コンテンツパック・リリースノート（参考訳）

コンテンツパックには、クエリやプリセットの改善が含まれています。コンテンツパックを適用することで、DB テーブルがアップグレードされます。

注意事項：

1. 本コンテンツパックは「Checkmarx CxSAST 8.9.0 GA」用であり、8.8.0 以前のバージョンには適用されません。

2. コンテンツパックは、CxSAST のポータルサーバーにインストールします。
（エンジンサーバーへのインストールは必要ありません。）

3. C#用のコンテンツパックと Java 用のコンテンツパックの両方を適用する場合は、CP 番号の 8.9.0 の後に来る数字が小さい方から適用する必要があります。

4. Java 用のコンテンツパックに関しては、最新のもの（CP.8.9.0.94）を適用すれば、過去にリリースされたコンテンツパックの内容もすべて反映されます。

5. コンテンツパック（CP.8.9.0.94）適用時には、HF12 以降の Hotfix が適用済みの状態である必要があります。

詳細な改善内容については、以下に記します。

Content Pack Version – CP.8.9.0.12 Java 用

改善内容
本コンテンツパックには、誤検知を減らすための改善が含まれています。 次の **Java クエリ**が更新されます。 • LDAP_Injection • Stored_Absolute_Path_Traversal • Stored_Command_Injection • Stored_Relative_Path_Traversal • Improper_Restriction_of_stored_XXE_Ref

- Plaintext_Storage_of_a_Password
- Stored_LDAP_Injection
- Stored_Code_Injection
- Stored_HTTP_Response_Splitting
- Stored_Open_Redirect
- Stored_XPath_Injection
- Connection_String_Injection

クエリの変更の詳細:

- *LDAP_Injection* – ディレクトリコンテキスト検索メソッドを改善。 LDAP ESAPI を更新
- *Stored_XPath_Injection* – データベース出力とファイルストリームに対するサポート向上により、蓄積型入力を特定するメソッドを改善
- *Connection_String_Injection* –接続文字列の出力を改善
- データベースの入出力とファイルアクセスに関連した、その他クエリの改善

また、精度が向上された以下の Java クエリを含む、新しいプリセット:**Checkmarx Express** も本コンテンツパックには含まれています。

- LDAP_Injection
- Plaintext_Storage_of_a_Password
- Stored_LDAP_Injection
- Connection_String_Injection

本コンテンツパックによる解析精度の改善:

- **高リスクの脆弱性クエリ**については、**20%**精度が向上します。
- **中リスクの脆弱性クエリ**については、**22%**精度が向上します。

Content Pack Version – CP.8.9.0.53 Java 用

改善内容
本コンテンツパックには、誤検知を減らすための改善が含まれています。 次の **Java クエリ**が更新されます。 • Java.Java_Android.Android_Improper_Resource_Shutdown_or_Release • Java.Java_Android.Client_Side_Injection • Java.Java_Android.Client_Side_ReDoS • Java.Java_Android.Copy_Paste_Buffer_Caching • Java.Java_Android.General_Android_Find_Request_Permissions • Java.Java_Android.Implicit_Intent_With_Read_Write_Permissions • Java.Java_Android.Insecure_Data_Storage • Java.Java_Android.Insecure_Data_Storage_Usage • Java.Java_Android.Insecure_WebView_Usage • Java.Java_Android.Insufficient_Sensitive_Transport_Layer • Java.Java_Android.Insufficient_Transport_Layer_Protect • Java.Java_Android.Keyboard_Cache_Information_Leak • Java.Java_Android.Missing_Certificate_Pinning • Java.Java_Android.Missing_Rooted_Device_Check • Java.Java_Android.Passing_Non_Encrypted_Data_Between_Activities • Java.Java_Android.Poor_Authorization_and_Authentication • Java.Java_Android.Side_Channel_Data_Leakage • Java.Java_Android.Unsafe_Permission_Check • Java.Java_Android.Use_Of_Implicit_Intent_For_Sensitive_Communication • Java.Java_Android.Use_of_WebView_AddJavascriptInterface • Java.Java_Android.Weak_Encryption • Java.Java_Android.WebView_Cache_Information_Leak • Java.Java_Best_Coding_Practice.Access_Specifier_Manipulation • Java.Java_Best_Coding_Practice.clone_Method_Without_super_clone • Java.Java_Best_Coding_Practice.Comparison_of_Classes_By_Name • Java.Java_Best_Coding_Practice.Dynamic_SQL_Queries • Java.Java_Best_Coding_Practice.ESAPI_Banned_API • Java.Java_Best_Coding_Practice.Explicit_Call_to_Finalize • Java.Java_Best_Coding_Practice.finalize_Method_Without_super_finalize • Java.Java_Best_Coding_Practice.Hardcoded_Connection_String • Java.Java_Best_Coding_Practice.Incorrect_Conversion_between_Numeric_Types • Java.Java_Best_Coding_Practice.Input_Not_Normalized • Java.Java_Best_Coding_Practice.Non_serializable_Object_Stored_in_Session • Java.Java_Best_Coding_Practice.Portability_Flaw_In_File_Separator • Java.Java_Best_Coding_Practice.Potentially_Serializable_Class_With_Sensitive_Data • Java.Java_Best_Coding_Practice.Reliance_On_Untrusted_Inputs_In_Security_Decision

- Java.Java_Best_Coding_Practice.Unclosed_Objects
- Java.Java_Best_Coding_Practice.Uncontrolled_Recursion
- Java.Java_Best_Coding_Practice.Unused_Variable
- Java.Java_Best_Coding_Practice.Use_of_Obsolete_Functions
- Java.Java_Best_Coding_Practice.Use_of_System_Output_Stream
- Java.Java_Best_Coding_Practice.Use_of_Wrong_Operator_in_String_Comparison
- Java.Java_GWT.GWT_DOM_XSS
- Java.Java_GWT.GWT_Reflected_XSS
- Java.Java_GWT.JSON_Hijacking
- Java.Java_Heuristic.Heuristic_2nd_Order_SQL_Injection
- Java.Java_Heuristic.Heuristic_CGI_Stored_XSS
- Java.Java_Heuristic.Heuristic_DB_Parameter_Tampering
- Java.Java_Heuristic.Heuristic_Parameter_Tampering
- Java.Java_Heuristic.Heuristic_SQL_Injection
- Java.Java_Heuristic.Heuristic_Stored_XSS
- Java.Java_Heuristic.Heuristic_XSRF
- Java.Java_High_Risk.Code_Injection
- Java.Java_High_Risk.Command_Injection
- Java.Java_High_Risk.Connection_String_Injection
- Java.Java_High_Risk.Deserialization_of_Untrusted_Data_in_JMS
- Java.Java_High_Risk.Expression_Language_Injection_OGNL
- Java.Java_High_Risk.Expression_Language_Injection_SPEL
- Java.Java_High_Risk.LDAP_Injection
- Java.Java_High_Risk.Reflected_XSS_All_Clients
- Java.Java_High_Risk.Resource_Injection
- Java.Java_High_Risk.Second_Order_SQL_Injection
- Java.Java_High_Risk.Stored_XSS
- Java.Java_High_Risk.XPath_Injection
- Java.Java_Low_Visibility.Authorization_Bypass_Through_User_Controlled_SQL_PrimaryKe
- Java.Java_Low_Visibility.Blind_SQL_Injections
- Java.Java_Low_Visibility.Channel_Accessible_by_NonEndpoint
- Java.Java_Low_Visibility.Citrus_Developer_Mode_Enabled
- Java.Java_Low_Visibility.Collapse_of_Data_into_Unsafe_Value
- Java.Java_Low_Visibility.Cookie_Overly_Broad_Path
- Java.Java_Low_Visibility.Creation_of_Temp_File_With_Insecure_Permissions
- Java.Java_Low_Visibility.DB_Control_of_System_or_Config_Setting
- Java.Java_Low_Visibility.Divide_By_Zero
- Java.Java_Low_Visibility.Empty_Password_In_Connection_String
- Java.Java_Low_Visibility.ESAPI_Same_Password_Repeats_Twice
- Java.Java_Low_Visibility.Escape_False
- Java.Java_Low_Visibility.Exposure_of_System_Data
- Java.Java_Low_Visibility.Improper_Exception_Handling
- Java.Java_Low_Visibility.Improper_Resource_Access_Authorization
- Java.Java_Low_Visibility.Improper_Resource_Shutdown_or_Release

- Java.Java_Low_Visibility.Improper_Transaction_Handling
- Java.Java_Low_Visibility.Incorrect_Permission_Assignment_For_Critical_Resources
- Java.Java_Low_Visibility.Information_Exposure_Through_an_Error_Message
- Java.Java_Low_Visibility.Information_Exposure_Through_Debug_Log
- Java.Java_Low_Visibility.Information_Exposure_Through_Server_Log
- Java.Java_Low_Visibility.Information_Leak_Through_Comments
- Java.Java_Low_Visibility.Information_Leak_Through_Persistent_Cookies
- Java.Java_Low_Visibility.Information_Leak_Through_Shell_Error_Message
- Java.Java_Low_Visibility.Insufficiently_Protected_Credentials
- Java.Java_Low_Visibility.Integer_Overflow
- Java.Java_Low_Visibility.Integer_Underflow
- Java.Java_Low_Visibility.Leaving_Temporary_File
- Java.Java_Low_Visibility.Log_Forging
- Java.Java_Low_Visibility.Logic_Time_Bomb
- Java.Java_Low_Visibility.Missing_Password_Field_Masking
- Java.Java_Low_Visibility.Open_Redirect
- Java.Java_Low_Visibility.Logic_Time_Bomb
- Java.Java_Low_Visibility.Missing_Password_Field_Masking
- Java.Java_Low_Visibility.Open_Redirect
- Java.Java_Low_Visibility.Parse_Double_DoS
- Java.Java_Low_Visibility.Plaintext_Storage_in_a_Cookie
- Java.Java_Low_Visibility.Portability_Flaw_Locale_Dependent_Comparison
- Java.Java_Low_Visibility.Potential_ReDoS
- Java.Java_Low_Visibility.Potential_ReDoS_By_Injection
- Java.Java_Low_Visibility.Potential_ReDoS_In_Match
- Java.Java_Low_Visibility.Potential_ReDoS_In_Replace
- Java.Java_Low_Visibility.Potential_ReDoS_In_Static_Field
- Java.Java_Low_Visibility.Private_Array_Returned_From_A_Public_Method
- Java.Java_Low_Visibility.Public_Data_Assigned_to_Private_Array
- Java.Java_Low_Visibility.Race_Condition_Format_Flaw
- Java.Java_Low_Visibility.Relative_Path_Traversal
- Java.Java_Low_Visibility.Reversible_One_Way_Hash
- Java.Java_Low_Visibility.Serializable_Class_Containing_Sensitive_Data
- Java.Java_Low_Visibility.Stored_Absolute_Path_Traversal
- Java.Java_Low_Visibility.Stored_Command_Injection
- Java.Java_Low_Visibility.Stored_Log_Forging
- Java.Java_Low_Visibility.Stored_Relative_Path_Traversal
- Java.Java_Low_Visibility.Storing_Passwords_in_a_Recoverable_Format
- Java.Java_Low_Visibility.Suspected_XSS
- Java.Java_Low_Visibility.TOCTOU
- Java.Java_Low_Visibility.Uncaught_Exception
- Java.Java_Low_Visibility.Uncontrolled_Memory_Allocation
- Java.Java_Low_Visibility.Unrestricted_File_Upload
- Java.Java_Low_Visibility.Unsynchronized_Access_To_Shared_Data

- Java.Java_Low_Visibility.Use_of_Broken_or_Risky_Cryptographic_Algorithm
- Java.Java_Low_Visibility.Use_of_Client_Side_Authentication
- Java.Java_Low_Visibility.Use_Of_getenv
- Java.Java_Low_Visibility.Use_of_Hard_coded_Security_Constants
- Java.Java_Low_Visibility.Use_Of_Hardcoded_Password
- Java.Java_Low_Visibility.UTF7_XSS
- Java.Java_Medium_Threat.Absolute_Path_Traversal
- Java.Java_Medium_Threat.CGI_Reflected_XSS_All_Clients
- Java.Java_Medium_Threat.CGI_Stored_XSS
- Java.Java_Medium_Threat.Cleartext_Submission_of_Sensitive_Information
- Java.Java_Medium_Threat.Cross_Site_History_Manipulation
- Java.Java_Medium_Threat.Dangerous_File_Inclusion
- Java.Java_Medium_Threat.DB_Parameter_Tampering
- Java.Java_Medium_Threat.Direct_Use_of_Unsafe_JNI
- Java.Java_Medium_Threat.DoS_by_Sleep
- Java.Java_Medium_Threat.Download_of_Code_Without_Integrity_Check
- Java.Java_Medium_Threat.External_Control_of_Critical_State_Data
- Java.Java_Medium_Threat.External_Control_of_System_or_Config_Setting
- Java.Java_Medium_Threat.Frameable_Login_Page
- Java.Java_Medium_Threat.Hardcoded_password_in_Connection_String
- Java.Java_Medium_Threat.Heap_Inspection
- Java.Java_Medium_Threat.HTTP_Response_Splitting
- Java.Java_Medium_Threat.HttpOnlyCookies
- Java.Java_Medium_Threat.Improper_Restriction_of_Stored_XXE_Ref
- Java.Java_Medium_Threat.Improper_Restriction_of_XXE_Ref
- Java.Java_Medium_Threat.Inadequate_Encryption_Strength
- Java.Java_Medium_Threat.Input_Path_Not_Canonicalized
- Java.Java_Medium_Threat.Multiple_Binds_to_the_Same_Port
- Java.Java_Medium_Threat.Parameter_Tampering
- Java.Java_Medium_Threat.Plaintext_Storage_of_a_Password
- Java.Java_Medium_Threat.Privacy_Violation
- Java.Java_Medium_Threat.Process_Control
- Java.Java_Medium_Threat.ReDoS_From_Regex_Injection
- Java.Java_Medium_Threat.ReDoS_In_Match
- Java.Java_Medium_Threat.ReDoS_In_Pattern
- Java.Java_Medium_Threat.ReDoS_In_Replace
- Java.Java_Medium_Threat.Session_Fixation
- Java.Java_Medium_Threat.Spring_ModelView_Injection
- Java.Java_Medium_Threat.SQL_Injection_Evasion_Attack
- Java.Java_Medium_Threat.SSRF
- Java.Java_Medium_Threat.Stored_LDAP_Injection
- Java.Java_Medium_Threat.Trust_Boundary_Violation
- Java.Java_Medium_Threat.Unchecked_Input_for_Loop_Condition
- Java.Java_Medium_Threat.Uncontrolled_Format_String

- Java.Java_Medium_Threat.Unvalidated_Forwards
- Java.Java_Medium_Threat.Use_of_a_One_Way_Hash_with_a_Predictable_Salt
- Java.Java_Medium_Threat.Use_of_Cryptographically_Weak_PRNG
- Java.Java_Medium_Threat.Use_of_Insufficiently_Random_Values
- Java.Java_Medium_Threat.Use_of_Native_Language
- Java.Java_Medium_Threat.XQuery_Injection
- Java.Java_Medium_Threat.XSRF
- Java.Java_Potential.Potential_Code_Injection
- Java.Java_Potential.Potential_Command_Injection
- Java.Java_Potential.Potential_Connection_String_Injection
- Java.Java_Potential.Potential_GWT_Reflected_XSS
- Java.Java_Potential.Potential_I_Reflected_XSS_All_Clients
- Java.Java_Potential.Potential_IO_Reflected_XSS_All_Clients
- Java.Java_Potential.Potential_LDAP_Injection
- Java.Java_Potential.Potential_O_Reflected_XSS_All_Clients
- Java.Java_Potential.Potential_Parameter_Tampering
- Java.Java_Potential.Potential_Resource_Injection
- Java.Java_Potential.Potential_SQL_Injection
- Java.Java_Potential.Potential_Stored_XSS
- Java.Java_Potential.Potential_UTF7_XSS
- Java.Java_Potential.Potential_XPath_Injection
- Java.Java_Potential.Potential_XXE_Injection
- Java.Java_Stored.Stored_Boundary_Violation
- Java.Java_Stored.Stored_Code_Injection
- Java.Java_Stored.Stored_HTTP_Response_Splitting
- Java.Java_Stored.Stored_Open_Redirect
- Java.Java_Stored.Stored_XPath_Injection
- Java.Java_Struts.Struts2_Action_Field_Without_Validator

クエリの変更の詳細

- クロスサイトスクリプティングの AWT および Swing の制御を改善
- Base 64 エンコーダーとデコーダーの無害化処理を改善
- Expression_Language_Injection の実行箇所を改善
- コマンドインジェクションの出力を改善
- すでにアプリケーションスコープ内に存在するクラスをロードする場合、コードインジェクションを取り止め
- データベース接続文字列の使用を改善
- LDAP 安全なメソッドに対するサポートを強化
- JSP 入力の精度を向上
- データベース入力を改善
- ファイル入力の改善
- XSS での JSON API を取り止め
- パスワード関連の変数を改善

- 機密データ情報の SSL ソケットに対するサポートを拡張
- ヒープインスペクション結果の信頼度を改善
- ハードコードされた暗号化キーを改善
- ハードコードされたデータベース認証情報を改善
- プロパティリソースを無害化処理の入力と認識するように改善
- Inadequate_Encryption_Strength クエリを非推奨に
- CGI html 出力を改善

また、精度が向上された以下の Java クエリを含む、新しいプリセット：**Checkmarx Express** も本コンテンツパックには含まれています。

- Code_Injection
- Command_Injection
- Connection_String_Injection
- LDAP_Injection
- Reflected_XSS_All_Clients
- Resource_Injection
- Second_Order_SQL_Injection
- SQL_Injection
- Stored_XSS
- XPath_Injection
- Use_Of_Hardcoded_Password
- Log_Forging
- Open_Redirect
- Use_of_Broken_or_Risky_Cryptographic_Algorithm
- DB_Parameter_Tampering
- DoS_by_Sleep
- Use_of_Hard_coded_Cryptographic_Key
- Hardcoded_password_in_Connection_String
- Parameter_Tampering
- Privacy_Violation
- Spring_ModelView_Injection
- SQL_Injection_Evasion_Attack
- Trust_Boundary_Violation
- XSRF
- Struts_Incomplete_Validate_Method_Definition
- Struts_Form_Does_Not_Extend_Validation_Class
- Struts_Validation_Turned_Off
- Absolute_Path_Traversal
- Cleartext_Submission_of_Sensitive_Information
- Plaintext_Storage_of_a_Password
- Stored_LDAP_Injection
- Use_of_Cryptographically_Weak_PRNG
- Use_of_a_One_Way_Hash_with_a_Predictable_Salt

- Use_of_a_One_Way_Hash_without_a_Salt
- Unchecked_Input_for_Loop_Condition
- Session_Fixation
- HttpOnlyCookies
- Unvalidated_Forwards
- Improper_Restriction_of_XXE_Ref
- Heap_Inspection
- Inadequate_Encryption_Strength
- SSRF
- Improper_Restriction_of_Stored_XXE_Ref
- Password_In_Comment
- Deserialization_of_Untrusted_Data
- Unvalidated_SSL_Certificate_Hostname
- Expression_Language_Injection_OGNL
- Deserialization_of_Untrusted_Data_in_JMS
- Missing_HSTS_Header
- Unsafe_Object_Binding
- GWT_DOM_XSS
- GWT_Reflected_XSS

本コンテンツパックによる解析精度の改善：

- Checkmarx Express プリセットに登録されている**高リスクの脆弱性クエリ**については、**31%**精度が向上します。
- Checkmarx Express プリセットに登録されている**中リスクの脆弱性クエリ**については、**62%**精度が向上します。

Content Pack Version – CP.8.9.0.94 Java 用

改善内容
（注）本コンテンツパックの適用は、HF12 以降の Hotfix の適用後にお願いします。 本コンテンツパックには、誤検知を減らすための改善が含まれています。 次の **Java クエリ**について、コンテンツパック 53 から更なる改善が行われました。 • ハードコードされた暗号化キーを改善 • 接続文字列パスワードの無害化処理を改善 • ログ出力を改善 • 安全なランダム値をサポート • 暗号化されていない通信チャネルの検出を追加 • XSS の無害化処理をサポート。 • ORM 使用時のデータベース出力をサポート • DOS_by_Sleep 攻撃の無害化処理を追加 • ユニットテストを悪用可能な結果としての考慮から除外 • コードインジェクションの無害化処理を改善 • コマンドインジェクションの無害化処理を改善 • 機密情報の平文テキスト送信の入力元を改善 • ハードコードされた暗号化キーの使用のための入力元を改善 • 接続文字列でのハードコードされたパスワードの入力元を改良 • 暗号の弱い PRNG の使用に関する入力元を拡張 • データベースクエリ入力を拡張 • Potential_Hardcoded_password_in_Connection_String を追加 • Potential_Use_of_Hard_coded_Cryptographic_Key を追加 また、本コンテンツパックには以下の 52 のクエリを含む **Checkmarx Express** プリセットも含まれています。 • Java_GWT.GWT_DOM_XSS • Java_GWT.GWT_Reflected_XSS • Java_High_Risk.Code_Injection • Java_High_Risk.Command_Injection • Java_High_Risk.Connection_String_Injection • Java_High_Risk.LDAP_Injection • Java_High_Risk.Reflected_XSS_All_Clients • Java_High_Risk.Resource_Injection • Java_High_Risk.Second_Order_SQL_Injection • Java_High_Risk.SQL_Injection • Java_High_Risk.Stored_XSS • Java_High_Risk.XPath_Injection

- Java_Low_Visibility.Use_Of_Hardcoded_Password
- Java_Low_Visibility.Log_Forging
- Java_Low_Visibility.Open_Redirect
- Java_Low_Visibility.Use_of_Broken_or_Risky_Cryptographic_Algorithm
- Java_Medium_Threat.DB_Parameter_Tampering
- Java_Medium_Threat.DoS_by_Sleep
- Java_Medium_Threat.Use_of_Hard_coded_Cryptographic_Key
- Java_Medium_Threat.Hardcoded_password_in_Connection_String
- Java_Medium_Threat.Parameter_Tampering
- Java_Medium_Threat.Privacy_Violation
- Java_Medium_Threat.Spring_ModelView_Injection
- Java_Medium_Threat.SQL_Injection_Evasion_Attack
- Java_Medium_Threat.Trust_Boundary_Violation
- Java_Medium_Threat.XSRF
- Java_Struts.Struts_Incomplete_Validate_Method_Definition
- Java_Struts.Struts_Form_Does_Not_Extend_Validation_Class
- Java_Struts.Struts_Validation_Turned_Off
- Java_Medium_Threat.Absolute_Path_Traversal
- Java_Medium_Threat.Cleartext_Submission_of_Sensitive_Information
- Java_Medium_Threat.Plaintext_Storage_of_a_Password
- Java_Medium_Threat.Stored_LDAP_Injection
- Java_Medium_Threat.Use_of_Cryptographically_Weak_PRNG
- Java_Medium_Threat.Use_of_a_One_Way_Hash_with_a_Predictable_Salt
- Java_Medium_Threat.Use_of_a_One_Way_Hash_without_a_Salt
- Java_Medium_Threat.Unchecked_Input_for_Loop_Condition
- Java_Medium_Threat.Session_Fixation
- Java_Medium_Threat.HttpOnlyCookies
- Java_Medium_Threat.Unvalidated_Forwards
- Java_Medium_Threat.Improper_Restriction_of_XXE_Ref
- Java_Medium_Threat.Heap_Inspection
- Java_Medium_Threat.Inadequate_Encryption_Strength
- Java_Medium_Threat.SSRF
- Java_Medium_Threat.Improper_Restriction_of_Stored_XXE_Ref
- Java_Low_Visibility.Password_In_Comment
- Java_High_Risk.Deserialization_of_Untrusted_Data
- Java_Medium_Threat.Unvalidated_SSL_Certificate_Hostname
- Java_High_Risk.Expression_Language_Injection_OGNL
- Java_High_Risk.Deserialization_of_Untrusted_Data_in_JMS
- Java_Medium_Threat.Missing_HSTS_Header
- Java_Medium_Threat.Unsafe_Object_Binding

精度= TP ／（ TP + FP ）

本コンテンツパックによって影響受けるクエリ

- Java.Java_Medium_Threat.Improper_Restriction_of_XXE_Ref
- Java.Java_Low_Visibility.Information_Leak_Through_Persistent_Cookies
- Java.Java_Best_Coding_Practice.Unused_Variable
- Java.Java_Android.Copy_Paste_Buffer_Caching
- Java.Java_Medium_Threat.DB_Parameter_Tampering
- Java.Java_Low_Visibility.Improper_Exception_Handling
- Java.Java_Medium_Threat.Cleartext_Submission_of_Sensitive_Information
- Java.Java_Medium_Threat.Trust_Boundary_Violation
- Java.Java_Medium_Threat.Use_of_Cryptographically_Weak_PRNG
- Java.Java_Low_Visibility.Potential_ReDoS_In_Replace
- Java.Java_Potential.Potential_Stored_XSS
- Java.Java_Best_Coding_Practice.Access_Specifier_Manipulation
- Java.Java_Low_Visibility.Citrus_Developer_Mode_Enabled
- Java.Java_Low_Visibility.Collapse_of_Data_into_Unsafe_Value
- Java.Java_Medium_Threat.SSRF
- Java.Java_Best_Coding_Practice.finalize_Method_Without_super_finalize
- Java.Java_Low_Visibility.Portability_Flaw_Locale_Dependent_Comparison
- Java.Java_Low_Visibility.Uncaught_Exception
- Java.Java_Best_Coding_Practice.Incorrect_Conversion_between_Numeric_Types
- Java.Java_Medium_Threat.Spring_ModelView_Injection
- Java.Java_Stored.Stored_HTTP_Response_Splitting
- Java.Java_Low_Visibility.Use_Of_Hardcoded_Password
- Java.Java_Low_Visibility.Information_Exposure_Through_Debug_Log
- Java.Java_Best_Coding_Practice.Comparison_of_Classes_By_Name
- Java.Java_Medium_Threat.Stored_LDAP_Injection
- Java.Java_Low_Visibility.Potential_ReDoS_In_Match
- Java.Java_Heuristic.Heuristic_SQL_Injection
- Java.Java_Best_Coding_Practice.Reliance_On_Untrusted_Inputs_In_Security_Decision
- Java.Java_Android.Missing_Rooted_Device_Check
- Java.Java_Low_Visibility.Use_of_Hard_coded_Security_Constants
- Java.Java_Medium_Threat.Privacy_Violation
- Java.Java_Android.Client_Side_Injection
- Java.Java_Low_Visibility.Exposure_of_System_Data
- Java.Java_Low_Visibility.Serializable_Class_Containing_Sensitive_Data
- Java.Java_Low_Visibility.Divide_By_Zero
- Java.Java_Low_Visibility.Incorrect_Permission_Assignment_For_Critical_Resources
- Java.Java_Low_Visibility.Logic_Time_Bomb
- Java.Java_Best_Coding_Practice.clone_Method_Without_super_clone
- Java.Java_Potential.Potential_I_Reflected_XSS_All_Clients
- Java.Java_High_Risk.Command_Injection
- Java.Java_Low_Visibility.Potential_ReDoS_By_Injection
- Java.Java_Medium_Threat.ReDoS_In_Replace

- Java.Java_Low_Visibility.Relative_Path_Traversal
- Java.Java_Low_Visibility.Cookie_Overly_Broad_Path
- Java.Java_Potential.Potential_Resource_Injection
- Java.Java_High_Risk.Stored_XSS
- Java.Java_Medium_Threat.External_Control_of_System_or_Config_Setting
- Java.Java_Best_Coding_Practice.Portability_Flaw_In_File_Separator
- Java.Java_Best_Coding_Practice.Uncontrolled_Recursion
- Java.Java_Low_Visibility.Stored_Log_Forging
- Java.Java_Low_Visibility.Creation_of_Temp_File_With_Insecure_Permissions
- Java.Java_Best_Coding_Practice.Potentially_Serializable_Class_With_Sensitive_Data
- Java.Java_Android.Missing_Certificate_Pinning
- Java.Java_Medium_Threat.ReDoS_In_Match
- Java.Java_Best_Coding_Practice.Use_of_Wrong_Operator_in_String_Comparison
- Java.Java_Android.General_Android_Find_Request_Permissions
- Java.Java_Best_Coding_Practice.Non_serializable_Object_Stored_in_Session
- Java.Java_Android.Implicit_Intent_With_Read_Write_Permissions
- Java.Java_Medium_Threat.ReDoS_In_Pattern
- Java.Java_Low_Visibility.Leaving_Temporary_File
- Java.Java_Android.Weak_Encryption
- Java.Java_Low_Visibility.Suspected_XSS
- Java.Java_Potential.Potential_IO_Reflected_XSS_All_Clients
- Java.Java_Low_Visibility.Stored_Relative_Path_Traversal
- Java.Java_Potential.Potential_UTF7_XSS
- Java.Java_Low_Visibility.Improper_Transaction_Handling
- Java.Java_Stored.Stored_Code_Injection
- Java.Java_Potential.Potential_Parameter_Tampering
- Java.Java_High_Risk.Resource_Injection
- Java.Java_Medium_Threat.Frameable_Login_Page
- Java.Java_Medium_Threat.Input_Path_Not_Canonicalized
- Java.Java_Low_Visibility.Stored_Absolute_Path_Traversal
- Java.Java_Potential.Potential_O_Reflected_XSS_All_Clients
- Java.Java_Android.Poor_Authorization_and_Authentication
- Java.Java_Potential.Potential_Use_of_Hard_coded_Cryptographic_Key
- Java.Java_Medium_Threat.Process_Control
- Java.Java_Low_Visibility.Use_of_Broken_or_Risky_Cryptographic_Algorithm
- Java.Java_High_Risk.Code_Injection
- Java.Java_Stored.Stored_XPath_Injection
- Java.Java_Android.Insecure_Data_Storage
- Java.Java_Low_Visibility.Use_of_Client_Side_Authentication
- Java.Java_Low_Visibility.UTF7_XSS
- Java.Java_Low_Visibility.DB_Control_of_System_or_Config_Setting
- Java.Java_Best_Coding_Practice.Input_Not_Normalized
- Java.Java_Low_Visibility.Integer_Underflow
- Java.Java_Medium_Threat.Dangerous_File_Inclusion

- Java.Java_Medium_Threat.Use_of_Insufficiently_Random_Values
- Java.Java_Heuristic.Heuristic_DB_Parameter_Tampering
- Java.Java_Best_Coding_Practice.Use_of_Obsolete_Functions
- Java.Java_Android.Keyboard_Cache_Information_Leak
- Java.Java_Medium_Threat.Absolute_Path_Traversal
- Java.Java_Low_Visibility.Race_Condition_Format_Flaw
- Java.Java_Medium_Threat.Use_of_a_One_Way_Hash_with_a_Predictable_Salt
- Java.Java_Medium_Threat.Multiple_Binds_to_the_Same_Port
- Java.Java_Low_Visibility.Uncontrolled_Memory_Allocation
- Java.Java_Low_Visibility.Plaintext_Storage_in_a_Cookie
- Java.Java_GWT.GWT_Reflected_XSS
- Java.Java_Low_Visibility.Unsynchronized_Access_To_Shared_Data
- Java.Java_GWT.GWT_DOM_XSS
- Java.Java_Medium_Threat.Download_of_Code_Without_Integrity_Check
- Java.Java_Heuristic.Heuristic_Stored_XSS
- Java.Java_Low_Visibility.Empty_Password_In_Connection_String
- Java.Java_Low_Visibility.Unrestricted_File_Upload
- Java.Java_Low_Visibility.Reversible_One_Way_Hash
- Java.Java_Medium_Threat.Unchecked_Input_for_Loop_Condition
- Java.Java_Potential.Potential_GWT_Reflected_XSS
- Java.Java_Medium_Threat.ReDoS_From_Regex_Injection
- Java.Java_Low_Visibility.Insufficiently_Protected_Credentials
- Java.Java_Low_Visibility.Use_Of_getenv
- Java.Java_Android.Insufficient_Sensitive_Transport_Layer
- Java.Java_Potential.Potential_Command_Injection
- Java.Java_Medium_Threat.Inadequate_Encryption_Strength
- Java.Java_Potential.Potential_Connection_String_Injection
- Java.Java_Heuristic.Heuristic_XSRF
- Java.Java_Low_Visibility.Private_Array_Returned_From_A_Public_Method
- Java.Java_Low_Visibility.Potential_ReDoS_In_Static_Field
- Java.Java_Low_Visibility.Improper_Resource_Shutdown_or_Release
- Java.Java_Low_Visibility.Authorization_Bypass_Through_User_Controlled_SQL_PrimaryKey
- Java.Java_Best_Coding_Practice.Unclosed_Objects
- Java.Java_High_Risk.Second_Order_SQL_Injection
- Java.Java_Low_Visibility.Channel_Accessible_by_NonEndpoint
- Java.Java_Potential.Potential_XPath_Injection
- Java.Java_Medium_Threat.Improper_Restriction_of_Stored_XXE_Ref
- Java.Java_Low_Visibility.Missing_Password_Field_Masking
- Java.Java_Medium_Threat.Uncontrolled_Format_String
- Java.Java_Best_Coding_Practice.Explicit_Call_to_Finalize
- Java.Java_High_Risk.Reflected_XSS_All_Clients
- Java.Java_Potential.Potential_SQL_Injection
- Java.Java_Medium_Threat.Use_of_Native_Language
- Java.Java_Medium_Threat.External_Control_of_Critical_State_Data

- Java.Java_Low_Visibility.Information_Leak_Through_Shell_Error_Message
- Java.Java_Medium_Threat.Session_Fixation
- Java.Java_Low_Visibility.ESAPI_Same_Password_Repeats_Twice
- Java.Java_Medium_Threat.Hardcoded_password_in_Connection_String
- Java.Java_Low_Visibility.Public_Data_Assigned_to_Private_Array
- Java.Java_Low_Visibility.Information_Exposure_Through_Server_Log
- Java.Java_Low_Visibility.Stored_Command_Injection
- Java.Java_Medium_Threat.Heap_Inspection
- Java.Java_Best_Coding_Practice.Use_of_System_Output_Stream
- Java.Java_High_Risk.Deserialization_of_Untrusted_Data_in_JMS
- Java.Java_Best_Coding_Practice.Hardcoded_Connection_String
- Java.Java_Android.Android_Improper_Resource_Shutdown_or_Release
- Java.Java_Medium_Threat.SQL_Injection_Evasion_Attack
- Java.Java_Low_Visibility.Information_Exposure_Through_an_Error_Message
- Java.Java_Medium_Threat.XSRF
- Java.Java_Potential.Potential_Code_Injection
- Java.Java_High_Risk.Connection_String_Injection
- Java.Java_Android.Use_of_WebView_AddJavascriptInterface
- Java.Java_Android.Passing_Non_Encrypted_Data_Between_Activities
- Java.Java_Android.Side_Channel_Data_Leakage
- Java.Java_Best_Coding_Practice.ESAPI_Banned_API
- Java.Java_High_Risk.Expression_Language_Injection_OGNL
- Java.Java_Low_Visibility.Information_Leak_Through_Comments
- Java.Java_Potential.Potential_XXE_Injection
- Java.Java_Stored.Stored_Open_Redirect
- Java.Java_High_Risk.Expression_Language_Injection_SPEL
- Java.Java_High_Risk.LDAP_Injection
- Java.Java_Low_Visibility.Blind_SQL_Injections
- Java.Java_Android.Insecure_WebView_Usage
- Java.Java_Low_Visibility.Integer_Overflow
- Java.Java_Heuristic.Heuristic_2nd_Order_SQL_Injection
- Java.Java_Low_Visibility.Open_Redirect
- Java.Java_Medium_Threat.CGI_Reflected_XSS_All_Clients
- Java.Java_Stored.Stored_Boundary_Violation
- Java.Java_Heuristic.Heuristic_Parameter_Tampering
- Java.Java_Medium_Threat.XQuery_Injection
- Java.Java_Android.Insufficient_Transport_Layer_Protect
- Java.Java_Low_Visibility.Improper_Resource_Access_Authorization
- Java.Java_Android.Use_Of_Implicit_Intent_For_Sensitive_Communication
- Java.Java_High_Risk.XPath_Injection
- Java.Java_Low_Visibility.Storing_Passwords_in_a_Recoverable_Format
- Java.Java_Struts.Struts2_Action_Field_Without_Validator
- Java.Java_Medium_Threat.Cross_Site_History_Manipulation
- Java.Java_Heuristic.Heuristic_CGI_Stored_XSS

- Java.Java_Medium_Threat.DoS_by_Sleep
- Java.Java_Medium_Threat.HttpOnlyCookies
- Java.Java_Medium_Threat.CGI_Stored_XSS
- Java.Java_Android.WebView_Cache_Information_Leak
- Java.Java_Best_Coding_Practice.Dynamic_SQL_Queries
- Java.Java_Medium_Threat.Plaintext_Storage_of_a_Password
- Java.Java_Medium_Threat.Unvalidated_Forwards
- Java.Java_Android.Insecure_Data_Storage_Usage
- Java.Java_Low_Visibility.Parse_Double_DoS
- Java.Java_GWT.JSON_Hijacking
- Java.Java_Android.Unsafe_Permission_Check
- Java.Java_Medium_Threat.HTTP_Response_Splitting
- Java.Java_Medium_Threat.Parameter_Tampering
- Java.Java_Medium_Threat.Direct_Use_of_Unsafe_JNI
- Java.Java_Low_Visibility.TOCTOU
- Java.Java_Low_Visibility.Escape_False
- Java.Java_Low_Visibility.Potential_ReDoS
- Java.Java_Android.Client_Side_ReDoS
- Java.Java_Low_Visibility.Log_Forging
- Java.Java_Potential.Potential_LDAP_Injection
- Java.Java_Potential.Potential_Hardcoded_password_in_Connection_String

本コンテンツパックによる解析精度の改善：

- Checkmarx Express プリセットに登録されている**高リスクの脆弱性クエリ**については、**58%**精度が向上します。
- Checkmarx Express プリセットに登録されている **中リスクの脆弱性クエリ**については、**97%**精度が向上します。
- **OWASP Benchmark** のグレードアップ、現在のスコアは **72%**

Content Pack Version – CP.8.9.0.60123 C#用

改善内容
本コンテンツパックは、C#言語用です。クエリの改善とコンテンツパックの適用で利用可能となる Checkmarx Express プリセットの機能拡張が含まれています。 本コンテンツパックによる、Checkmarx Express の C# クエリにおける解析精度の改善: • **高リスクの脆弱性クエリ**については、 **39%**精度が向上します。 • **中リスクの脆弱性クエリ**については、 **2%**精度が向上します。 本コンテンツパックの適用により新たな脆弱性の検出が可能となる場合もありますが、 それは副次的な結果であり、適用の主な目的は誤検知の削減と解析精度の向上にあることを ご了承ください。 **C# クエリ** について、次の改善が行われました。 • Code_Injection において、スクリプトおよび非同期 API を使用したシンク箇所の特定機能を改善 • 静的な文字列を対象から除外するように、Connection_String_Injection の無害化処理を改善 • Deserialization_of_Untrusted_Data を使ったデシリアライズ処理に BinaryFormatter と SerializationBinder を含むことで、シンク箇所の特定機能を改善 • 文字列の無害化処理メソッド、エンコーディング、ホワイトリスト方式を、Resource_Injection の無害化処理に追加 • Stored_XSS の無害化処理を改善 • XPath_Injection と Stored_XPath_Injection の無害化処理を改善 • Stored_Code_Injection の無害化処理を改善し、コンパイラオプションの Output Assembly を追加 • 権限チェックの有無を考慮するように、DB_Parameter_Tampering の無害化処理を改善 • SpinWait と ThreadSleep API が適切に設定された場合における、DOS_By_Sleep の無害化処理を改善 • 静的な文字列を含む変数を接続文字列の入力値に使用した時に、誤検出しないように、Hardcoded_Password を改善 • ページビューコントロールに対する Heap_Inspection の解析結果に誤検知が発生する問題を修正 • デコード API の更なる拡張により、SQL_Injection_Evasion_Attack の無害化処理を改善 • 数値型を使用している箇所およびにセッションを保存しているシンク箇所を Trust_Boundary_Violation の無害化処理対象に追加 • OID(暗号オブジェクトの識別子)を避けて、復号化した値を安全と見なすように Use_of_Hard_coded_Cryptographic_Key の無害化処理を改善

- 不適切な構成が使用されている場合に、API から結果が返されるまでの時間が適切に確保されるように Missing_HSTS_Header を改善
- ASP の MVC コントローラに対するサポートを改善
- ASP の MVC/Razor XSRF トークンに対するサポートを改善
- ホワイトリスト方式と数値型の API を使用したときの一般的な無害化処理を改善
- Entity Framework の API に対するサポートを改善
- 非同期 API に対するデータベースのサポートを改善
- LINQ で使われる API に対するデータベースのサポートを改善
- Salesforce の API に対するデータベースのサポートを改善
- 安全なハッシュアルゴリズムに対するサポートを改善
- Deserialization_of_untrusted_data を改善
- 改良したソースとシンクの特定処理を用いて、Unsafe_Object_Binding を書き直し

本コンテンツパックには、以下の 38 の C#用クエリを含む **Checkmarx Express** プリセットも含まれています。

- CSharp.High_Risk.Code_Injection
- CSharp.High_Risk.Command_Injection
- CSharp.High_Risk.Connection_String_Injection
- CSharp.High_Risk.LDAP_Injection
- CSharp.High_Risk.Reflected_XSS_All_Clients
- CSharp.High_Risk.Resource_Injection
- CSharp.High_Risk.Second_Order_SQL_Injection
- CSharp.High_Risk.SQL_Injection
- CSharp.High_Risk.Stored_XSS
- CSharp.High_Risk.XPath_Injection
- CSharp.Low_Visibility.Use_Of_Hardcoded_Password
- CSharp.Low_Visibility.Log_Forging
- CSharp.Low_Visibility.Open_Redirect
- CSharp.Medium_Threat.DB_Parameter_Tampering
- CSharp.Medium_Threat.DoS_by_Sleep
- CSharp.Medium_Threat.Path_Traversal
- CSharp.Medium_Threat.Use_of_Hard_coded_Cryptographic_Key
- CSharp.Medium_Threat.Hardcoded_password_in_Connection_String
- CSharp.Medium_Threat.Privacy_Violation
- CSharp.Medium_Threat.ReDoS_By_Regex_Injection
- CSharp.Medium_Threat.SQL_Injection_Evasion_Attack
- CSharp.Medium_Threat.Trust_Boundary_Violation
- CSharp.Medium_Threat.XSRF
- CSharp.Medium_Threat.Session_Fixation
- CSharp.Medium_Threat.Use_of_Cryptographically_Weak_PRNG
- CSharp.Low_Visibility.Use_Of_Broken_Or_Risky_Cryptographic_Algorithm
- CSharp.Medium_Threat.HttpOnlyCookies
- CSharp.Medium_Threat.MVC_View_Injection

- CSharp.Medium_Threat.No_Request_Validation
- CSharp.Medium_Threat.Stored_LDAP_Injection
- CSharp.Medium_Threat.Stored_XPath_Injection
- CSharp.Medium_Threat.Insecure_Cookie
- CSharp.Medium_Threat.Improper_Restriction_of_XXE_Ref
- CSharp.Medium_Threat.Heap_Inspection
- CSharp.Medium_Threat.Unsafe_Object_Binding
- CSharp.High_Risk.Deserialization_of_Untrusted_Data
- CSharp.Medium_Threat.Missing_HSTS_Header
- CSharp.High_Risk.Deserialization_of_Untrusted_Data_MSMQ

本コンテンツパックをインストールすることで以下のクエリが改善され、解析精度が向上します。

- CSharp.CSharp_Best_Coding_Practice.Dynamic_SQL_Queries
- CSharp.CSharp_Heuristic.Heuristic_2nd_Order_SQL_Injection
- CSharp.CSharp_Heuristic.Heuristic_DB_Parameter_Tampering
- CSharp.CSharp_Heuristic.Heuristic_Parameter_Tampering
- CSharp.CSharp_Heuristic.Heuristic_SQL_Injection
- CSharp.CSharp_Heuristic.Heuristic_Stored_XSS
- CSharp.CSharp_Heuristic.Heuristic_XSRF
- CSharp.CSharp_High_Risk.Code_Injection
- CSharp.CSharp_High_Risk.Command_Injection
- CSharp.CSharp_High_Risk.Connection_String_Injection
- CSharp.CSharp_High_Risk.Deserialization_of_Untrusted_Data
- CSharp.CSharp_High_Risk.Deserialization_of_Untrusted_Data_MSMQ
- CSharp.CSharp_High_Risk.LDAP_Injection
- CSharp.CSharp_High_Risk.Reflected_XSS_All_Clients
- CSharp.CSharp_High_Risk.Resource_Injection
- CSharp.CSharp_High_Risk.Second_Order_SQL_Injection
- CSharp.CSharp_High_Risk.Stored_XSS
- CSharp.CSharp_High_Risk.UTF7_XSS
- CSharp.CSharp_High_Risk.XPath_Injection
- CSharp.CSharp_Medium_Threat.Buffer_Overflow
- CSharp.CSharp_Medium_Threat.CGI_XSS
- CSharp.CSharp_Medium_Threat.Cookie_Injection
- CSharp.CSharp_Medium_Threat.Data_Filter_Injection
- CSharp.CSharp_Medium_Threat.DB_Parameter_Tampering
- CSharp.CSharp_Medium_Threat.DoS_by_Sleep
- CSharp.CSharp_Medium_Threat.Hardcoded_password_in_Connection_String
- CSharp.CSharp_Medium_Threat.Heap_Inspection
- CSharp.CSharp_Medium_Threat.HTTP_Response_Splitting
- CSharp.CSharp_Medium_Threat.Improper_Restriction_of_XXE_Ref
- CSharp.CSharp_Medium_Threat.Insufficient_Connection_String_Encryption
- CSharp.CSharp_Medium_Threat.Missing_Column_Encryption

- CSharp.CSharp_Medium_Threat.MVC_View_Injection
- CSharp.CSharp_Medium_Threat.Parameter_Tampering
- CSharp.CSharp_Medium_Threat.Path_Traversal
- CSharp.CSharp_Medium_Threat.Persistent_Connection_String
- CSharp.CSharp_Medium_Threat.Privacy_Violation
- CSharp.CSharp_Medium_Threat.ReDoS_By_Regex_Injection
- CSharp.CSharp_Medium_Threat.ReDoS_In_Code
- CSharp.CSharp_Medium_Threat.Reflected_XSS_Specific_Clients
- CSharp.CSharp_Medium_Threat.Session_Fixation
- CSharp.CSharp_Medium_Threat.SQL_Injection_Evasion_Attack
- CSharp.CSharp_Medium_Threat.Stored_Command_Injection
- CSharp.CSharp_Medium_Threat.Stored_LDAP_Injection
- CSharp.CSharp_Medium_Threat.Stored_XPath_Injection
- CSharp.CSharp_Medium_Threat.Trust_Boundary_Violation
- CSharp.CSharp_Medium_Threat.Unsafe_Object_Binding
- CSharp.CSharp_Medium_Threat.Use_of_Hard_coded_Cryptographic_Key
- CSharp.CSharp_Medium_Threat.XSRF
- CSharp.CSharp_Low_Visibility.Blind_SQL_Injections
- CSharp.CSharp_Low_Visibility.Cleansing_Canonicalization_and_Comparison_Errors
- CSharp.CSharp_Low_Visibility.Dangerous_File_Upload
- CSharp.CSharp_Low_Visibility.Impersonation_Issue
- CSharp.CSharp_Low_Visibility.Improper_Exception_Handling
- CSharp.CSharp_Low_Visibility.Information_Exposure_Through_an_Error_Message
- CSharp.CSharp_Low_Visibility.Insufficiently_Protected_Credentials
- CSharp.CSharp_Low_Visibility.JavaScript_Hijacking
- CSharp.CSharp_Low_Visibility.Leaving_Temporary_Files
- CSharp.CSharp_Low_Visibility.Log_Forging
- CSharp.CSharp_Low_Visibility.Open_Redirect
- CSharp.CSharp_Low_Visibility.Potential_ReDoS
- CSharp.CSharp_Low_Visibility.Potential_ReDoS_By_Injection
- CSharp.CSharp_Low_Visibility.Potential_ReDoS_In_Code
- CSharp.CSharp_Low_Visibility.Potential_ReDoS_In_Static_Field
- CSharp.CSharp_Low_Visibility.Stored_Code_Injection
- CSharp.CSharp_Low_Visibility.Thread_Safety_Issue
- CSharp.CSharp_Low_Visibility.Use_of_RSA_Algorithm_without_OAEP
- CSharp.CSharp_Low_Visibility.XSS_Evasion_Attack
- CSharp.CSharp_Windows_Phone.Client_Side_Injection
- CSharp.CSharp_Windows_Phone.Insecure_Data_Storage
- CSharp.CSharp_Windows_Phone.Poor_Authorization_and_Authentication

本コンテンツパックによって、以下のクエリが変更されます

- CSharp_High_Risk.Code_Injection.cxq
- CSharp_High_Risk.Connection_String_Injection.cxq

- CSharp_High_Risk.Deserialization_of_Untrusted_Data_MSMQ.cxq
- CSharp_High_Risk.Resource_Injection.cxq
- CSharp_High_Risk.Second_Order_SQL_Injection.cxq
- CSharp_High_Risk.Stored_XSS.cxq
- CSharp_High_Risk.XPath_Injection.cxq
- CSharp_Low_Visibility.Improper_Exception_Handling.cxq
- CSharp_Low_Visibility.Stored_Code_Injection.cxq
- CSharp_Medium_Threat.DB_Parameter_Tampering.cxq
- CSharp_Medium_Threat.DoS_by_Sleep.cxq
- CSharp_Medium_Threat.Hardcoded_password_in_Connection_String.cxq
- CSharp_Medium_Threat.Heap_Inspection.cxq
- CSharp_Medium_Threat.SQL_Injection_Evasion_Attack.cxq
- CSharp_Medium_Threat.Stored_XPath_Injection.cxq
- CSharp_Medium_Threat.Trust_Boundary_Violation.cxq
- CSharp_Medium_Threat.Use_of_Hard_coded_Cryptographic_Key.cxq
- General.Find_ASP_MVC_Controllers.cxq
- General.Find_ASP_MVC_Outputs.cxq
- General.Find_ASP_MVC_XSRF.cxq
- General.Find_CollectionAccesses.cxq
- General.Find_Command_Injection_Sanitize.cxq
- General.Find_Connection_String.cxq
- General.Find_Connection_String_Sanitize.cxq
- General.Find_DB_Command_DataSource_QSqlQuery.cxq
- General.Find_DB_Command_ExecuteNonQuery.cxq
- General.Find_DB_EF_In.cxq
- General.Find_DB_Entlib_Execute.cxq
- General.Find_DB_Ibatis.cxq
- General.Find_DB_Linq_Full.cxq
- General.Find_DB_Out.cxq
- General.Find_DB_Salesforce.cxq
- General.Find_DB_Sqlite_Xamarin.cxq
- General.Find_Deserialization_Sanitizers.cxq
- General.Find_FileSystem_Read.cxq
- General.Find_Hashing_Functions.cxq
- General.Find_Inherited_Classes.cxq
- General.Find_Insecure_Hash.cxq
- General.Find_Integers.cxq
- General.Find_Interactive_Inputs.cxq
- General.Find_Match.cxq
- General.Find_ReDoS.cxq
- General.Find_Read.cxq
- General.Find_Regex.cxq
- General.Find_Regex_Safe_Arguments.cxq
- General.Find_Replace.cxq

- General.Find_Request.cxq
- General.Find_SQL_Sanitize.cxq
- General.Find_Sanitize.cxq
- General.Find_Secure_Hash.cxq
- General.Find_Stored_Inputs.cxq
- General.Find_Unsafe_DeserializeObject.cxq
- General.Find_Unsafe_Deserializers.cxq
- General.Find_Unsafe_Implementation_of_SerializationBinder.cxq
- General.Find_XPath_Injection_Sanitizers.cxq
- General.Find_XPath_Output.cxq
- General.Find_XSS_Outputs.cxq
- General.Get_Controller_Of_View.cxq
- General.Get_Rightmost_Members_From_References.cxq
- Common_High_Risk.Deserialization_of_Untrusted_Data.cxq