Parameter_Tampering	472		Medium	
Perl	Perl_Medium_Threat	Privacy_Violation	359		Medium	
Perl	Perl_Medium_Threat	Resource_Injection	99		Medium	
Perl	Perl_Medium_Threat	Uncontrolled_Format_String	134		Medium	
Perl	Perl_Medium_Threat	Uncontrolled_Memory_Allocation	789		Medium	
Perl	Perl_Medium_Threat	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327		Medium	
Perl	Perl_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
Perl	Perl_Low_Visibility	Compromised_CDN	0		Low	
Perl	Perl_Low_Visibility	Deprecated_Functions_or_Properties	477		Low	
Perl	Perl_Low_Visibility	Deprecated_Modules_or_Libraries	477		Low	
Perl	Perl_Low_Visibility	Improper_Filtering_of_Special_Elements	790		Low	
Perl	Perl_Low_Visibility	Information_Exposure_Through_an_Error_Message	209		Low	
Perl	Perl_Low_Visibility	Log_Forging	117		Low	
Perl	Perl_Low_Visibility	Not_Checking_Regular_Expressions_Results	252		Low	
Perl	Perl_Low_Visibility	Overloading_Reserved_Keywords_or_Subroutines	627		Low	
Perl	Perl_Low_Visibility	Permissive_Regular_Expression	625		Low	
Perl	Perl_Low_Visibility	Prohibit_Indirect_Object_Call_Syntax	665		Low	
Perl	Perl_Low_Visibility	Signifying_Inheritance_At_Runtime	0		Low	
Perl	Perl_Low_Visibility	Use_of_Two_Argument_Form_of_Open	77		Low	
Perl	Perl_Low_Visibility	Variables_Outside_The_Scope_of_a_Regex	824		Low	
Perl	Perl_Best_Coding_Practice	Empty_Methods	0		Information	
Perl	Perl_Best_Coding_Practice	Hardcoded_Absolute_Path	426		Information	
Perl	Perl_Best_Coding_Practice	Prepending_Leading_Zeroes_To_Integer_Literals	0		Information	
Perl	Perl_Best_Coding_Practice	Reusing_Variable_Names_In_Subscopes	0		Information	
Perl	Perl_Best_Coding_Practice	Unchecked_Return_Value	252		Information	
Perl	Perl_Best_Coding_Practice	Using_Perl4_Package_Names	477		Information	
Perl	Perl_Best_Coding_Practice	Using_Subroutine_Prototypes	628		Information	
PHP	PHP_Critical_Risk	Code_Injection	94		Critical	
PHP	PHP_Critical_Risk	Command_Injection	77		Critical	
PHP	PHP_Critical_Risk	MongoDB_NoSQL_Injection	89		Critical	
PHP	PHP_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
PHP	PHP_Critical_Risk	Server_Side_Template_Injection	1336		Critical	
PHP	PHP_Critical_Risk	SQL_Injection	89		Critical	
PHP	PHP_Critical_Risk	SSTI_Twig	1336		Critical	
PHP	PHP_Critical_Risk	Stored_Code_Injection	94		Critical	
PHP	PHP_Critical_Risk	Stored_Command_Injection	77		Critical	
PHP	PHP_Critical_Risk	Stored_XSS	79		Critical	
PHP	PHP_High_Risk	Absolute_Path_Traversal	36		High	
PHP	PHP_High_Risk	Dangerous_File_Extension	434		High	
PHP	PHP_High_Risk	Dangerous_File_Inclusion	829		High	
PHP	PHP_High_Risk	Deserialization_of_Untrusted_Data	502		High	
PHP	PHP_High_Risk	Improper_Restriction_of_Stored_XXE_Ref	611		High	
PHP	PHP_High_Risk	Improper_Restriction_of_XXE_Ref	611		High	
PHP	PHP_High_Risk	JWT_No_Signature_Verification	347		High	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
PHP	PHP_High_Risk	JWT_Use_Of_None_Algorithm	287		High	
PHP	PHP_High_Risk	LDAP_Injection	90		High	
PHP	PHP_High_Risk	Observable_Time_Discrepancy	208		High	
PHP	PHP_High_Risk	Reflected_XSS	79	Updated	High	High
PHP	PHP_High_Risk	Relative_Path_Traversal	23		High	
PHP	PHP_High_Risk	SSRF	918		High	
PHP	PHP_High_Risk	Stored_LDAP_Injection	90		High	
PHP	PHP_High_Risk	Stored_XPath_Injection	643		High	
PHP	PHP_High_Risk	Unsafe_Reflection	470		High	
PHP	PHP_Medium_Threat	Broken_or_Risky_Encryption_Algorithm	327		Medium	
PHP	PHP_Medium_Threat	Broken_or_Risky_Hashing_Function	327		Medium	
PHP	PHP_Medium_Threat	Command_Argument_Injection	88		Medium	
PHP	PHP_Medium_Threat	CSRF	352		Medium	
PHP	PHP_Medium_Threat	DoS_by_Sleep	606		Medium	
PHP	PHP_Medium_Threat	DoS_from_Evil_Regex	1333		Medium	
PHP	PHP_Medium_Threat	DoS_from_Regex_Injection	1333		Medium	
PHP	PHP_Medium_Threat	Encoding_Used_Instead_of_Encryption	326		Medium	
PHP	PHP_Medium_Threat	Error_Messages_Misconfiguration	209		Medium	
PHP	PHP_Medium_Threat	Hardcoded_Salt	760		Medium	
PHP	PHP_Medium_Threat	Hashing_Length_Extension_Attack	326		Medium	
PHP	PHP_Medium_Threat	Header_Injection	113		Medium	
PHP	PHP_Medium_Threat	HttpOnly_Cookie_Flag_Not_Set	1004		Medium	
PHP	PHP_Medium_Threat	HttpOnly_Cookie_Flag_Not_Set_In_Config	1004		Medium	
PHP	PHP_Medium_Threat	Insecure_Asymmetric_Cryptographic_Algorithm_Parameters	326		Medium	
PHP	PHP_Medium_Threat	Insecure_Value_of_the_SameSite_Cookie_Attribute	1275		Medium	
PHP	PHP_Medium_Threat	Insecure_Value_of_the_SameSite_Cookie_Attribute_In_Config	1275		Medium	
PHP	PHP_Medium_Threat	Insecure_WebSocket_Connection	1385		Medium	
PHP	PHP_Medium_Threat	Insufficiently_Secure_Password_Storage_Algorithm_Parameters	522		Medium	
PHP	PHP_Medium_Threat	JWT_Sensitive_Information_Exposure	201		Medium	
PHP	PHP_Medium_Threat	JWT_Use_Of_Hardcoded_Secret	321		Medium	
PHP	PHP_Medium_Threat	Loose_Comparison	480		Medium	
PHP	PHP_Medium_Threat	Missing_HSTS_Header	346		Medium	
PHP	PHP_Medium_Threat	Open_Redirect	601		Medium	
PHP	PHP_Medium_Threat	Parameter_Tampering	472		Medium	
PHP	PHP_Medium_Threat	Plaintext_Storage_of_a_Password	256		Medium	
PHP	PHP_Medium_Threat	Privacy_Violation	359		Medium	
PHP	PHP_Medium_Threat	Regex_Filter_Bypass	358		Medium	
PHP	PHP_Medium_Threat	Reliance_on_Reverse_DNS_Lookups_in_an_Action	350		Medium	
PHP	PHP_Medium_Threat	Secure_Cookie_Flag_Not_Set	614		Medium	
PHP	PHP_Medium_Threat	Secure_Cookie_Flag_Not_Set_In_Config	614		Medium	
PHP	PHP_Medium_Threat	Session_Fixation	384		Medium	
PHP	PHP_Medium_Threat	SSL_Verification_Bypass	599		Medium	
PHP	PHP_Medium_Threat	Storage_Controlled_Dynamic_Variable	914		Medium	
PHP	PHP_Medium_Threat	Stored_Absolute_Path_Traversal	36		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
PHP	PHP_Medium_Threat	Stored_Command_Argument_Injection	88		Medium	
PHP	PHP_Medium_Threat	Stored_Dangerous_File_Inclusion	829		Medium	
PHP	PHP_Medium_Threat	Stored_DoS_from_Evil_Regex	1333		Medium	
PHP	PHP_Medium_Threat	Stored_DoS_from_Regex_Injection	1333		Medium	
PHP	PHP_Medium_Threat	Stored_Relative_Path_Traversal	23		Medium	
PHP	PHP_Medium_Threat	Stored_Unsafe_Reflection	470		Medium	
PHP	PHP_Medium_Threat	Unchecked_Input_for_Loop_Condition	606		Medium	
PHP	PHP_Medium_Threat	Use_of_Cryptographically_Weak_PRNG	338		Medium	
PHP	PHP_Medium_Threat	Use_of_Hard_coded_Cryptographic_Key	321		Medium	
PHP	PHP_Medium_Threat	Use_of_Hardcoded_Cryptographic_IV	547		Medium	
PHP	PHP_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
PHP	PHP_Medium_Threat	User_Controlled_Dynamic_Variable	914		Medium	
PHP	PHP_Medium_Threat	Value_Shadowing	233		Medium	
PHP	PHP_Medium_Threat	XPath_Injection	643		Medium	
PHP	PHP_Medium_Threat	XSLT_Injection	94		Medium	
PHP	PHP_Low_Visibility	Compromised_CDN	0		Low	
PHP	PHP_Low_Visibility	Cookie_Overly_Broad_Path	539		Low	
PHP	PHP_Low_Visibility	Cookie_Overly_Broad_Path_In_Config	539		Low	
PHP	PHP_Low_Visibility	Deprecated_Functions_or_Properties	477		Low	
PHP	PHP_Low_Visibility	Hardcoded_Public_Key	321		Low	
PHP	PHP_Low_Visibility	Improper_Exception_Handling	248		Low	
PHP	PHP_Low_Visibility	Improper_Transaction_Handling	460		Low	
PHP	PHP_Low_Visibility	Information_Exposure_Through_an_Error_Message	209		Low	
PHP	PHP_Low_Visibility	Information_Leak_Through_Persistent_Cookies	539		Low	
PHP	PHP_Low_Visibility	Insufficient_Sanitization_for_XSS	838		Low	
PHP	PHP_Low_Visibility	JWT_Excessive_Expiration_Time	613		Low	
PHP	PHP_Low_Visibility	JWT_Lack_Of_Expiration_Time	613		Low	
PHP	PHP_Low_Visibility	JWT_No_Expiration_Time_Validation	613		Low	
PHP	PHP_Low_Visibility	JWT_No_NotBefore_Validation	304		Low	
PHP	PHP_Low_Visibility	Log_Forging	117		Low	
PHP	PHP_Low_Visibility	Missing_Framing_Policy	1021		Low	
PHP	PHP_Low_Visibility	Trust_Boundary_Violation_in_Session_Variables	501		Low	
PHP	PHP_Low_Visibility	Unsafe_Use_Of_Target_Blank	1022		Low	
PHP	PHP_Low_Visibility	Use_of_Non_Cryptographic_Random	338		Low	
PHP	PHP_Best_Coding_Practice	Declaration_Of_Catch_For_Generic_Exception	396		Information	
PHP	PHP_Best_Coding_Practice	Detection_of_Error_Condition_Without_Action	390		Information	
PHP	PHP_Best_Coding_Practice	Exposure_of_Resource_to_Wrong_Sphere	493		Information	
PHP	PHP_Best_Coding_Practice	Hardcoded_Absolute_Path	426		Information	
PHP	PHP_Best_Coding_Practice	Outdated_Encryption_Algorithm	326		Information	
PHP	PHP_Best_Coding_Practice	Outdated_Hashing_Function	328		Information	
PHP	PHP_Best_Coding_Practice	Possible_Global_Variable_Overwrite	0		Information	
PHP	PHP_Best_Coding_Practice	Unchecked_Error_Condition	0		Information	
PHP	PHP_Best_Coding_Practice	Unclosed_Objects	459		Information	
PHP	PHP_Best_Coding_Practice	Use_of_Evil_Regex	0		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
PHP	PHP_Best_Coding_Practice	Use_Of_Namespace	0		Information	
PHP	PHP_Best_Coding_Practice	Use_Of_Private_Static_Variable	0		Information	
PHP	PHP_Best_Coding_Practice	Use_Of_SuperGLOBALS	766		Information	
PLSQL	PLSQL_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
PLSQL	PLSQL_Critical_Risk	SQL_Injection	89		Critical	
PLSQL	PLSQL_Critical_Risk	Stored_XSS	79		Critical	
PLSQL	PLSQL_High_Risk	Reflected_XSS	79		High	
PLSQL	PLSQL_Medium_Threat	Authorization_Bypass_Through_User_Controlled_SQL_PrimaryKey	566	Updated	Medium	Medium
PLSQL	PLSQL_Medium_Threat	DoS_By_Sleep	606		Medium	
PLSQL	PLSQL_Medium_Threat	Open_Redirect	601	Updated	Medium	Medium
PLSQL	PLSQL_Medium_Threat	Parameter_Tampering	472	Updated	Medium	Medium
PLSQL	PLSQL_Medium_Threat	Plaintext_Storage_of_a_Password	256		Medium	
PLSQL	PLSQL_Medium_Threat	Privacy_Violation	359	Updated	Medium	Medium
PLSQL	PLSQL_Medium_Threat	Resource_Injection	99		Medium	
PLSQL	PLSQL_Medium_Threat	Reversible_One_Way_Hash	328	Updated	Medium	Medium
PLSQL	PLSQL_Medium_Threat	Use_Of_Broken_Or_Risky_Cryptographic_Algorithm	327	Updated	Medium	Medium
PLSQL	PLSQL_Medium_Threat	Use_Of_Hardcoded_Password	259	Updated	Medium	Medium
PLSQL	PLSQL_Low_Visibility	Compromised_CDN	0		Low	
PLSQL	PLSQL_Low_Visibility	Dangling_Database_Cursor	619	Updated	Low	Low
PLSQL	PLSQL_Low_Visibility	Default_Definer_Rights_in_Method_Definition	277	Updated	Low	Low
PLSQL	PLSQL_Low_Visibility	Default_Definer_Rights_in_Package_or_Object_Definition	277		Low	
PLSQL	PLSQL_Low_Visibility	Improper_Privilege_Management	269	Updated	Low	Low
PLSQL	PLSQL_Low_Visibility	Improper_Resource_Shutdown_or_Release	404	Updated	Low	Low
PLSQL	PLSQL_Low_Visibility	Server_Information_Exposure	497		Low	
PLSQL	PLSQL_Low_Visibility	Trust_Boundary_Violation_in_Session_Variables	501	Updated	Low	Low
PLSQL	PLSQL_Low_Visibility	Use_of_Insufficiently_Random_Values	338	Updated	Low	Low
PLSQL	PLSQL_Best_Coding_Practice	Unchecked_Error_Condition	0		Information	
PLSQL	PLSQL_Best_Coding_Practice	Use_of_Potentially_Dangerous_Function	676		Information	
Python	Python_AWS_Lambda	DynamoDB_NoSQL_Injection	943		Critical	
Python	Python_Critical_Risk	Code_Injection	94	Updated	Critical	
Python	Python_Critical_Risk	Command_Injection	77		Critical	
Python	Python_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
Python	Python_Critical_Risk	SQL_Injection	89		Critical	
Python	Python_Critical_Risk	Stored_Code_Injection	94		Critical	
Python	Python_Critical_Risk	Stored_Command_Injection	77		Critical	
Python	Python_Critical_Risk	Stored_XSS	79		Critical	
Python	Python_AWS_Lambda	AWS_Credentials_Leak	522		High	
Python	Python_High_Risk	Connection_String_Injection	99		High	
Python	Python_High_Risk	Debug_Enabled	489		High	
Python	Python_High_Risk	Deserialization_of_Untrusted_Data	502		High	
Python	Python_High_Risk	Improper_Restriction_of_XXE_Ref	611		High	
Python	Python_High_Risk	LDAP_Injection	90		High	
Python	Python_High_Risk	Local_File_Inclusion	829		High	
Python	Python_High_Risk	Path_Traversal	22		High	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Python	Python_High_Risk	Reflected_XSS	79		High	
Python	Python_High_Risk	SSRF	918	Updated	High	High
Python	Python_High_Risk	Stored_LDAP_Injection	90		High	
Python	Python_AWS_Lambda	Hardcoded_AWS_Credentials	798		Medium	
Python	Python_AWS_Lambda	Permission_Manipulation_in_S3	281		Medium	
Python	Python_AWS_Lambda	Unrestricted_Delete_S3	639		Medium	
Python	Python_AWS_Lambda	Unrestricted_Read_S3	639		Medium	
Python	Python_AWS_Lambda	Unrestricted_Write_S3	639		Medium	
Python	Python_AWS_Lambda	Use_of_Hardcoded_Cryptographic_Key_On_Server	321		Medium	
Python	Python_Medium_Threat	Command_Argument_Injection	88		Medium	
Python	Python_Medium_Threat	Communication_Over_HTTP	319		Medium	
Python	Python_Medium_Threat	CSRF	352		Medium	
Python	Python_Medium_Threat	Django_Improper_Resource_Access_Authorization	285		Medium	
Python	Python_Medium_Threat	Django_Missing_Function_Level_Authorization	862		Medium	
Python	Python_Medium_Threat	Django_Missing_Object_Level_Authorization	862		Medium	
Python	Python_Medium_Threat	DoS_by_Sleep	606		Medium	
Python	Python_Medium_Threat	Hardcoded_Password_in_Connection_String	547		Medium	
Python	Python_Medium_Threat	Header_Injection	113		Medium	
Python	Python_Medium_Threat	HttpOnly_Cookie_Flag_Not_Set_In_Config	1004		Medium	
Python	Python_Medium_Threat	Insufficiently_Protected_Credentials	522		Medium	
Python	Python_Medium_Threat	Missing_HSTS_Header	346		Medium	
Python	Python_Medium_Threat	Object_Access_Violation	99		Medium	
Python	Python_Medium_Threat	Open_Redirect	601		Medium	
Python	Python_Medium_Threat	OS_Access_Violation	77	Updated	Medium	Medium
Python	Python_Medium_Threat	Parameter_Tampering	472		Medium	
Python	Python_Medium_Threat	Password_In_Comment	615		Medium	
Python	Python_Medium_Threat	Privacy_Violation	359	Updated	Medium	Medium
Python	Python_Medium_Threat	ReDoS_From_Regex_Injection	1333		Medium	
Python	Python_Medium_Threat	ReDoS_Injection	1333		Medium	
Python	Python_Medium_Threat	Resource_Injection	99		Medium	
Python	Python_Medium_Threat	Secure_Cookie_Flag_Not_Set_In_Config	614		Medium	
Python	Python_Medium_Threat	SSL_Verification_Bypass	599		Medium	
Python	Python_Medium_Threat	Stored_Command_Argument_Injection	88		Medium	
Python	Python_Medium_Threat	Unchecked_Input_for_Loop_Condition	606		Medium	
Python	Python_Medium_Threat	Uncontrolled_Format_String	134		Medium	
Python	Python_Medium_Threat	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327		Medium	
Python	Python_Medium_Threat	Use_of_Hardcoded_Cryptographic_Key	321		Medium	
Python	Python_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
Python	Python_Medium_Threat	XPath_Injection	643		Medium	
Python	Python_AWS_Lambda	Race_Condition_Global_Scope	1108		Low	
Python	Python_AWS_Lambda	User_Based_SDK_Configurations	15		Low	
Python	Python_Low_Visibility	Compromised_CDN	0		Low	
Python	Python_Low_Visibility	Cookie_Poisoning	472		Low	
Python	Python_Low_Visibility	Django_Information_Exposure_Through_an_Error_Message	209		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Python	Python_Low_Visibility	Filtering_Sensitive_Logs	532	Updated	Low	Low
Python	Python_Low_Visibility	Improper_Resource_Shutdown_or_Release	404		Low	
Python	Python_Low_Visibility	Information_Exposure_Through_an_Error_Message	209		Low	
Python	Python_Low_Visibility	Insecure_Randomness	338		Low	
Python	Python_Low_Visibility	Log_Forging	117		Low	
Python	Python_Low_Visibility	Marshmallow_Dumping_Without_Validation	1173		Low	
Python	Python_Low_Visibility	Missing_Content_Security_Policy	346		Low	
Python	Python_Low_Visibility	Overly_Permissive_Cross-Origin_Resource_Sharing_Policy	346		Low	
Python	Python_Low_Visibility	Permissive_Content_Security_Policy	346		Low	
Python	Python_Low_Visibility	Trust_Boundary_Violation_in_Session_Variables	501		Low	
Python	Python_Best_Coding_Practice	Hardcoded_Absolute_Path	426		Information	
Python	Python_Best_Coding_Practice	Use_of_Unknown_Fields	0		Information	
RPG	RPG_Critical_Risk	Buffer_Overrun	126		Critical	
RPG	RPG_Critical_Risk	Control_Language_Injection	77		Critical	
RPG	RPG_Critical_Risk	SQL_Injection	89		Critical	
RPG	RPG_Medium_Threat	DoS_by_Sleep	606		Medium	
RPG	RPG_Medium_Threat	Path_Traversal	22		Medium	
RPG	RPG_Medium_Threat	ReDoS_From_Regexp_Injection	1333		Medium	
RPG	RPG_Medium_Threat	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327		Medium	
RPG	RPG_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
RPG	RPG_Low_Visibility	Compromised_CDN	0		Low	
RPG	RPG_Low_Visibility	Ignored_Error_Conditions	754		Low	
RPG	RPG_Low_Visibility	Improper_Resource_Shutdown_or_Release	404		Low	
RPG	RPG_Low_Visibility	Information_Exposure_Through_Dump	528		Low	
RPG	RPG_Low_Visibility	Integer_Overflow	190		Low	
RPG	RPG_Low_Visibility	Library_Search_Order_Hijacking	427		Low	
Ruby	Ruby_Critical_Risk	Code_Injection	94		Critical	
Ruby	Ruby_Critical_Risk	Command_Injection	77		Critical	
Ruby	Ruby_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
Ruby	Ruby_Critical_Risk	SQL_Injection	89		Critical	
Ruby	Ruby_Critical_Risk	Stored_Code_Injection	94		Critical	
Ruby	Ruby_Critical_Risk	Stored_XSS	79		Critical	
Ruby	Ruby_High_Risk	Connection_String_Injection	99		High	
Ruby	Ruby_High_Risk	Dangerous_File_Inclusion	829		High	
Ruby	Ruby_High_Risk	Dangerous_Send	77		High	
Ruby	Ruby_High_Risk	Download_Arbitrary_File	0		High	
Ruby	Ruby_High_Risk	Nonvalidated_File_Upload	434		High	
Ruby	Ruby_High_Risk	Path_Traversal	22		High	
Ruby	Ruby_High_Risk	Reflected_XSS	79		High	
Ruby	Ruby_Medium_Threat	CSRF	352		Medium	
Ruby	Ruby_Medium_Threat	DB_Tampering	20		Medium	
Ruby	Ruby_Medium_Threat	Default_Routes	0		Medium	
Ruby	Ruby_Medium_Threat	DoS_by_Sleep	606		Medium	
Ruby	Ruby_Medium_Threat	DOS_To_Symbol	401		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Ruby	Ruby_Medium_Threat	Hardcoded_Session_Secret_Token	798		Medium	
Ruby	Ruby_Medium_Threat	HttpOnly_Cookie_Flag_Not_Set	1004		Medium	
Ruby	Ruby_Medium_Threat	Insufficiently_Protected_Credentials	522		Medium	
Ruby	Ruby_Medium_Threat	Interactive_Render_Path	73		Medium	
Ruby	Ruby_Medium_Threat	Open_Redirect	601		Medium	
Ruby	Ruby_Medium_Threat	Parameter_Tampering	472		Medium	
Ruby	Ruby_Medium_Threat	Privacy_Violation	359		Medium	
Ruby	Ruby_Medium_Threat	Remote_Code_Execution	94		Medium	
Ruby	Ruby_Medium_Threat	Short_Session_Key	326		Medium	
Ruby	Ruby_Medium_Threat	SSL_Verification_Bypass	599		Medium	
Ruby	Ruby_Medium_Threat	Unsafe_Mass_Assignment	915		Medium	
Ruby	Ruby_Medium_Threat	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327		Medium	
Ruby	Ruby_Medium_Threat	Use_of_Hard_coded_Cryptographic_Key	321		Medium	
Ruby	Ruby_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
Ruby	Ruby_Low_Visibility	Attr_accessible_Not_Set	0		Low	
Ruby	Ruby_Low_Visibility	Compromised_CDN	0		Low	
Ruby	Ruby_Low_Visibility	DB_Information_Leak	200		Low	
Ruby	Ruby_Low_Visibility	Disabling_SAFE_Mode	250		Low	
Ruby	Ruby_Low_Visibility	Filtering_Sensitive_Logs	532		Low	
Ruby	Ruby_Low_Visibility	Full_Error_Reports_In_Production	209		Low	
Ruby	Ruby_Low_Visibility	Improper_Exception_Handling	248		Low	
Ruby	Ruby_Low_Visibility	Improper_Transaction_Handling	460		Low	
Ruby	Ruby_Low_Visibility	Information_Exposure_Through_an_Error_Message	209		Low	
Ruby	Ruby_Low_Visibility	Information_Leak_Through_Persistent_Cookies	539		Low	
Ruby	Ruby_Low_Visibility	Insecure_Randomness	338		Low	
Ruby	Ruby_Low_Visibility	Insufficient_Format_Validation	625		Low	
Ruby	Ruby_Low_Visibility	Leftover_Debug_Code	489		Low	
Ruby	Ruby_Low_Visibility	Local_File_Inclusion	829		Low	
Ruby	Ruby_Low_Visibility	Log_Forging	117		Low	
Ruby	Ruby_Low_Visibility	No_Protection_From_Forgery	352		Low	
Ruby	Ruby_Low_Visibility	No_Session_Expiration	613		Low	
Ruby	Ruby_Low_Visibility	Personal_Info_In_Session	539		Low	
Ruby	Ruby_Low_Visibility	Trust_Boundary_Violation_in_Session_Variables	501		Low	
Ruby	Ruby_Low_Visibility	Use_of_Dangerous_Functions	242		Low	
Ruby	Ruby_Low_Visibility	Use_Of_raw	116		Low	
Ruby	Ruby_Low_Visibility	Use_Of_Sanitize_Instead_Of_h	116		Low	
Ruby	Ruby_Best_Coding_Practice	Caching_False_In_Production	772		Information	
Ruby	Ruby_Best_Coding_Practice	Declaration_Of_Catch_For_Generic_Exception	396		Information	
Ruby	Ruby_Best_Coding_Practice	Dynamic_Render_Path	0		Information	
Ruby	Ruby_Best_Coding_Practice	Dynamic_SQL_Queries	89		Information	
Ruby	Ruby_Best_Coding_Practice	Global_Variables_Without_Meaningful_Name	0		Information	
Ruby	Ruby_Best_Coding_Practice	Hardcoded_Absolute_Path	426		Information	
Ruby	Ruby_Best_Coding_Practice	Import_Relative_To_File	0		Information	
Ruby	Ruby_Best_Coding_Practice	Unchecked_Error_Condition	0		Information	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Ruby	Ruby_Best_Coding_Practice	Unclosed_Objects	459		Information	
Ruby	Ruby_Best_Coding_Practice	Use_Of_Global_Variables	766		Information	
Rust	Rust_Critical_Risk	Arbitrary_File_Write	669		Critical	
Rust	Rust_Critical_Risk	Command_Injection	77		Critical	
Rust	Rust_Critical_Risk	DynamoDB_NoSQL_Injection	943		Critical	
Rust	Rust_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
Rust	Rust_Critical_Risk	SQL_Injection	89		Critical	
Rust	Rust_Critical_Risk	Stored_Command_Injection	77		Critical	
Rust	Rust_Critical_Risk	Stored_XSS	79		Critical	
Rust	Rust_High_Risk	Absolute_Path_Traversal	36		High	
Rust	Rust_High_Risk	AWS_Credentials_Leak	522		High	
Rust	Rust_High_Risk	Connection_String_Injection	99		High	
Rust	Rust_High_Risk	Dangerous_File_Inclusion	829		High	
Rust	Rust_High_Risk	JWT_No_Signature_Verification	347		High	
Rust	Rust_High_Risk	LDAP_Injection	90		High	
Rust	Rust_High_Risk	Observable_Timing_Discrepancy	208		High	
Rust	Rust_High_Risk	Plaintext_Password_Storage	256		High	
Rust	Rust_High_Risk	Reflected_XSS	79		High	
Rust	Rust_High_Risk	Relative_Path_Traversal	23		High	
Rust	Rust_High_Risk	Sensitive_Information_Exposure_in_Cleartext_Channel	319		High	
Rust	Rust_High_Risk	SSRF	918		High	
Rust	Rust_High_Risk	Stored_LDAP_Injection	90		High	
Rust	Rust_High_Risk	Unsafe_Archive_Unpacking	22		High	
Rust	Rust_Medium_Threat	Broken_or_Risky_Hashing_Function	327		Medium	
Rust	Rust_Medium_Threat	Command_Argument_Injection	88		Medium	
Rust	Rust_Medium_Threat	DoS_by_Sleep	606		Medium	
Rust	Rust_Medium_Threat	Empty_Password_In_Connection_String	521		Medium	
Rust	Rust_Medium_Threat	Encoding_Used_Instead_of_Encryption	326		Medium	
Rust	Rust_Medium_Threat	Environment_Variable_Injection	15		Medium	
Rust	Rust_Medium_Threat	Excessive_Data_Exposure	201		Medium	
Rust	Rust_Medium_Threat	External_Control_of_System_or_Config_Setting	15		Medium	
Rust	Rust_Medium_Threat	Hardcoded_AWS_Credentials	798		Medium	
Rust	Rust_Medium_Threat	Hardcoded_Cryptographic_Key	321		Medium	
Rust	Rust_Medium_Threat	Hardcoded_Password_in_Connection_String	547		Medium	
Rust	Rust_Medium_Threat	Hardcoded_Salt	760		Medium	
Rust	Rust_Medium_Threat	HttpOnly_Cookie_Flag_Not_Set	1004		Medium	
Rust	Rust_Medium_Threat	Improper_Locking	667		Medium	
Rust	Rust_Medium_Threat	Insufficiently_Secure_Password_Storage_Algorithm_Parameters	522		Medium	
Rust	Rust_Medium_Threat	JWT_Sensitive_Information_Exposure	201		Medium	
Rust	Rust_Medium_Threat	JWT_Use_Of_Hardcoded_Secret	321		Medium	
Rust	Rust_Medium_Threat	Length_Extension_Attack	326		Medium	
Rust	Rust_Medium_Threat	Open_Redirect	601		Medium	
Rust	Rust_Medium_Threat	Parameter_Tampering	472		Medium	
Rust	Rust_Medium_Threat	Password_In_Comment	615		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Rust	Rust_Medium_Threat	PCI_Data_Exposure	312		Medium	
Rust	Rust_Medium_Threat	PCI_Data_Exposure_in_JWT	312		Medium	
Rust	Rust_Medium_Threat	Permission_Manipulation_in_S3	281		Medium	
Rust	Rust_Medium_Threat	Privacy_Violation	359		Medium	
Rust	Rust_Medium_Threat	Privacy_Violation_in_JWT	312		Medium	
Rust	Rust_Medium_Threat	Reliance_on_Reverse_DNS_Lookups_in_a_Decision	350		Medium	
Rust	Rust_Medium_Threat	Secret_Leak	312		Medium	
Rust	Rust_Medium_Threat	Secret_Leak_in_Error_Messages	209		Medium	
Rust	Rust_Medium_Threat	Secret_Leak_in_Files	312		Medium	
Rust	Rust_Medium_Threat	Secret_Leak_in_JWT	312		Medium	
Rust	Rust_Medium_Threat	Secret_Leak_in_Logs	532		Medium	
Rust	Rust_Medium_Threat	Secret_Leak_in_URL	312		Medium	
Rust	Rust_Medium_Threat	Secure_Cookie_Flag_Not_Set	614		Medium	
Rust	Rust_Medium_Threat	SSL_Verification_Bypass	599		Medium	
Rust	Rust_Medium_Threat	Stored_Absolute_Path_Traversal	36		Medium	
Rust	Rust_Medium_Threat	Stored_Command_Argument_Injection	88		Medium	
Rust	Rust_Medium_Threat	Stored_Environment_Variable_Injection	15		Medium	
Rust	Rust_Medium_Threat	Stored_Relative_Path_Traversal	23		Medium	
Rust	Rust_Medium_Threat	Unchecked_Input_for_Loop_Condition	606		Medium	
Rust	Rust_Medium_Threat	Uncontrolled_Memory_Allocation	789		Medium	
Rust	Rust_Medium_Threat	Unrestricted_Delete_S3	639		Medium	
Rust	Rust_Medium_Threat	Unrestricted_Read_S3	639		Medium	
Rust	Rust_Medium_Threat	Unrestricted_Write_S3	639		Medium	
Rust	Rust_Medium_Threat	Unsafe_Reflection	470		Medium	
Rust	Rust_Medium_Threat	Use_of_Cryptographically_Weak_PRNG	338		Medium	
Rust	Rust_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
Rust	Rust_Medium_Threat	Use_of_Native_Language	695		Medium	
Rust	Rust_Medium_Threat	Using_Referer_Field_for_Authentication	293		Medium	
Rust	Rust_Low_Visibility	Compromised_CDN	0		Low	
Rust	Rust_Low_Visibility	Cookie_Overly_Broad_Path	539		Low	
Rust	Rust_Low_Visibility	Dangerous_File_Extension	434		Low	
Rust	Rust_Low_Visibility	Divide_By_Zero	369		Low	
Rust	Rust_Low_Visibility	Frameable_Login_Page	829		Low	
Rust	Rust_Low_Visibility	Heap_Inspection	244		Low	
Rust	Rust_Low_Visibility	Improper_Error_Handling	248		Low	
Rust	Rust_Low_Visibility	Improper_Resource_Shutdown_or_Release	404		Low	
Rust	Rust_Low_Visibility	Improper_Transaction_Handling	460		Low	
Rust	Rust_Low_Visibility	Incorrect_Permission_Assignment_For_Critical_Resources	732		Low	
Rust	Rust_Low_Visibility	Insecure_Value_of_the_SameSite_Cookie_Attribute	1275		Low	
Rust	Rust_Low_Visibility	Integer_Overflow	190		Low	
Rust	Rust_Low_Visibility	JWT_Excessive_Expiration_Time	613		Low	
Rust	Rust_Low_Visibility	JWT_Lack_of_Expiration_Time	613		Low	
Rust	Rust_Low_Visibility	JWT_No_Expiration_Time_Validation	613		Low	
Rust	Rust_Low_Visibility	JWT_No_NotBefore_Validation	304		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Rust	Rust_Low_Visibility	Log_Forging	117		Low	
Rust	Rust_Low_Visibility	Misconfigured_HSTS	346		Low	
Rust	Rust_Low_Visibility	Misconfigured_X_Content_Type_Options	693		Low	
Rust	Rust_Low_Visibility	Missing_Content_Security_Policy	346		Low	
Rust	Rust_Low_Visibility	Missing_Framing_Policy	1021		Low	
Rust	Rust_Low_Visibility	Missing_HSTS	346		Low	
Rust	Rust_Low_Visibility	Missing_Password_Field_Masking	549		Low	
Rust	Rust_Low_Visibility	Off_By_One_Error	193		Low	
Rust	Rust_Low_Visibility	Overly_Permissive_Cross-Origin_Resource_Sharing_Policy	346		Low	
Rust	Rust_Low_Visibility	PCI_Data_Exposure_in_Error_Messages	209		Low	
Rust	Rust_Low_Visibility	PCI_Data_Exposure_in_Files	312		Low	
Rust	Rust_Low_Visibility	PCI_Data_Exposure_in_Logs	532		Low	
Rust	Rust_Low_Visibility	PCI_Data_Exposure_in_URL	312		Low	
Rust	Rust_Low_Visibility	Permissive_Content_Security_Policy	346		Low	
Rust	Rust_Low_Visibility	Privacy_Violation_in_Error_Messages	209		Low	
Rust	Rust_Low_Visibility	Privacy_Violation_in_Files	312		Low	
Rust	Rust_Low_Visibility	Privacy_Violation_in_Logs	532		Low	
Rust	Rust_Low_Visibility	Privacy_Violation_in_URL	312		Low	
Rust	Rust_Low_Visibility	Race_Condition_In_Cross_Functionality	362		Low	
Rust	Rust_Low_Visibility	Serializable_Class_Containing_Sensitive_Data	499		Low	
Rust	Rust_Low_Visibility	Trust_Boundary_Violation_in_Session_Variables	501		Low	
Rust	Rust_Low_Visibility	Type_Conversion_Error	681		Low	
Rust	Rust_Low_Visibility	Unchecked_Return_Value_to_NULL_Pointer_Dereference	252		Low	
Rust	Rust_Low_Visibility	Usage_of_temp_dir	0		Low	
Rust	Rust_Low_Visibility	Use_of_Deprecated_API	477		Low	
Rust	Rust_Low_Visibility	Use_of_Non_Cryptographic_Random	338		Low	
Rust	Rust_Low_Visibility	Use_of_Unsafe_Keyword	242		Low	
Rust	Rust_Best_Coding_Practice	Input_Path_Not_Canonicalized	73		Information	
Scala	Scala_Critical_Risk	Code_Injection	94		Critical	
Scala	Scala_Critical_Risk	Command_Injection	77		Critical	
Scala	Scala_Critical_Risk	Expression_Language_Injection_MVEL	917		Critical	
Scala	Scala_Critical_Risk	Expression_Language_Injection_SPEL	917		Critical	
Scala	Scala_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
Scala	Scala_Critical_Risk	SQL_Injection	89		Critical	
Scala	Scala_Critical_Risk	Stored_Code_Injection	94		Critical	
Scala	Scala_Critical_Risk	Stored_Command_Injection	77		Critical	
Scala	Scala_Critical_Risk	Stored_XSS	79		Critical	
Scala	Scala_High_Risk	Absolute_Path_Traversal	36		High	
Scala	Scala_High_Risk	Cleartext_Submission_of_Sensitive_Information	319		High	
Scala	Scala_High_Risk	Connection_String_Injection	99		High	
Scala	Scala_High_Risk	Dangerous_File_Inclusion	829		High	
Scala	Scala_High_Risk	Deserialization_of_Untrusted_Data	502		High	
Scala	Scala_High_Risk	Improper_Restriction_of_Stored_XXE_Ref	611		High	
Scala	Scala_High_Risk	Improper_Restriction_of_XXE_Ref	611		High	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Scala	Scala_High_Risk	JWT_No_Signature_Verification	347		High	
Scala	Scala_High_Risk	JWT_Use_Of_None_Algorithm	287		High	
Scala	Scala_High_Risk	LDAP_Injection	90		High	
Scala	Scala_High_Risk	Reflected_XSS	79		High	
Scala	Scala_High_Risk	Relative_Path_Traversal	23		High	
Scala	Scala_High_Risk	SSRF	918		High	
Scala	Scala_High_Risk	Stored_LDAP_Injection	90		High	
Scala	Scala_High_Risk	Unsafe_Reflection	470		High	
Scala	Scala_Medium_Threat	Akka_Disabling_Hostname_Verification	0		Medium	
Scala	Scala_Medium_Threat	Command_Argument_Injection	88		Medium	
Scala	Scala_Medium_Threat	CSRF	352		Medium	
Scala	Scala_Medium_Threat	DoS_by_Sleep	606		Medium	
Scala	Scala_Medium_Threat	Excessive_Data_Exposure	201		Medium	
Scala	Scala_Medium_Threat	Hardcoded_password_in_Connection_String	547		Medium	
Scala	Scala_Medium_Threat	HttpOnly_Cookie_Flag_Not_Set	1004		Medium	
Scala	Scala_Medium_Threat	Improper_Locking	667		Medium	
Scala	Scala_Medium_Threat	Inadequate_Encryption_Strength	326		Medium	
Scala	Scala_Medium_Threat	JWT_Sensitive_Information_Exposure	201		Medium	
Scala	Scala_Medium_Threat	JWT_Use_Of_Hardcoded_Secret	321		Medium	
Scala	Scala_Medium_Threat	Not_Using_a_Random_IV_with_CBC_Mode	329		Medium	
Scala	Scala_Medium_Threat	Open_Redirect	601		Medium	
Scala	Scala_Medium_Threat	Parameter_Tampering	472		Medium	
Scala	Scala_Medium_Threat	Plaintext_Storage_of_a_Password	256		Medium	
Scala	Scala_Medium_Threat	Privacy_Violation	359		Medium	
Scala	Scala_Medium_Threat	ReDoS_From_Regex_Injection	1333		Medium	
Scala	Scala_Medium_Threat	ReDoS_In_Match	1333		Medium	
Scala	Scala_Medium_Threat	ReDoS_In_Pattern	1333		Medium	
Scala	Scala_Medium_Threat	ReDoS_In_Replace	1333		Medium	
Scala	Scala_Medium_Threat	Resource_Injection	99		Medium	
Scala	Scala_Medium_Threat	Secure_Cookie_Flag_Not_Set	614		Medium	
Scala	Scala_Medium_Threat	Session_Fixation	384		Medium	
Scala	Scala_Medium_Threat	Spring_ModelView_Injection	94		Medium	
Scala	Scala_Medium_Threat	SQL_Injection_Evasion_Attack	89		Medium	
Scala	Scala_Medium_Threat	SSL_Verification_Bypass	599		Medium	
Scala	Scala_Medium_Threat	Stored_Open_Redirect	601		Medium	
Scala	Scala_Medium_Threat	Stored_XPath_Injection	643		Medium	
Scala	Scala_Medium_Threat	Unvalidated_Forwards	601		Medium	
Scala	Scala_Medium_Threat	Use_of_a_One_Way_Hash_with_a_Predictable_Salt	760		Medium	
Scala	Scala_Medium_Threat	Use_of_a_One_Way_Hash_without_a_Salt	759		Medium	
Scala	Scala_Medium_Threat	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327		Medium	
Scala	Scala_Medium_Threat	Use_of_Cryptographically_Weak_PRNG	338		Medium	
Scala	Scala_Medium_Threat	Use_of_Hardcoded_Cryptographic_Key	321		Medium	
Scala	Scala_Medium_Threat	Use_of_Unsafe_JNI	111		Medium	
Scala	Scala_Medium_Threat	XPath_Injection	643		Medium	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Scala	Scala_Medium_Threat	XQuery_Injection	652		Medium	
Scala	Scala_Low_Visibility	Akka_Debug_Loglevel_Enabled	15		Low	
Scala	Scala_Low_Visibility	Akka_Encrypt_Data_Disabled	15		Low	
Scala	Scala_Low_Visibility	Akka_Missing_Max_Age	15		Low	
Scala	Scala_Low_Visibility	Akka_Serialize_Enabled	15		Low	
Scala	Scala_Low_Visibility	Akka_Untrusted_Mode_Enabled	15		Low	
Scala	Scala_Low_Visibility	Akka_Verbose_Mode_Enabled	209		Low	
Scala	Scala_Low_Visibility	Compromised_CDN	0		Low	
Scala	Scala_Low_Visibility	Deprecated_Functions_or_Properties	477		Low	
Scala	Scala_Low_Visibility	Heap_Inspection	244		Low	
Scala	Scala_Low_Visibility	Integer_Overflow	190		Low	
Scala	Scala_Low_Visibility	JWT_Excessive_Expiration_Time	613		Low	
Scala	Scala_Low_Visibility	JWT_Lack_Of_Expiration_Time	613		Low	
Scala	Scala_Low_Visibility	Overtly_Permissive_Cross-Origin_Resource_Sharing_Policy	346		Low	
Scala	Scala_Low_Visibility	Same_Seed_in_PRNG	336		Low	
Scala	Scala_Low_Visibility	Use_of_Hard_coded_Security_Constants	547		Low	
Scala	Scala_Low_Visibility	Use_of_RSA_Algorithm_without_OAEP	780		Low	
Scala	Scala_Best_Coding_Practice	Potential_Usage_of_Vulnerable_Log4J	502		Information	
Scala	Scala_Best_Coding_Practice	Use_of_Non_Cryptographic_Random	338		Information	
SQL	SQL_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
SQL	SQL_Critical_Risk	Stored_Command_Injection	77		Critical	
SQL	SQL_Medium_Threat	Broken_or_Risky_Encryption_Algorithm	327		Medium	
SQL	SQL_Medium_Threat	Broken_or_Risky_Hashing_Function	327		Medium	
SQL	SQL_Medium_Threat	Dangling_Database_Cursor	619		Medium	
SQL	SQL_Medium_Threat	DoS_by_Sleep	606		Medium	
SQL	SQL_Medium_Threat	Dynamic_Data_Masking_Bypass	200		Medium	
SQL	SQL_Medium_Threat	JSON_Injection	116		Medium	
SQL	SQL_Medium_Threat	Password_In_Comment	615		Medium	
SQL	SQL_Medium_Threat	Race_Condition_In_Transaction	362		Medium	
SQL	SQL_Medium_Threat	Stored_Absolute_Path_Traversal	36		Medium	
SQL	SQL_Medium_Threat	Stored_External_XML_Entities_XXE	611		Medium	
SQL	SQL_Medium_Threat	Stored_Relative_Path_Traversal	23		Medium	
SQL	SQL_Medium_Threat	Unchecked_Input_for_Loop_Condition	606		Medium	
SQL	SQL_Medium_Threat	Unsafe_XACT_ABORT_in_Config	754		Medium	
SQL	SQL_Medium_Threat	Use_of_Cryptographically_Weak_PRNG	338		Medium	
SQL	SQL_Medium_Threat	Use_of_Non_Cryptographic_Random	338		Medium	
SQL	SQL_Medium_Threat	XML_Injection	91		Medium	
SQL	SQL_Low_Visibility	Execution_Context_Changed_Without_REVERT	250		Low	
SQL	SQL_Low_Visibility	Explicit_Administrator_Rights_in_Package_or_Method_Definition	250		Low	
SQL	SQL_Low_Visibility	Improper_Exception_Handling	248		Low	
SQL	SQL_Low_Visibility	Improper_Privilege_Management	269		Low	
SQL	SQL_Low_Visibility	PCI_Data_Exposure_in_Backups	200		Low	
SQL	SQL_Low_Visibility	PCI_Data_Exposure_in_Error_Messages	209		Low	
SQL	SQL_Low_Visibility	Privacy_Violation_in_Backups	200		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
SQL	SQL_Low_Visibility	Privacy_Violation_in_Error_Messages	209		Low	
SQL	SQL_Low_Visibility	Secret_Leak_in_Backups	200		Low	
SQL	SQL_Low_Visibility	Secret_Leak_in_Error_Messages	209		Low	
SQL	SQL_Low_Visibility	Server_Information_Exposure_via_Misconfiguration	312		Low	
SQL	SQL_Low_Visibility	Use_of_Hardcoded_Password	259		Low	
SQL	SQL_Best_Coding_Practice	Access_Control_Management_Without_Audit	778		Information	
SQL	SQL_Best_Coding_Practice	Assembly_Using_Unsafe_Permission	250		Information	
SQL	SQL_Best_Coding_Practice	Authentication_Management_Without_Audit	778		Information	
SQL	SQL_Best_Coding_Practice	Explicit_Definer_Rights_in_Package_or_Method_Definition	250		Information	
SQL	SQL_Best_Coding_Practice	Explicit_User_Rights_in_Package_or_Method_Definition	250		Information	
SQL	SQL_Best_Coding_Practice	Unrestricted_User_Access	200		Information	
SQL	SQL_Best_Coding_Practice	Use_of_Read_Uncommitted	362		Information	
Swift	Swift_High_Risk	Resource_Updated_By_URL_Data	939		High	
Swift	Swift_High_Risk	Sensitive_Information_Exposure_in_Cleartext_Channel	319		High	
Swift	Swift_High_Risk	Unencrypted_Sensitive_Information_in_Publicly_Accessible_iCloud_Storage	312		High	
Swift	Swift_High_Risk	Unsafe_Reflection	470		High	
Swift	Swift_High_Risk	Use_of_Hardcoded_Cryptographic_Key	321		High	
Swift	Swift_High_Risk	WebView_JavaScript_Injection_From_URL_Scheme	79		High	
Swift	Swift_Medium_Threat	Autocorrection_Keystroke_Logging	359		Medium	
Swift	Swift_Medium_Threat	Communication_over_HTTP	319		Medium	
Swift	Swift_Medium_Threat	Format_String_Attack	134		Medium	
Swift	Swift_Medium_Threat	Improper_Certificate_Validation	295		Medium	
Swift	Swift_Medium_Threat	Information_Exposure_Through_Extension	359		Medium	
Swift	Swift_Medium_Threat	Information_Exposure_Through_Query_String	598		Medium	
Swift	Swift_Medium_Threat	Password_In_Comment	615		Medium	
Swift	Swift_Medium_Threat	Pasteboard_Leakage	922		Medium	
Swift	Swift_Medium_Threat	Public_Storage_SQL_Injection	89		Medium	
Swift	Swift_Medium_Threat	Public_Storage_WebView_JavaScript_Injection	79		Medium	
Swift	Swift_Medium_Threat	ReDoS_From_Regex_Injection	1333		Medium	
Swift	Swift_Medium_Threat	Screen_Caching	524		Medium	
Swift	Swift_Medium_Threat	SQL_Injection_From_URL_Scheme	89		Medium	
Swift	Swift_Medium_Threat	Third_Party_Keyboard_Enabled	829		Medium	
Swift	Swift_Medium_Threat	Third_Party_Keyboards_On_Sensitive_Field	829		Medium	
Swift	Swift_Medium_Threat	Unencrypted_Sensitive_Information_in_External_Storage	922		Medium	
Swift	Swift_Medium_Threat	URL_Scheme_Hijacking	319		Medium	
Swift	Swift_Medium_Threat	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327		Medium	
Swift	Swift_Medium_Threat	Use_of_Hardcoded_Password	259		Medium	
Swift	Swift_Low_Visibility	Allowed_Backup	530		Low	
Swift	Swift_Low_Visibility	App_Transport_Security_Disabled	319		Low	
Swift	Swift_Low_Visibility	Compromised_CDN	0		Low	
Swift	Swift_Low_Visibility	Encrypted_Sensitive_Information_in_Publicly_Accessible_iCloud_Storage	922		Low	
Swift	Swift_Low_Visibility	Functions_Apple_Recommends_To_Avoid	477		Low	
Swift	Swift_Low_Visibility	Information_Leak_Through_Response_Caching	524		Low	
Swift	Swift_Low_Visibility	Insufficient_Encryption_Key_Size	326		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
Swift	Swift_Low_Visibility	Missing_Device_Lock_Verification	829		Low	
Swift	Swift_Low_Visibility	Missing_Jailbreak_Check	250		Low	
Swift	Swift_Low_Visibility	Null_Password	252		Low	
Swift	Swift_Low_Visibility	Path_Traversal	22		Low	
Swift	Swift_Low_Visibility	Private_Storage_SQL_Injection	89		Low	
Swift	Swift_Low_Visibility	Private_Storage_WebView_JavaScript_Injection	79		Low	
Swift	Swift_Low_Visibility	Secret_Stored_Outside_of_Keychain	922		Low	
Swift	Swift_Low_Visibility	Self_SQL_Injection	89		Low	
Swift	Swift_Low_Visibility	Self_WebView_JavaScript_Injection	79		Low	
Swift	Swift_Low_Visibility	Unencrypted_Sensitive_Information_in_Internal_Storage	922		Low	
Swift	Swift_Low_Visibility	Use_of_Insufficiently_Random_Values	338		Low	
Swift	Swift_Low_Visibility	User_Information_in_Publicly_Accessible_iCloud_Storage	312		Low	
Swift	Swift_Low_Visibility	XML_External_Entity	611		Low	
Swift	Swift_Best_Coding_Practices	Dynamic_SQL_Queries	89		Information	
Swift	Swift_Best_Coding_Practices	Empty_Methods	0		Information	
Swift	Swift_Best_Coding_Practices	Missing_Certificate_Pinning	295		Information	
VB6	VB6_Critical_Risk	Code_Injection	94		Critical	
VB6	VB6_Critical_Risk	Command_Injection	77		Critical	
VB6	VB6_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
VB6	VB6_Critical_Risk	SQL_Injection	89		Critical	
VB6	VB6_Critical_Risk	Stored_Code_Injection	94		Critical	
VB6	VB6_High_Risk	Connection_String_Injection	99		High	
VB6	VB6_High_Risk	Path_Traversal	22		High	
VB6	VB6_Medium_Threat	DoS_by_Sleep	606		Medium	
VB6	VB6_Medium_Threat	Hardcoded_password_in_Connection_String	547		Medium	
VB6	VB6_Medium_Threat	Insufficiently_Protected_Credentials	522		Medium	
VB6	VB6_Medium_Threat	Parameter_Tampering	472		Medium	
VB6	VB6_Medium_Threat	Privacy_Violation	359		Medium	
VB6	VB6_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
VB6	VB6_Low_Visibility	Bounds_Check_Disabled	118		Low	
VB6	VB6_Low_Visibility	Compromised_CDN	0		Low	
VB6	VB6_Low_Visibility	Improper_Error_Handling	248		Low	
VB6	VB6_Low_Visibility	Information_Exposure_Through_an_Error_Message	209		Low	
VB6	VB6_Low_Visibility	Insecure_Randomness	338		Low	
VB6	VB6_Low_Visibility	Log_Forging	117		Low	
VB6	VB6_Low_Visibility	Hardcoded_Absolute_Path	426		Information	
VbNet	VbNet_Critical_Risk	Code_Injection	94		Critical	
VbNet	VbNet_Critical_Risk	Command_Injection	77		Critical	
VbNet	VbNet_Critical_Risk	Second_Order_SQL_Injection	89		Critical	
VbNet	VbNet_Critical_Risk	SQL_Injection	89		Critical	
VbNet	VbNet_Critical_Risk	Stored_Code_Injection	94		Critical	
VbNet	VbNet_Critical_Risk	Stored_Command_Injection	77		Critical	
VbNet	VbNet_Critical_Risk	Stored_XSS	79		Critical	
VbNet	VbNet_High_Risk	Buffer_Overflow	120		High	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
VbNet	VbNet_High_Risk	CGI_XSS	79		High	
VbNet	VbNet_High_Risk	Connection_String_Injection	99		High	
VbNet	VbNet_High_Risk	Dangerous_File_Extension	434		High	
VbNet	VbNet_High_Risk	LDAP_Injection	90		High	
VbNet	VbNet_High_Risk	Path_Traversal	22		High	
VbNet	VbNet_High_Risk	Reflected_XSS	79		High	
VbNet	VbNet_High_Risk	Stored_LDAP_Injection	90		High	
VbNet	VbNet_Medium_Threat	CSRF	352		Medium	
VbNet	VbNet_Medium_Threat	Data_Filter_Injection	943		Medium	
VbNet	VbNet_Medium_Threat	DoS_by_Sleep	606		Medium	
VbNet	VbNet_Medium_Threat	Hardcoded_password_in_Connection_String	547		Medium	
VbNet	VbNet_Medium_Threat	Improper_Locking	667		Medium	
VbNet	VbNet_Medium_Threat	Insufficiently_Protected_Credentials	522		Medium	
VbNet	VbNet_Medium_Threat	No_Request_Validation	20		Medium	
VbNet	VbNet_Medium_Threat	Open_Redirect	601		Medium	
VbNet	VbNet_Medium_Threat	Parameter_Tampering	472		Medium	
VbNet	VbNet_Medium_Threat	Privacy_Violation	359		Medium	
VbNet	VbNet_Medium_Threat	Resource_Injection	99		Medium	
VbNet	VbNet_Medium_Threat	SQL_Injection_Evasion_Attack	89		Medium	
VbNet	VbNet_Medium_Threat	Stored_XPath_Injection	643		Medium	
VbNet	VbNet_Medium_Threat	Unsafe_Object_Binding	915		Medium	
VbNet	VbNet_Medium_Threat	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327		Medium	
VbNet	VbNet_Medium_Threat	Use_of_Hard_coded_Cryptographic_Key	321		Medium	
VbNet	VbNet_Medium_Threat	Use_Of_Hardcoded_Password	259		Medium	
VbNet	VbNet_Medium_Threat	Value_Shadowing	233		Medium	
VbNet	VbNet_Medium_Threat	XPath_Injection	643		Medium	
VbNet	VbNet_WebConfig	CookieLess_Authentication	642		Medium	
VbNet	VbNet_WebConfig	CookieLess_Session	0		Medium	
VbNet	VbNet_WebConfig	Elmah_Enabled	213		Medium	
VbNet	VbNet_WebConfig	HardcodedCredentials	798		Medium	
VbNet	VbNet_WebConfig	HttpOnly_Cookie_Flag_Not_Set_In_Config	1004		Medium	
VbNet	VbNet_WebConfig	RequireSSL	614		Medium	
VbNet	VbNet_WebConfig	TraceEnabled	749		Medium	
VbNet	VbNet_Low_Visibility	Client_Side_Only_Validation	602		Low	
VbNet	VbNet_Low_Visibility	Compromised_CDN	0		Low	
VbNet	VbNet_Low_Visibility	Heap_Inspection	244		Low	
VbNet	VbNet_Low_Visibility	Impersonation_Issue	520		Low	
VbNet	VbNet_Low_Visibility	Improper-Encoding_Of_Output	116		Low	
VbNet	VbNet_Low_Visibility	Improper_Exception_Handling	248		Low	
VbNet	VbNet_Low_Visibility	Improper_Resource_Shutdown_or_Release	404		Low	
VbNet	VbNet_Low_Visibility	Improper_Session_Management	201		Low	
VbNet	VbNet_Low_Visibility	Improper_Transaction_Handling	460		Low	
VbNet	VbNet_Low_Visibility	Information_Exposure_Through_an_Error_Message	209		Low	
VbNet	VbNet_Low_Visibility	Information_Leak_Through_Persistent_Cookies	539		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
VbNet	VbNet_Low_Visibility	Leaving_Temporary_Files	377		Low	
VbNet	VbNet_Low_Visibility	Log_Forging	117		Low	
VbNet	VbNet_Low_Visibility	Overly_Permissive_Cross-Origin_Resource_Sharing_Policy	346		Low	
VbNet	VbNet_Low_Visibility	Session_Clearing_Problems	613		Low	
VbNet	VbNet_Low_Visibility	Thread_Safety_Issue	567		Low	
VbNet	VbNet_Low_Visibility	Trust_Boundary_Violation_in_Session_Variables	501		Low	
VbNet	VbNet_Low_Visibility	URL_Canonicalization_Issue	647		Low	
VbNet	VbNet_WebConfig	CustomError	12		Low	
VbNet	VbNet_WebConfig	DebugEnabled	11		Low	
VbNet	VbNet_WebConfig	Missing_Framing_Policy	1021		Low	
VbNet	VbNet_WebConfig	NonUniqueFormName	694		Low	
VbNet	VbNet_WebConfig	Password_In_Configuration_File	260		Low	
VbNet	VbNet_WebConfig	SlidingExpiration	613		Low	
VbNet	VbNet_Best_Coding_Practice	Aptca_Methods_Call_Non_Aptca_Methods	0		Information	
VbNet	VbNet_Best_Coding_Practice	Declaration_Of_Catch_For_Generic_Exception	396		Information	
VbNet	VbNet_Best_Coding_Practice	Deprecated_Functions_or_Properties	477		Information	
VbNet	VbNet_Best_Coding_Practice	Detection_of_Error_Condition_Without_Action	390		Information	
VbNet	VbNet_Best_Coding_Practice	Direct_Use_of_Sockets	246		Information	
VbNet	VbNet_Best_Coding_Practice	Dynamic_SQL_Queries	89		Information	
VbNet	VbNet_Best_Coding_Practice	Exposure_of_Resource_to_Wrong_Sphere	493		Information	
VbNet	VbNet_Best_Coding_Practice	GetLastWin32Error_Is_Not_Called_After_Pinvoke	0		Information	
VbNet	VbNet_Best_Coding_Practice	Hardcoded_Absolute_Path	426		Information	
VbNet	VbNet_Best_Coding_Practice	Hardcoded_Connection_String	798		Information	
VbNet	VbNet_Best_Coding_Practice	Just_One_of_Equals_and_Hash_code_Defined	581		Information	
VbNet	VbNet_Best_Coding_Practice	Leftover_Debug_Code	489		Information	
VbNet	VbNet_Best_Coding_Practice	Missing_XML_Validation	112		Information	
VbNet	VbNet_Best_Coding_Practice	Non_Private_Static_Constructors	0		Information	
VbNet	VbNet_Best_Coding_Practice	NULL_Argument_to_Equals	0		Information	
VbNet	VbNet_Best_Coding_Practice	Pages_Without_Global_Error_Handler	544		Information	
VbNet	VbNet_Best_Coding_Practice	PersistSecurityInfo_is_True	0		Information	
VbNet	VbNet_Best_Coding_Practice	Threads_in_WebApp	383		Information	
VbNet	VbNet_Best_Coding_Practice	Unchecked_Error_Condition	0		Information	
VbNet	VbNet_Best_Coding_Practice	Unclosed_Objects	459		Information	
VbNet	VbNet_Best_Coding_Practice	Unvalidated_Arguments_Of_Public_Methods	0		Information	
VbNet	VbNet_Best_Coding_Practice	Use_of_System_Output_Stream	117		Information	
VbNet	VbNet_Best_Coding_Practice	Visible_Pointers	0		Information	
VbScript	VbScript_High_Risk	DOM_Code_Injection	94		High	
VbScript	VbScript_High_Risk	DOM_XSS	79		High	
VbScript	VbScript_Medium_Threat	Client_Untrusted_Activex	618		Medium	
VbScript	VbScript_Medium_Threat	DOM_Cookie_Poisoning	472		Medium	
VbScript	VbScript_Medium_Threat	DOM_CSRF	352		Medium	
VbScript	VbScript_Medium_Threat	DOM_Open_Redirect	601		Medium	
VbScript	VbScript_Low_Visibility	Client_DoS_By_Sleep	606		Low	
VbScript	VbScript_Low_Visibility	Compromised_CDN	0		Low	

Language Name	Package Name	Query Name	CWE ID	Status	Query Severity	Previous Query Severity
VbScript	VbScript_Low_Visibility	Cookies_Inspection	315		Low	
VbScript	VbScript_Low_Visibility	Weak_Password_Authentication	798		Low	