[2018-04-04] Change Log

New version of CQM (v1.2.15) and Kiuwan Engine

A new Kiuwan's CQM and Engine is available.

Features of this new version are:

- New **PHP security rules** (10)
- Improved **Java** support with **new rules for Android** (7) and **support for Play Framework**
- New security rules *(2) for* **Django (Python)**
- New **ABAP** rules (17)

You can find these new rules by comparing v1.2.15 of CQM against previous version.

A detailed description of the behavior of these new rules is available in rule's description.

Unless you have blocked Kiuwan Engine, **Kiuwan Local Analyzer will automatically upgrade it to the last version once a new analysis is run**.

In order for these new rules be applicable, your Kiuwan account must be configured to allow automatic engine upgrade:

- If you are using *CQM*, these new rules will *automatically become active* and will be applied to new analyses.
- If you are using your own *custom model*, *you can activate them* in case you want to be applied to your code.

New PHP Security Rules

- OPT.PHP.SEC.PlaintextStorageInACookieRule
- OPT.PHP.SEC.InsufficientSessionExpirationRule
- OPT.PHP.SEC.CookiesInSecurityDecision
- OPT.PHP.SEC.CrossSiteHistoryManipulation
- OPT.PHP.SEC.InsufficientKeySizeRule
- OPT.PHP.SEC.TrustBoundaryViolationRule
- OPT.PHP.SEC.UncheckedInputInLoopCondition
- OPT.PHP.SEC.ImproperValidationOfArrayIndex
- OPT.PHP.SEC.UserControlledSQLPrimaryKey
- OPT.PHP.SEC.PotentialInfiniteLoop

Improved Java support (Android and Play Framework)

Android support has been improved with the addition of new rules:

- OPT.JAVA.ANDROID.ReceiverWithoutPermission
- OPT.JAVA.ANDROID.PrivilegeEscalationAttack
- OPT.JAVA.ANDROID.ExportedProvider
- OPT.JAVA.ANDROID.ExportedActivity
- OPT.JAVA.ANDROID.CheckLocationPermission
- OPT.JAVA.ANDROID.CheckInternetPermission
- OPT.JAVA.ANDROID.CheckExternalStoragePermission

Also, support for **Play Framework** (OPT.JAVA.SEC_JAVA.PlaySecurityMisconfiguration) has been added to Kiuwan.

Enhanced Django Python support

Existing security rules for Django framework have been enhanced by supporting new sinks/sources as well as improvements in tainting propagation.

Besides, 2 new security rules have added to current Django set:

- OPT.PYTHON.SECURITY.MemcachedInjection
- OPT.PYTHON.SECURITY.InformationExposureThroughDebugLog

You can find Django rules by filtering by "Django" Framework in CQM model.

New ABAP Rules

- OPT.ABAP.SEC.UsagesOfSyUname
- OPT.ABAP.SEC.UsagesOfSySysid
- OPT.ABAP.SEC.RfcDestinationInjection
- OPT.ABAP.SEC.RfcCallbackAttack
- OPT.ABAP.SEC.NoAuthorizationGroup4Table
- OPT.ABAP.SEC.HardcodedUsernameCheck
- OPT.ABAP.SEC.DangerousFileUpload
- OPT.ABAP.SEC.DangerousFileDownload
- OPT.ABAP.SEC.Calls2CriticalFunctions
- OPT.ABAP.SEC.AuthorityChecks
- OPT.ABAP.RELIABILITY.UncaughtExceptionInRfcCall
- OPT.ABAP.RELIABILITY.ModifiedInputParameter
- OPT.ABAP.RELIABILITY.LogicDependingOnTextSymbols
- OPT.ABAP.RELIABILITY.DirectRecursiveCall
- OPT.ABAP.PORTABILITY.DeprecatedAsyncronousRFC
- OPT.ABAP.EFFICIENCY.LoopAtInto
- OPT.ABAP.EFFICIENCY.JoinInsteadOfSelectInLoop