[2017-06-27] Change Log

CQM (v1.2.9) and Kiuwan Engine (master.p453.q7002)

A new Kiuwan's CQM version (v.1.2.9) is available.

Basically, v1.2.9 contains ***new rules for Python and Javascript (node.js)***.

These new rules are available in new CQM together with **new Kiuwan Engine (master.p453.q7002)**.

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

Please remember that you can also find new rules by comparing v1.2.9 of CQM against previous versions.

New Python Rules

Support to **Python** (our last supported technology) is being improved by adding new rules to the current set (95).

This new release of Kiuwan adds **24 new rules** :

- OPT.PYTHON.PORTABILITY.HardcodedAbsolutePath : Improper control of resource identifiers ("Resource Injection")
- OPT.PYTHON.SECURITY.ConnectionStringParameterPollution : Connection string polluted with untrusted input
- OPT.PYTHON.SECURITY.CookiePoisoning : Cookie Poisoning
- OPT.PYTHON.SECURITY.CrossSiteRequestForgery : Cross-site request forgery (CSRF)
- OPT.PYTHON.SECURITY.CrossSiteScripting : Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- OPT.PYTHON.SECURITY.DoSRegexp Potential denial-of-service attack through malicious regular expression (ReDoS)
- OPT.PYTHON.SECURITY.HardcodedCredential : Empty or hardcoded passwords may compromise system security in a way that cannot be easily remedied
- OPT.PYTHON.SECURITY.InsecureRandomness : Standard pseudo-random number generators cannot withstand cryptographic attacks
- OPT.PYTHON.SECURITY.InsecureTransport : Insecure transport
- OPT.PYTHON.SECURITY.MailCommandInjection : Mail Command Injection
- OPT.PYTHON.SECURITY.PasswordInComments : Storing passwords or password details in plaintext anywhere in the system or system code can compromise system security
- OPT.PYTHON.SECURITY.ResourceInjection : Improper control of resource identifiers ("Resource Injection")
- OPT.PYTHON.SECURITY.ServerInsecureTransport : Insecure transport in Node.js HTTP servers
- OPT.PYTHON.SECURITY.ServerSideRequestForgery : Creation of requests from a vulnerable server using untrusted input (server side request forgery, SSRF)
- OPT.PYTHON.SECURITY.StoredCrossSiteScripting : Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- OPT.PYTHON.SECURITY.UnsafeCookie : Generate server-side cookies with adequate security properties
- OPT.PYTHON.SECURITY.WeakCryptographicHash : Weak cryptographic hash
- OPT.PYTHON.SECURITY.WeakEncryptionAlgorithm : Weak symmetric encryption algorithm
- OPT.PYTHON.DJANGO.CookieBasedSessions : Cookie-based session with a unsafe configuration
- OPT.PYTHON.DJANGO.InsecureDirectObjectReferences : Check for user authentication and/ or authorization before let him modifying a sensible system resource
- OPT.PYTHON.DJANGO.MassAssigmentAttack : Insufficient form fields validation
- OPT.PYTHON.DJANGO.MissingBrowserXssFilter : Secure browser XSS filter
- OPT.PYTHON.DJANGO.MissingFunctionLevelAccessControl : Perform an authorization check when performing an action which requires authorization
- OPT.PYTHON.DJANGO.WeakCryptographicHashInSettings : Weak cryptographic hashes cannot guarantee data integrity

New JavaScript (Node.js) Rules

Support to JavaScript is also being improved by adding new rules to the current set (150).

This new release of Kiuwan adds **25 new rules**:

- OPT.JAVASCRIPT.ANGULARJS.ContextualEscapingDisabled : Strict Contextual Escaping (SCE) disabled
- OPT.JAVASCRIPT.ANGULARJS.UnsafeUrlWhitelist : Unsafe URL whitelist
- OPT.JAVASCRIPT.AvoidArguments : Do not use arguments object
- OPT.JAVASCRIPT.AvoidWebSQL : Avoid Web SQL

- OPT.JAVASCRIPT.ClickjackingProtection : No clickjacking protection configured
- OPT.JAVASCRIPT.ClientSideTemplateInjection : Client-side Template Injection
- OPT.JAVASCRIPT.CommandInjection : Avoid non-neutralized user-controlled input to be part of an OS command
- OPT.JAVASCRIPT.ConnectionStringParameterPollution : Connection string polluted with untrusted input
- OPT.JAVASCRIPT.CookiePoisoning : Cookie Poisoning
- OPT.JAVASCRIPT.DoSRegexp : Potential denial-of-service attack through malicious regular expression (ReDoS)
- OPT.JAVASCRIPT.ExternalControlOfConfigurationSetting : External Control of System or Configuration Setting
- OPT.JAVASCRIPT.HardcodedCryptoKey : Hardcoded cryptographic keys
- OPT.JAVASCRIPT.HidePoweredByHeader : Deactivate X-Powered-By header
- OPT.JAVASCRIPT.ImproperCertificateValidation : Improper Certificate Validation
- OPT.JAVASCRIPT.InsecureTransport : Insecure transport
- OPT.JAVASCRIPT.NoSQLInjection : Improper neutralization of special elements in data query logic (NoSQL injection)
- OPT.JAVASCRIPT.OpenRedirectHanaXS : Open Redirect (HANA XS)
- OPT.JAVASCRIPT.PreventMIMESniffing : Prevent MIME sniffing
- OPT.JAVASCRIPT.ServerInsecureTransport : Insecure transport in Node.js HTTP servers
- OPT.JAVASCRIPT.ServerSideRequestForgery : Creation of requests from a vulnerable server using untrusted input (server side request forgery, SSRF)
- OPT.JAVASCRIPT.ServerSideTemplateInjection : Server-side Template Injection
- OPT.JAVASCRIPT.StoredCrossSiteScripting : Improper neutralization of input during web content generation (Cross-site Scripting, XSS)
- OPT.JAVASCRIPT.UnsafeCookie : Generate server-side cookies with adequate security properties
- OPT.JAVASCRIPT.UseStrictTransportSecurity : Use HTTP Strict Transport Security
- OPT.JAVASCRIPT.XssProtectionDisabled : Cross-site scripting protection disabled

Rules renaming to match CWE identifiers

With the aim of normalization with CWE, many Kiuwan rules have been renamed to match CWE identifiers, as well as to unify rule nomenclature between different technologies.

This will make easier to understand the meaning of the rule as well as to find associated CWE identifiers.

Moreover, Kiuwan rules have been exhaustively reviewed to fully match their corresponding CWE identifier.

This renaming is completeley transparent to previous analyses (the Kiuwan internal code remains unchanged), although you could find a different name for a rule due to these changes.

Improvements in Kiuwan Engine (master.p453.q7002)

New Kiuwan engine contains enhanced versions of parsers and rules:

- Enhancements in JSP, PL_SQL, JS and Cobol parsers
- Cobol, Java and Obj-C rules documentation improvements
- Bug fixing, performance and reliability issues in C#, HTML, JS, Cobol, ASP.NET, PYTHON and Java rules

New searching criteria for Defects and Rules

Kiuwan ruleset is becoming larger, as we add new rules.

That’s OK for analytics purposes, but searching and browsing over the whole set of rules is becoming an important feature.

In this sense, we have added some **new searching criteria to Defects and Rules pages**:

- **Normative**
- **Framework**

You can use them right now to better search for specific rules and defects.

Normatives

You can filter now your defects or your model’s rules using the new search “Normative” field.

You could select one or various values among the most common and broadly accepted security and quality normatives : CWE, OWASP, CERT-Java/C /C++, SANS-Top25, WASC, PCI-DSS, NIST, MISRA, BIZEC, etc.

Framework

Same way as with Normatives, you can filter now your defects or your model’s rules using the new search “Framework” field.

You could select one or various values among the most common and broadly used programming frameworks : Android, AngularJS, CakePHP, Hibernate, JAX, JAX-RS, JAX-WS, jsf, Node.js, Spring, Spring-Batch, Spring-Boot, Spring-Core, Spring-Data, Spring-Data-REST, Spring-MVC, struts1, struts2, Symfony, Zend.

Enhanced Calendar behavior

Kiuwan’s Calendar behavior has been improved to better satisfy your filtering needs:

- FROM and TO dates are both now being considered (formerly, only TO date was being used to filter analyses data)
- If no analyses are found within the selected date range, a warning page is displayed, and you are presented the option to load all the analyses of the current application.
- If you select a date range that leaves out the newest analyses of your application, a warning will inform you (preventing you to forget you have selected a date range not displaying data for the newest analyses of your application).