Code Quality Java

Spring AU 2021

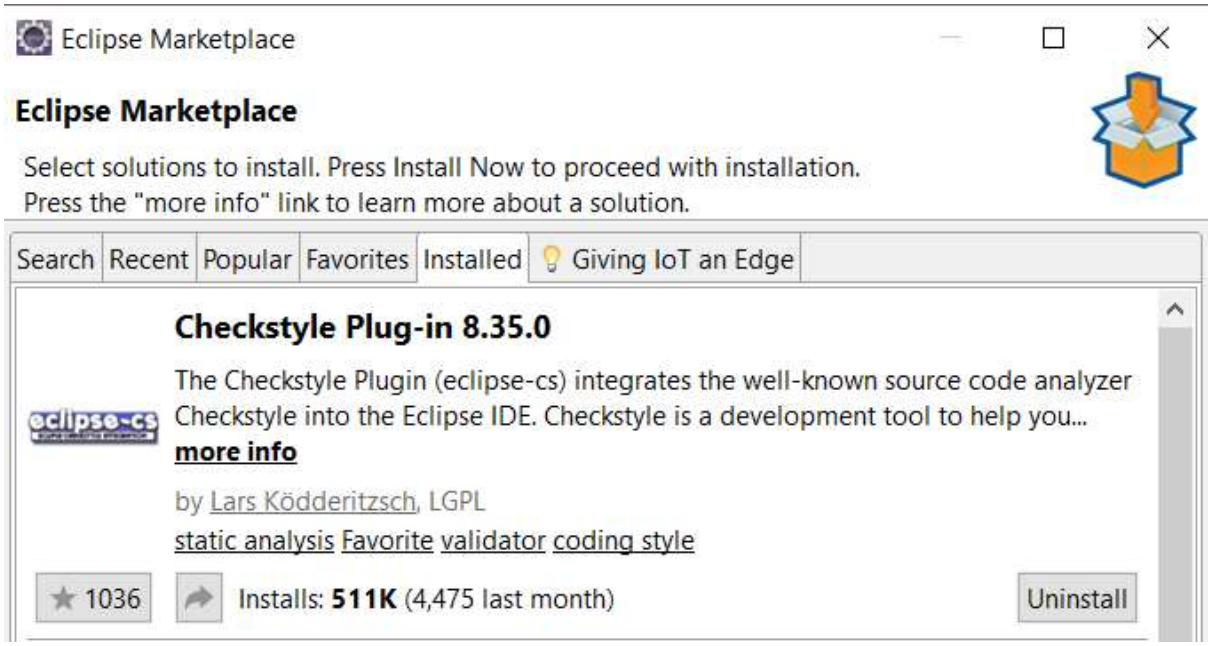
Archit Somayajula archit.somayajula@accolitedigital.com

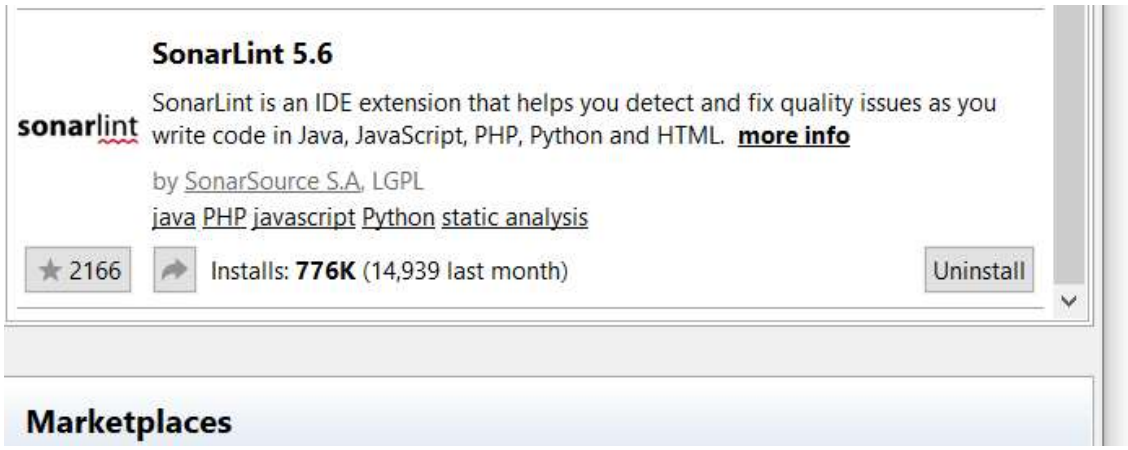
---

1. Code Quality Plugins

IDE: Eclipse

Plugin installation marketplace





Eclipse Marketplace

Eclipse Marketplace

ⓘ One solution selected for install

Search | Recent | Popular | Favorites | Installed | Giving IoT an Edge

Find: pmd | All Markets | All Categories | Go

eclipse-pmd 2.4.2

The eclipse-pmd plug-in integrates the source code analyzer PMD into the Eclipse IDE. Everytime you save your work, eclipse-pmd scans your source code and looks... **more info**

by Philip Graf, EPL

PMD Static Code Analysis code analyzer code quality

★ 280 | Installs: **182K** (722 last month) | **Install**

pmd-eclipse-plugin 4.20.0

PMD is a source code analyzer. It finds common programming flaws like unused variables, empty catch blocks, unnecessary object creation, and so forth. It supports... **more info**

by PMD, BSD

PMD linter Source Code Analyzer code quality java

★ 114 | Installs: **50.9K** (1,450 last month) | *Install Pending*

SWAMP Eclipse Plug-in

The SWAMP Eclipse Plug-in allows users to easily run static analysis tools available

One solution selected | Deselect all

Marketplaces

Configuring provisioning operation: Fetching compositeContent.xml from https://dl.bintray.com/pmd/

< Back | Install Now > | Finish | Cancel

Sonarlint Report

Problems | Javadoc | Declaration | Console | JUnit | SonarLint Report

0 items

Resource	Date	Description

Checkstyle Report

Problems | Javadoc | Declaration | Console | JUnit | Checkstyle violations

Overview of Checkstyle violations - 395 markers in 15 categories (filter matched 395 of 395 items)

Checkstyle violation type	Occurrences
'X' is not preceded with whitespace.	16
Wrong lexicographical order for 'X' import. Should be be...	24
'X' should be separated from previous statement.	16
Using the '.*' form of import should be avoided - X.	2
Line is longer than X characters (found X).	7
'X' child has incorrect indentation level X, expected level ...	92
'X' construct must use '{}'s.	1
'X' has incorrect indentation level X, expected level shoul...	76
'X' is not followed by whitespace.	23
'X' at column X should have line break before.	1
Abbreviation in name 'X' must contain no more than 'X' c...	3
Line contains a tab character.	126
Extra separation in import group before 'X'	5
Missing a Javadoc comment.	2
Import statement for 'X' is in the wrong order. Should be ...	1

PMD Report

Violations Overview

Element	# Violations	# Violations...	# Violations...	Project
com.asr.main.controller	1	19.6	0.25	SpringMVC
EmployeeControllerTest.java	1	19.6	0.25	SpringMVC
UnusedImports	1	19.6	0.25	SpringMVC
com.asr.main.model	9	250.0	1.50	SpringMVC
EmployeeTest.java	9	250.0	1.50	SpringMVC
UnnecessaryFullyQualifiedI	5	138.9	0.83	SpringMVC
UnusedImports	4	111.1	0.67	SpringMVC
com.asr.main.service	1	40.0	0.50	SpringMVC
EmployeeServiceImplTest.java	1	40.0	0.50	SpringMVC
UnusedPrivateField	1	40.0	0.50	SpringMVC
com.asr.main.service	2	181.8	0.50	SpringMVC
EmployeeService.java	2	1000.0	1.00	SpringMVC
UnnecessaryModifier	2	1000.0	1.00	SpringMVC

2. Secure coding standards

a. CWE - Common Weakness Enumeration

It's a list of common software and hardware security weakness.

2020 Top few CWE list

- Cross-site scripting
- SQL injection
- Cross-site Request Forgery
- Improper Authentication
- Null Pointer dereference

b. OWASP top 10

The Open Web Application Security Project

A community which provides documentation and tools for web app security

Few of the top OWASP security risks

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities
- Broken Access Control

c. CERT

A secure coding standard with a risk assessment for violations

Aims to provide security and code quality

CERT Risk assessment

Each has a value between 1 - 3

1 - lowest

1. Severity
2. Likelihood
3. Remediation cost

The above 3 are grouped together to determine the level of Vulnerability

Level	Priorities	Interpretation
L1	**12, 18, 27**	**Severity: High Severity** **Likelihood: Likely** **Remediation Cost: Inexpensive to Repair**
L2	**6, 8, 9**	**Severity: Medium Severity** **Likelihood: Probable** **Remediation Cost: Medium Cost to Repair**
L3	**1, 2, 3, 4**	**Severity: Low Severity** **Likelihood: Unlikely** **Remediation Cost: Expensive to Repair**

Sonarqube Report