Calidad Estatica con Sonar

Victor Herrero Cazurro

Contenidos

1. Calidad estática del código

1.1. Calidad del Código

Decimos que un código tiene calidad, cuando tenemos facilidad de mantenimiento y de desarrollo.

¿Como podemos hacer que nuestro código tenga mas calidad? Consiguiendo que nuestro código no tenga partes que hagan que:

- Se reduzca el rendimiento.
- Se provoquen errores en el software.
- Se compliquen los flujos de datos.
- Lo hagan mas complejo.
- Supongan un problema en la seguridad.

Tendremos dos técnicas para mejorar el código fuente de nuestra aplicación y, con ello, el software que utilizan los usuarios como producto final:

- Test. Son una serie de procesos que permiten verificar y comprobar que el software cumple con los objetivos y con las exigencias para las que fue creado.
- Análisis estático del código. Proceso de evaluar el software sin ejecutarlo.

1.2. Análisis Estático del Código

Es una técnica que se aplica directamente sobre el código fuente tal cual, sin transformaciones previas ni cambios de ningún tipo.

La idea es que, en base a ese código fuente, podamos obtener información que nos permita mejorar la base de código manteniendo la semántica original.

Esta información nos vendrá dada en forma de sugerencias para mejorar el código.

Emplearemos herramientas que incluyen

- Analizadores léxicos y sintácticos que procesan el código fuente.
- Conjunto de reglas que aplicar sobre determinadas estructuras.

Si nuestro código fuente posee una estructura concreta que el analizador considere

como "mejorable" en base a sus reglas nos lo indicará y nos sugerirá una mejora.

Se deberian realizar análisis estáticos del código cada vez que se crea una nueva funcionalidad, así como cuando el desarrollo se complica, nos cuesta implementar algo que supuestamente debe ser sencillo.

1.3. PMD

Detecta patrones de posibles errores que pueden aparecer en tiempo de ejecución, por ejemplo

- Código que no se puede ejecutar nunca porque no hay manera de llegar a él.
- Código que puede ser optimizado.
- Expresiones lógicas que puedan ser simplificadas.
- Malos usos del lenguaje, etc
- Tambien incluye detección de CopyPaste (CPD)

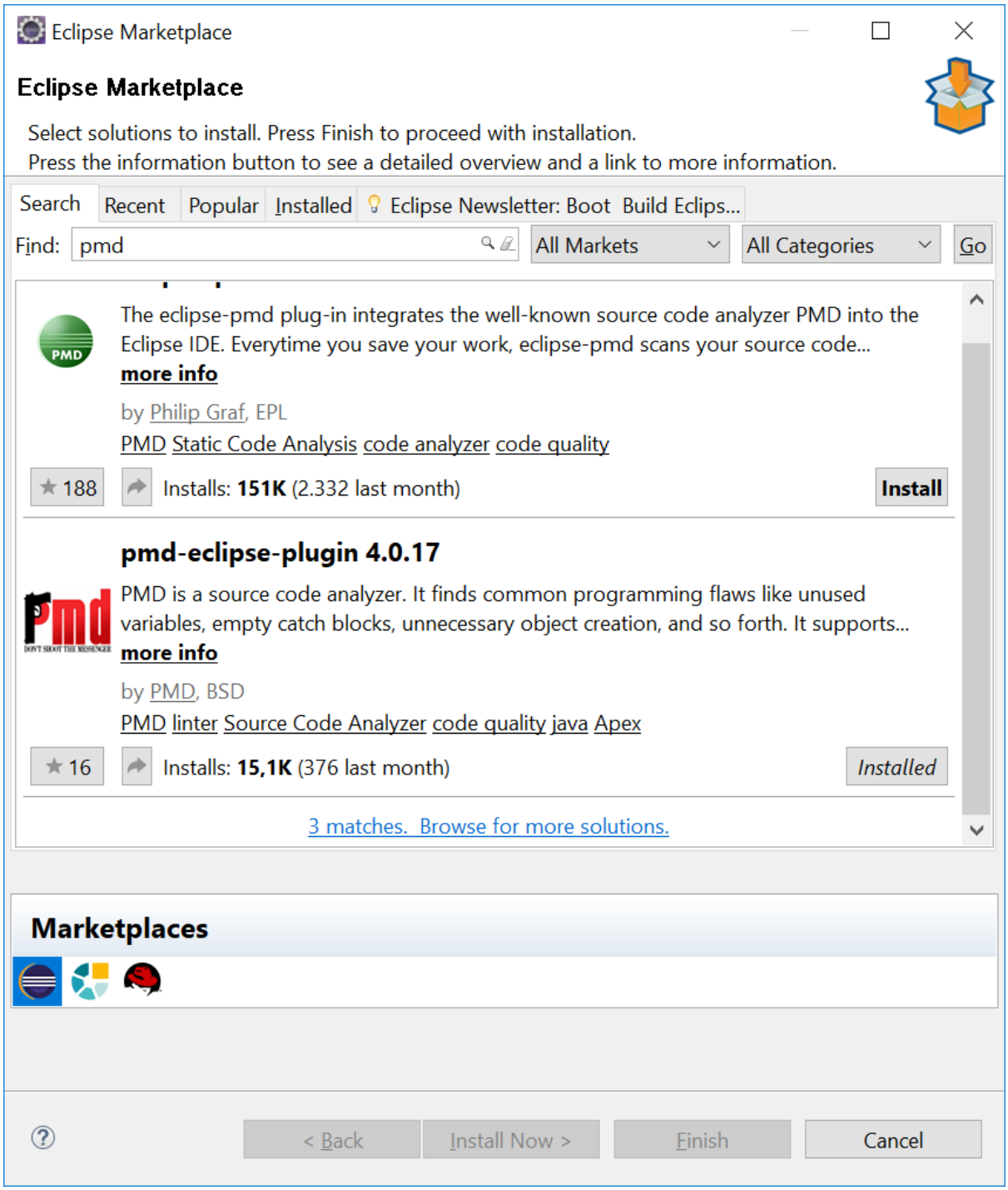
La pagina de referencia aquí

Los patrones que se emplean se encuentran catalogados en distintas categorías, se pueden consultar aquí

Se pueden añadir nuevas reglas o configurar las que ya se incluyen en caso de que esto fuera necesario.

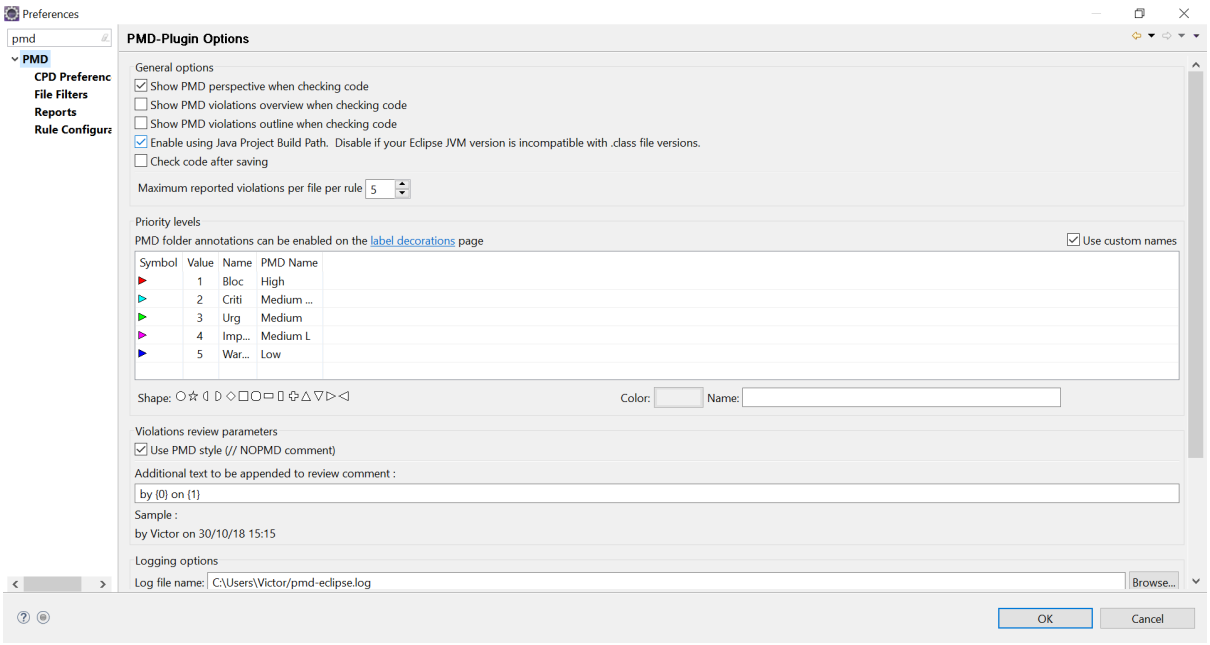
1.3.1. Plugin de Eclipse

Se puede descargar desde el Market de eclipse.



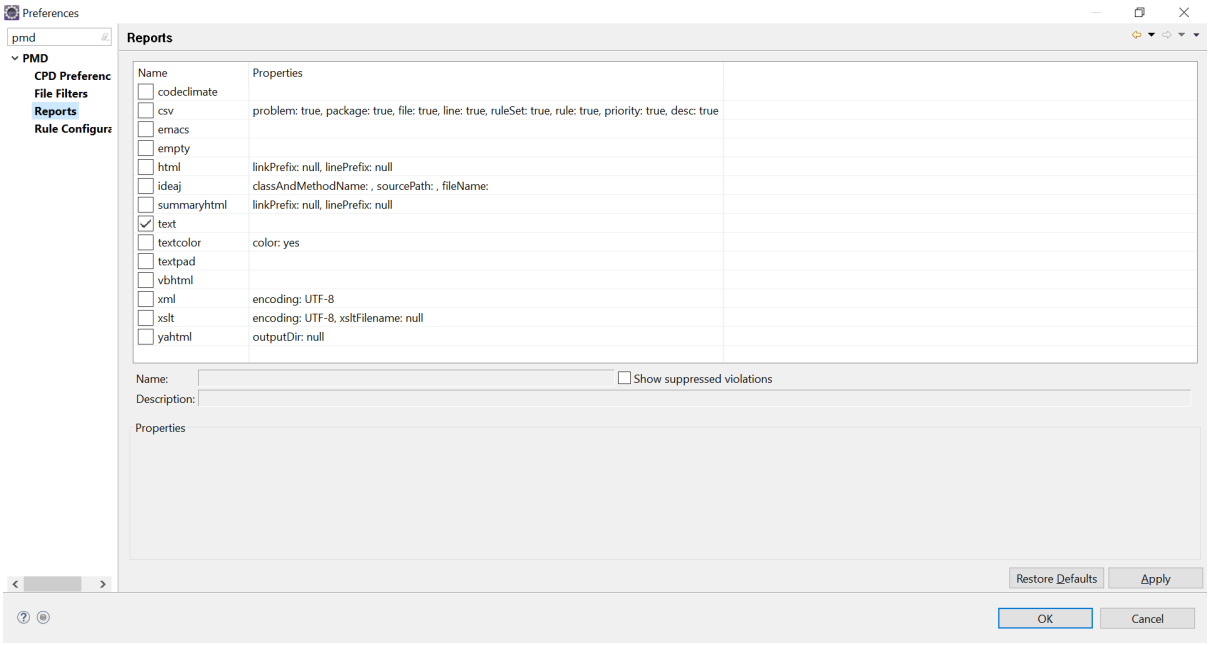
Permite configurar desde **Window - Preferences**:

- La infromacion a mostrar cuando se realiza el analisis.
- Los estilos de pintado de los mensajes
- El fichero de log y el nivel de log

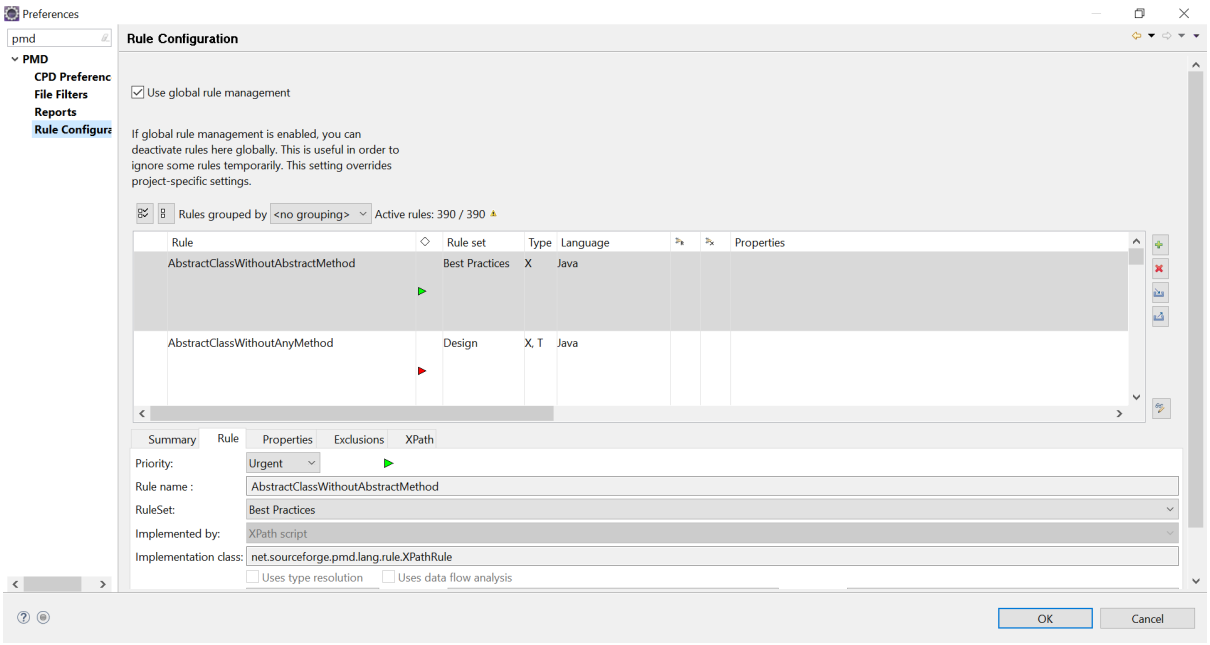


Desde esa opcion de **Window - Preference - PMD**, se tiene acceso a otras opciones como son

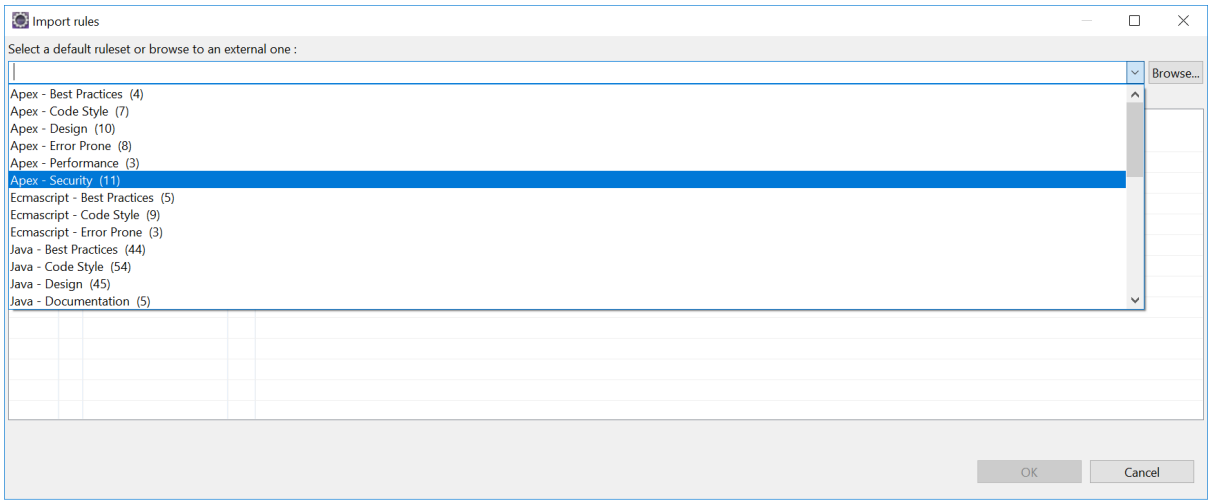
- CPD Preferences: Donde se puede configurar el tamaño del trozo de codigo repetido para considerarlo un **Copy - Paste**
- File Filter: Para filtrar los ficheros sobre los que se aplican las reglas
- Reports: Para indicar los formatos de reportes generados.



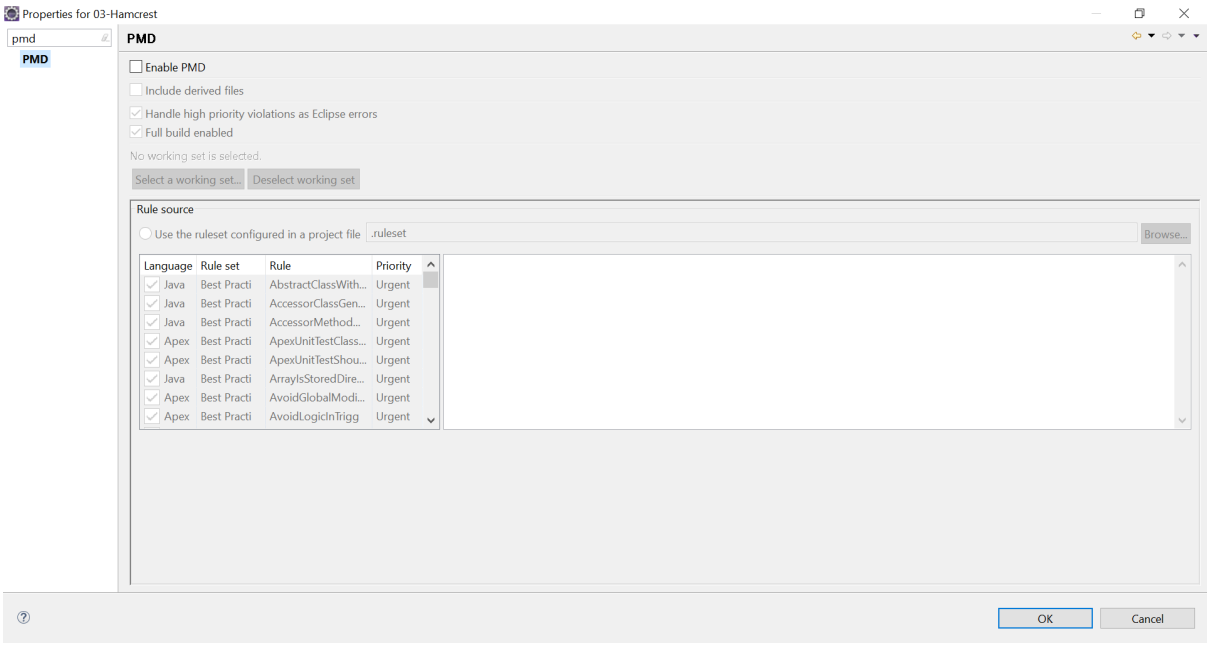
- Rule Configuration: Para configurar las reglas a aplicar de forma general.



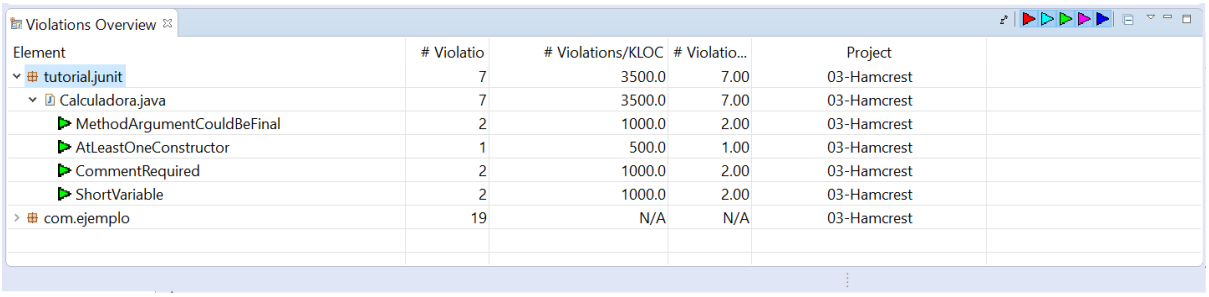
Dentro de esta opcion se pueden importar nuevas reglas.



Desde el menu de propiedades del proyecto, se pueden activar o desactivar reglas para el proyecto



Para aplicar las reglas basta con acceder al menu del proyecto seleccionando la opcion **PMD - Check Code**, obteniendo los resultados en la vista **Violations Overview**.



Tambien se pueden generar **reports** con la opcion **PMD - Generate reports**, que generará todos los reportes seleccionados en la capeta **reports** del proyecto.

1.3.2. Plugin de Maven

Se dipone de un plugin de Maven para la generacion de reportes

```
<reporting>
    <plugins>
        <plugin>
            <groupId>org.apache.maven.plugins</groupId>
            <artifactId>maven-pmd-plugin</artifactId>
            <version>3.6</version>
            <configuration>
                <linkXref>true</linkXref>
            </configuration>
        </plugin>
    </plugins>
</reporting>
```

Este plugin tambien puede ser configurado como plugin de la fase de Test

```
<build>
    <plugins>
        <plugin>
            <groupId>org.apache.maven.plugins</groupId>
            <artifactId>maven-pmd-plugin</artifactId>
            <version>3.6</version>
            <configuration>
                <failOnViolation>true</failOnViolation>
                <failurePriority>2</failurePriority>
                <minimumPriority>5</minimumPriority>
            </configuration>
            <executions>
                <execution>
                    <phase>test</phase>
                    <goals>
                        <goal>pmd</goal>
                        <goal>cpd</goal>
                        <goal>cpd-check</goal>
                        <goal>check</goal>
                    </goals>
                </execution>
            </executions>
        </plugin>
    </plugins>
</build>
```

Con los parametros

- **failOnViolation**: le indicamos que si hay fallos, haga que la fase de Test falle, supeditamos el exito de los Test al analisis de PMD
- **failurePriority**: le indicamos a partir de que prioridad se considera fallo, las prioridades van de 1 a 5, siendo 1 la maxima y 5 la menor, si se define por ejemplo 2, solo se consideran las reglas con prioridad 1 y 2.
- **minimumPriority**: Minima prioridad de las reglas a evaluar.

Y los goal

- **pmd**: Ejecuta las reglas de pmd
- **cpd**: Ejecuta las reglas de cpd
- **cpd-check**: Chequea los resultados de cpd
- **check**: Chequea los resultados de pmd

1.4. Checkstyle

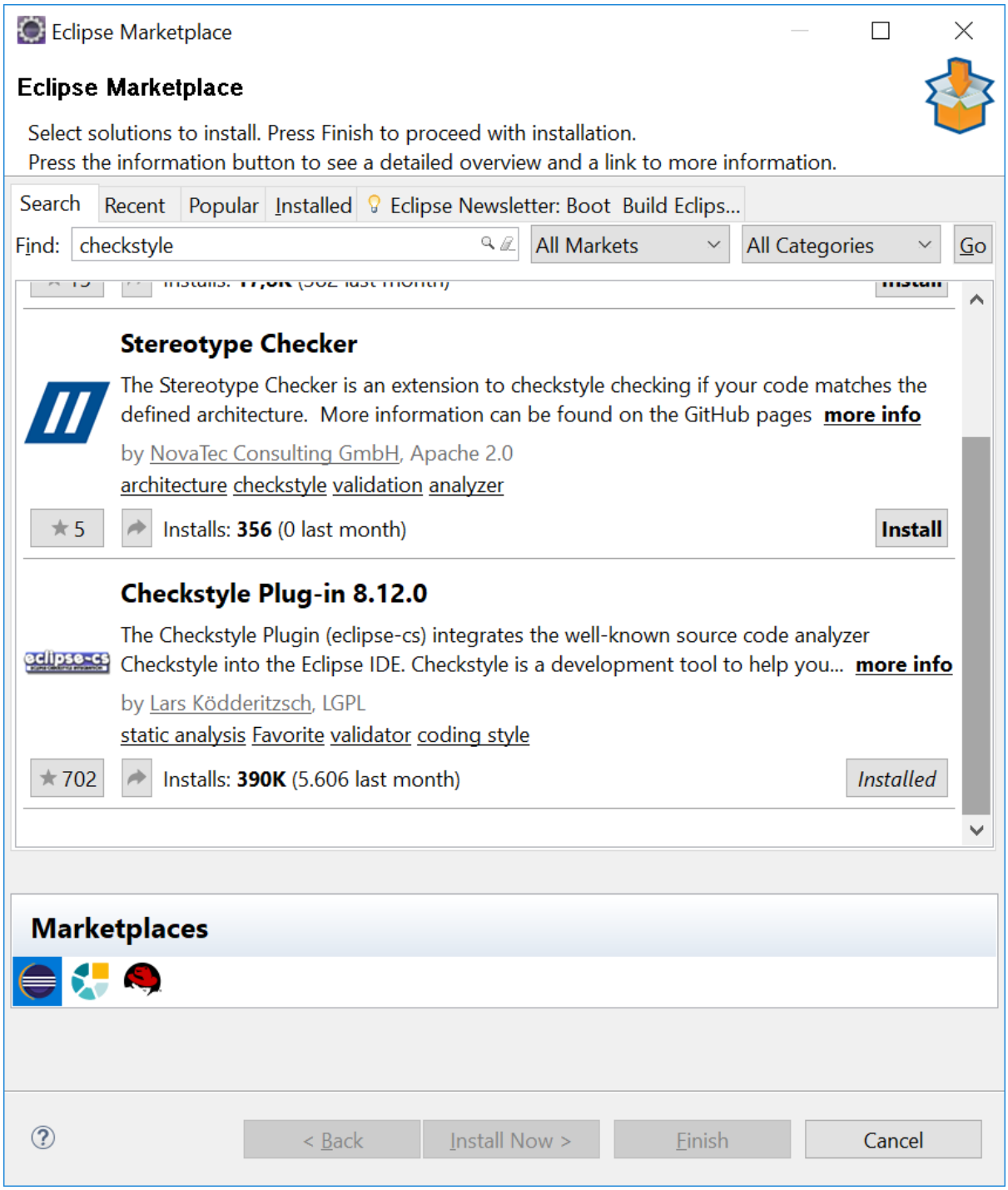
Inicialmente se desarrolló con el objetivo de crear una herramienta que permitiese comprobar que el código de las aplicaciones se ajustase a los estándares dictados por **Sun Microsystems**.

Posteriormente se añadieron nuevas capacidades que han hecho que sea un producto muy similar a PMD. Es por ello que también busca patrones en el código que se ajustan a categorías muy similares a las de este analizador.

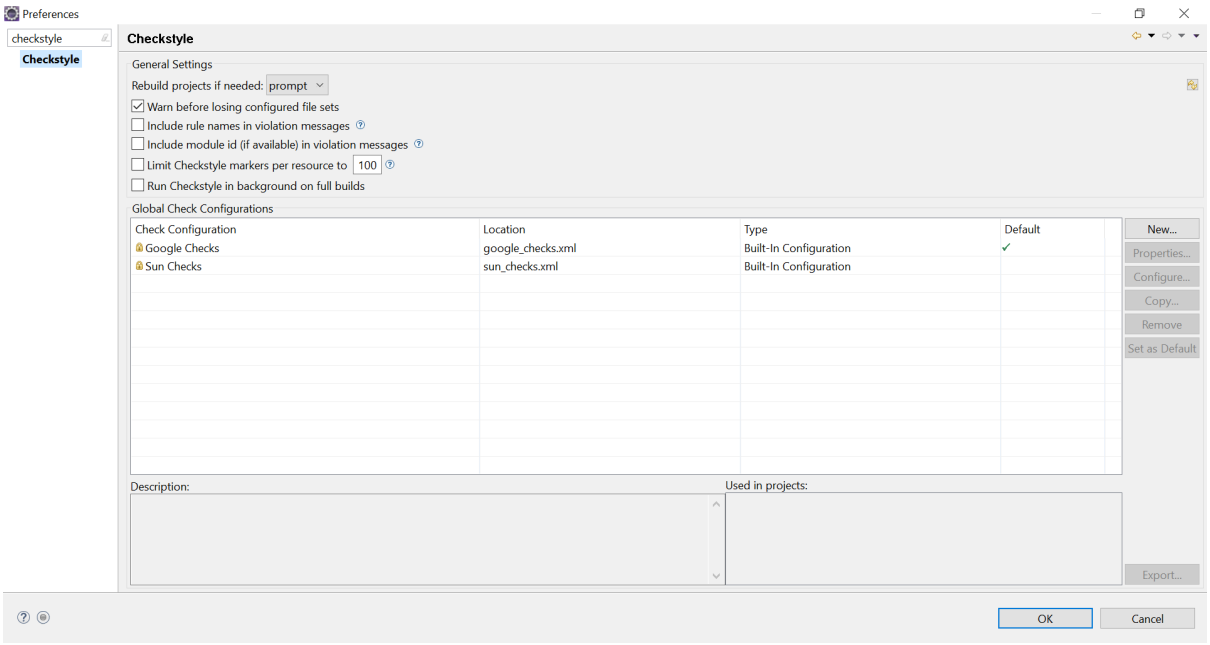
La página de referencia aquí

1.4.1. Plugin de Eclipse

Se puede descargar desde el Market de eclipse.



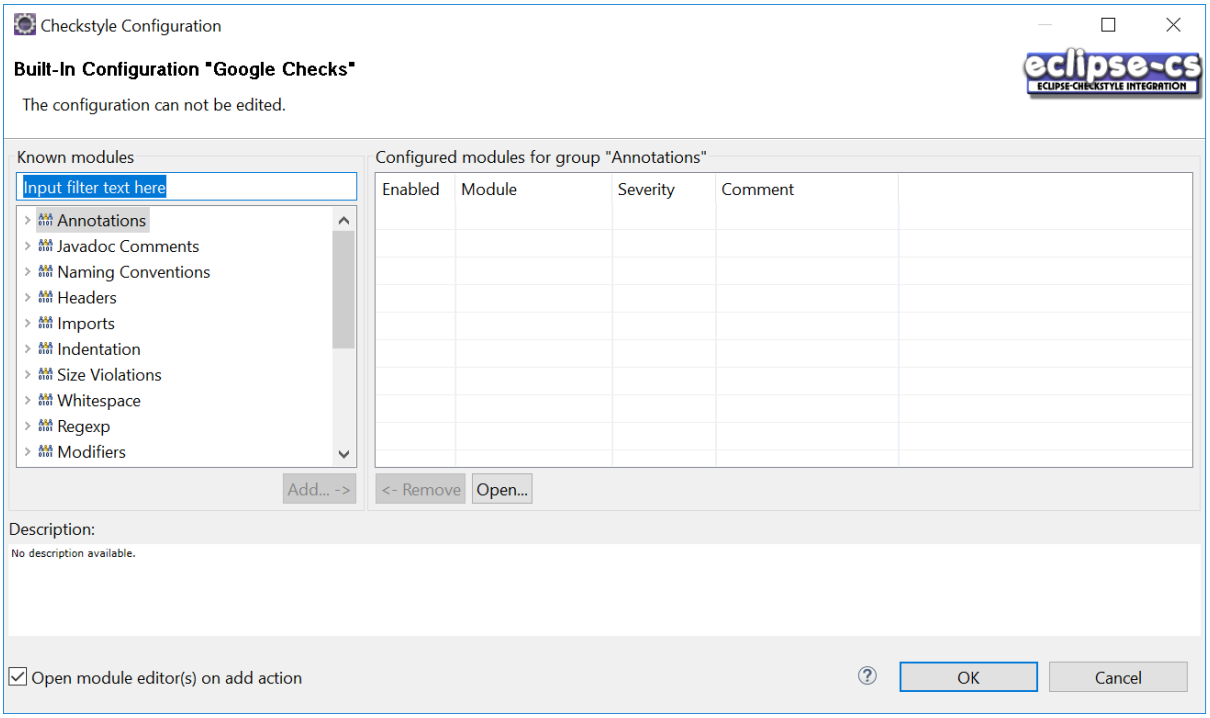
Permite configurar desde **Window - Preferences** las configuraciones de reglas disponibles para todo el workspace.



Por defecto se definen dos:

- Google checks
- Sun cheks

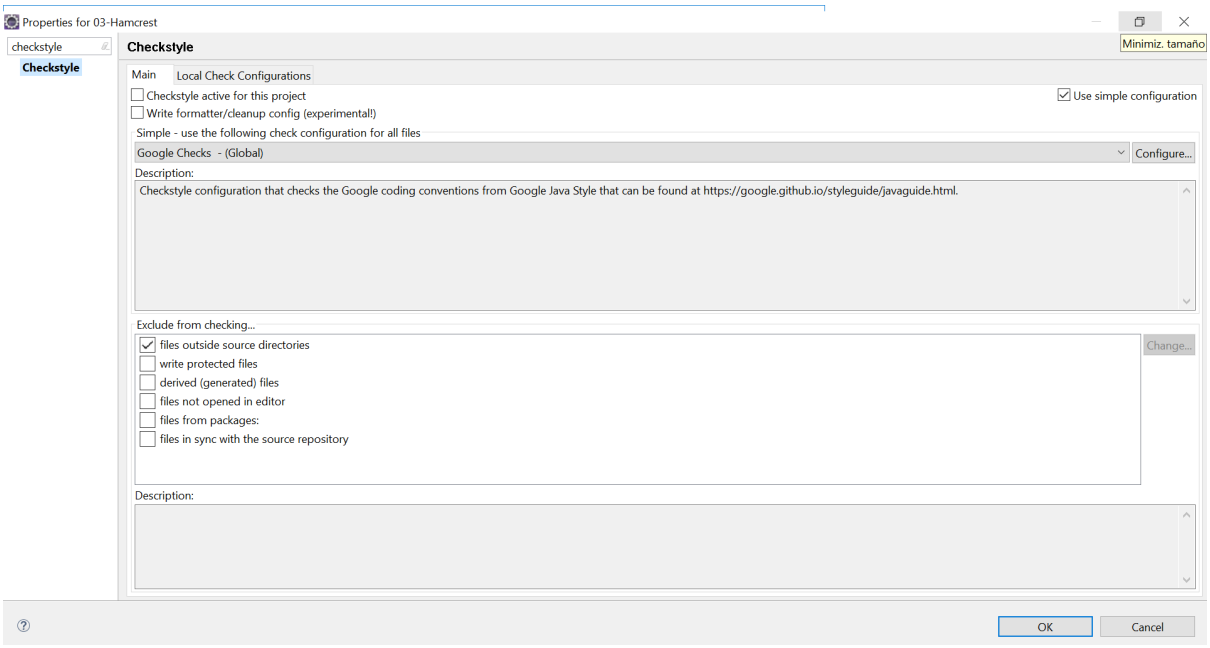
Cada una definiendo un conjunto de reglas a aplicar. Estas reglas se pueden ver desde la opcion **Configure** de la tabla donde salen listadas



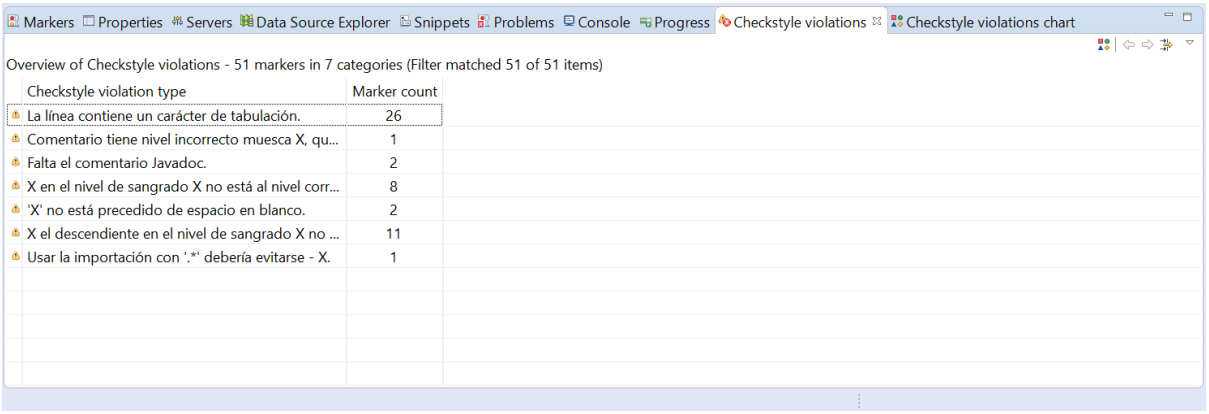
Desde el menu de propiedades del proyecto, se puede:

- Activar o desactivar el uso de checkstyle para el proyecto

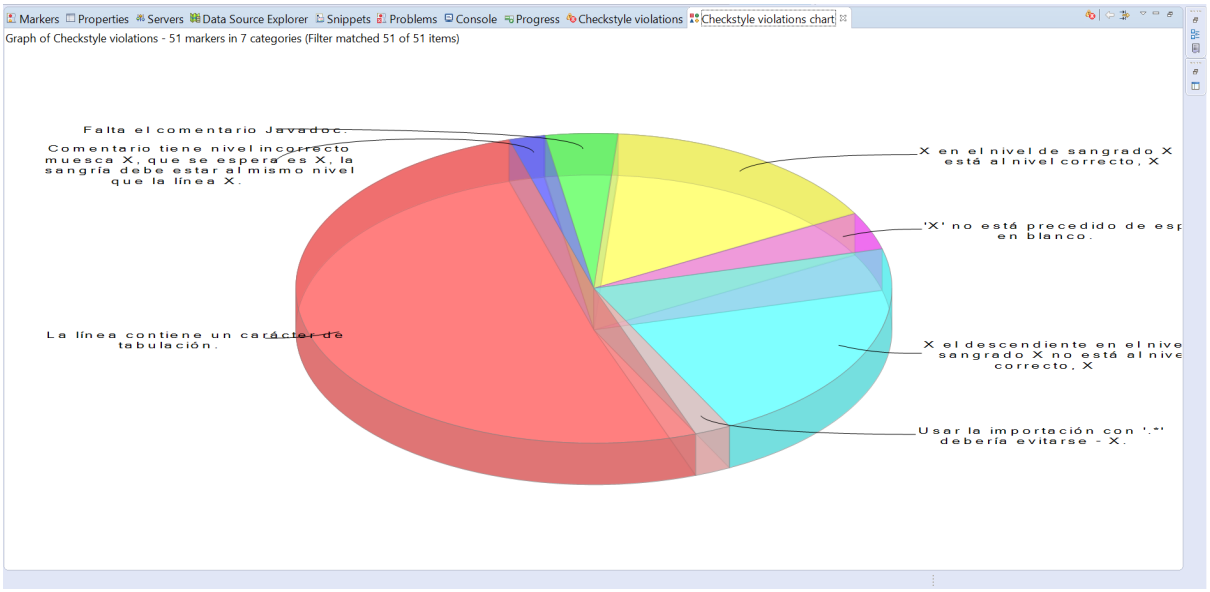
- Seleccionar el conjunto de reglas a aplicar.
- Excluir ficheros del analisis
- Añadir reglas propias del proyecto.



Para aplicar las reglas basta con acceder al menu del proyecto seleccionando la opcion **Checkstyle - Check Code with checkstyle**, obteniendo los resultados en la vista **Checkstyle Violations**, la cual hay que añadir a la perspectiva.



Tambien se dispone de una vista grafica, que muestra los resultados



1.4.2. Plugin de Maven

Dispone de un plugin de Maven

```
<reporting>
    <plugins>
        <plugin>
            <groupId>org.apache.maven.plugins</groupId>
            <artifactId>maven-checkstyle-plugin</artifactId>
            <version>2.9.1</version>
        </plugin>
    </plugins>
</reporting>
```

1.5. Findbugs

Es un producto de la Universidad de Maryland que, como su nombre indica, está especializado en encontrar errores.

Tiene una serie de categorías que catalogan los errores

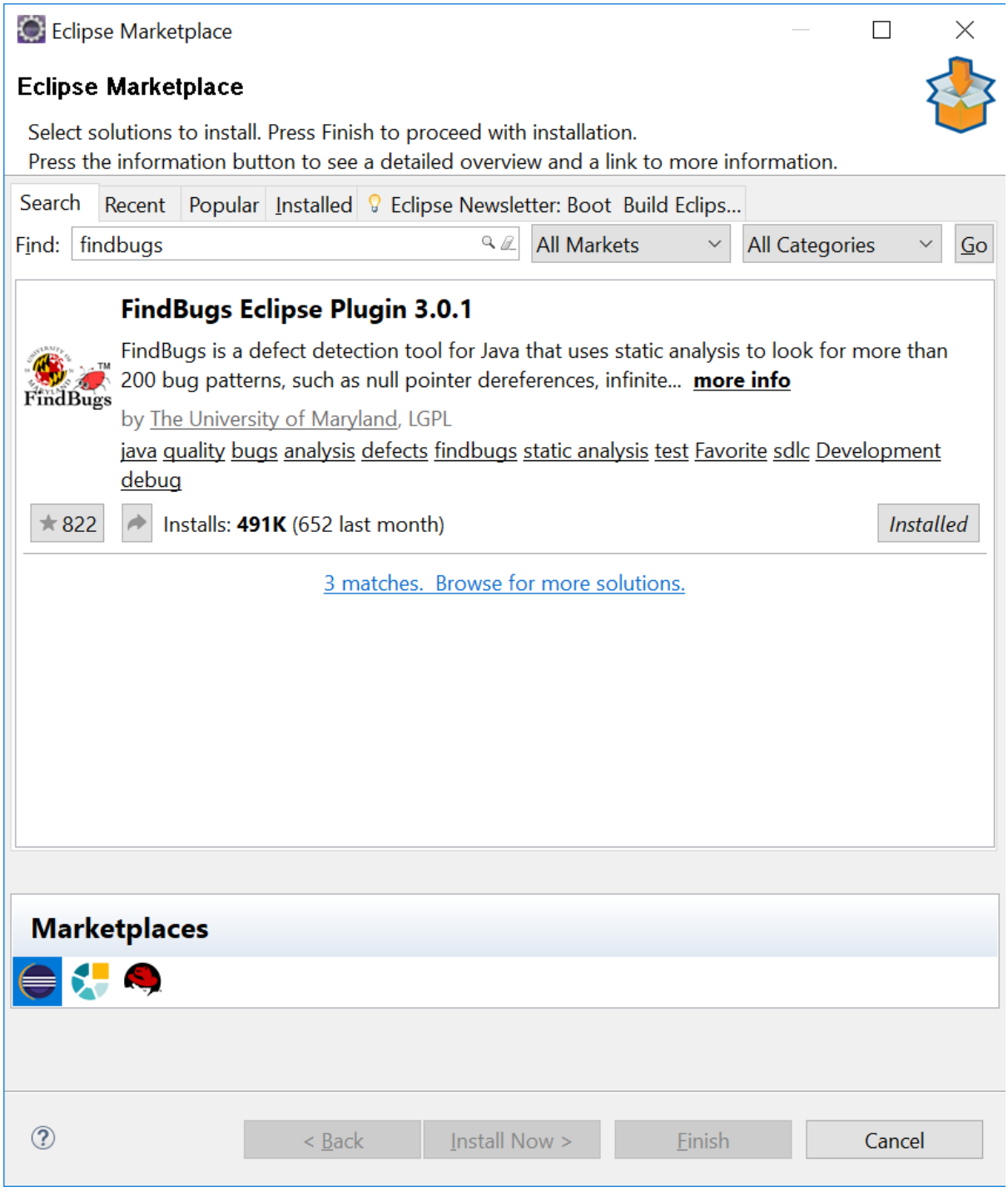
- malas prácticas
- mal uso del lenguaje
- internacionalización
- posibles vulnerabilidades
- mal uso de multihilo

- rendimiento
- seguridad, . . .

La página de referencia aquí y la descripción de los bugs aquí

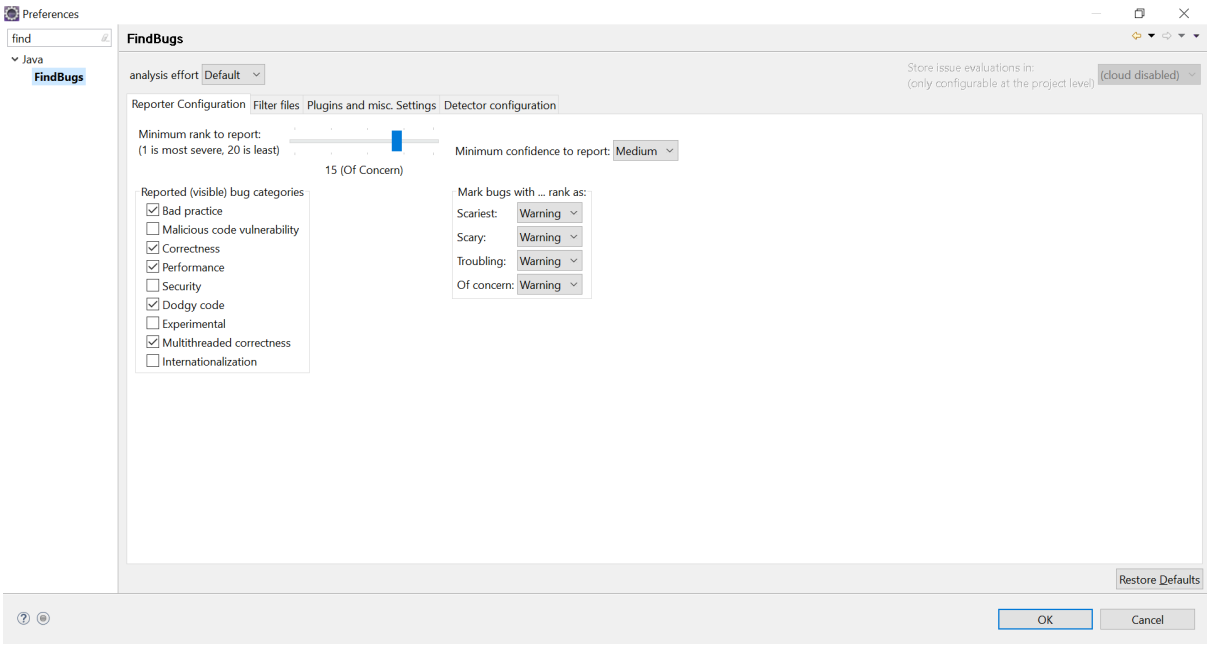
1.5.1. Plugin de Eclipse

Se puede descargar desde el Market de eclipse.

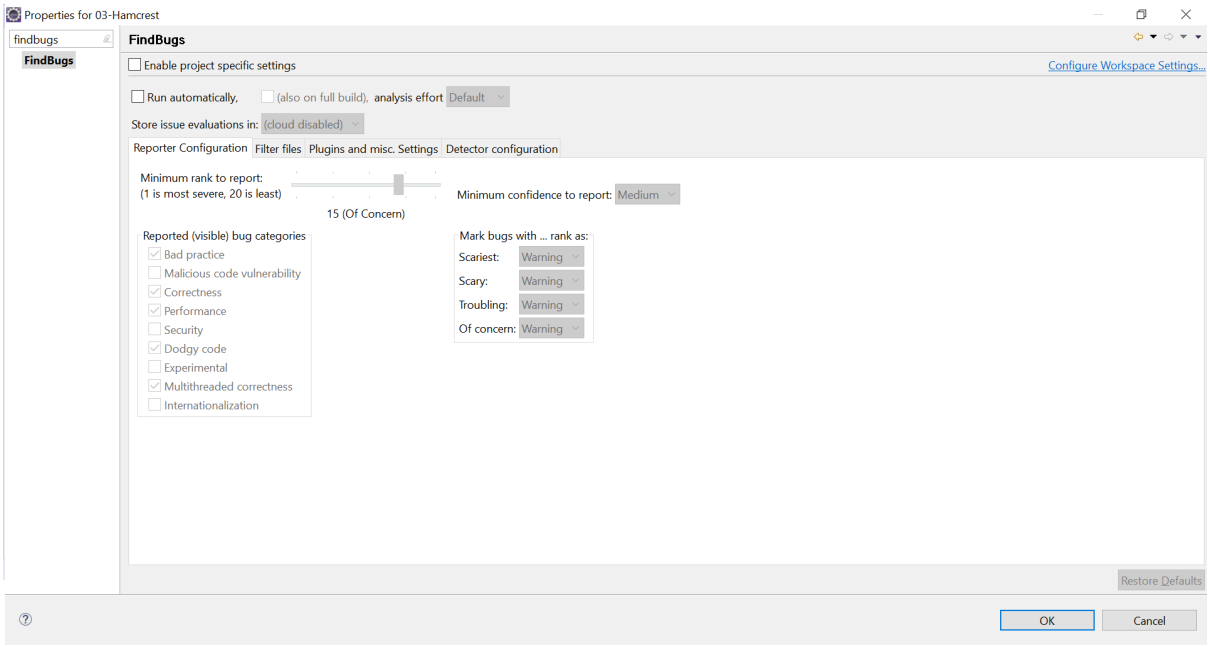


Permite configurar desde **Window - Preferences**:

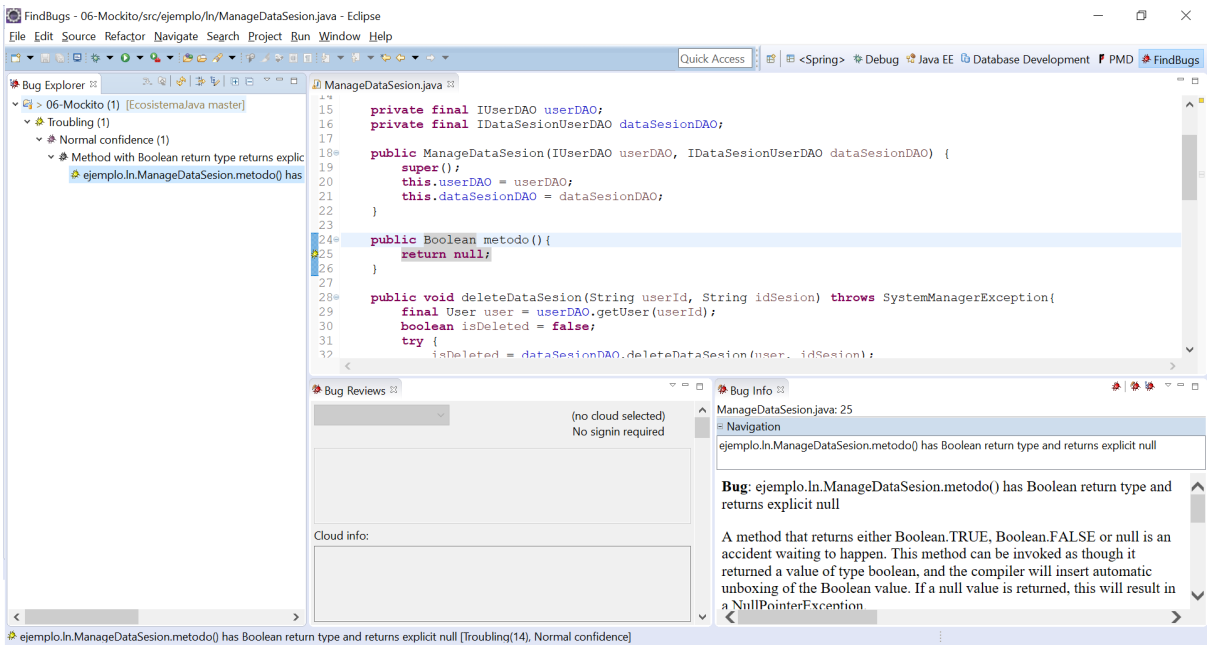
- Que incluir en los reportes
- Que ficheros participan del analisis
- Plugins activados
- Reglas activas



Desde el menu de propiedades del proyecto, se puede cambiar la configuracion global para el poryecto particular.



Para aplicar las reglas basta con acceder al menu del proyecto seleccionando la opcion **Findbugs - Finbugs**, mostrando los resultados en la perspectiva **Findbugs**.



1.5.2. Plugin de Maven

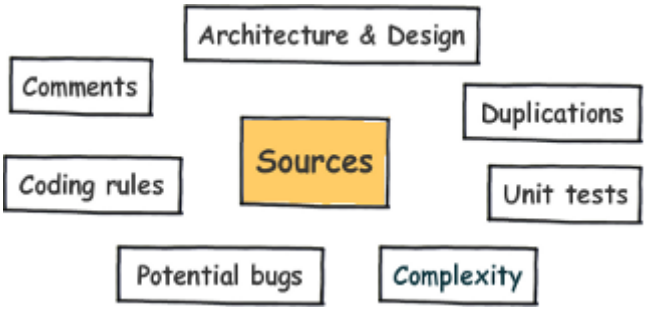
Hay un plugin de maven

```
<reporting>
    <plugins>
        <plugin>
            <groupId>org.codehaus.mojo</groupId>
            <artifactId>findbugs-maven-plugin</artifactId>
            <version>2.5.2</version>
        </plugin>
    </plugins>
</reporting>
```

2. Sonarqube

2.1. Introducción

Herramienta que centraliza otras herramientas que analizan la calidad estática del código de un proyecto. Cubre 7 ejes principales de la calidad del software



Ofrece información sobre

- Cobertura
- Complejidad ciclomatica.
- Buenas practicas.

A traves de herramientas como

- Checkstyle
- PMD
- FindBugs

Hay disponible una demo con APIs conocidas aquí

También hay un grupo español, que ofrece información aquí

Algunos de los plugins mas interesantes de Sonar

- PDF Export. Plugin que permite generqar pdf con la info de Sonar
- Motion Chart. Pluginque permite mostrar graficos en movimineto con la evolucion de las metricas
- Timeline. Plugin que visualiza el historico de las metricas
- Sonargraph. Plugin enables you to check and measure the overall coupling and the level of cyclic dependencies
- Taglist. Plugin handles Checkstyle ToDoComment rule and Squid NoSonar rule and generates a report.

2.2. Instalación

Descargar la distribución de aquí

Por defecto, trabaja con una base de datos **derby** y un user administrador

admin/admin

Configurar la base de datos en el fichero

```
SONAR_HOME/conf/sonar.properties
```

Estos son los posibles valores para mysql, de no configurarse se empleará una base de datos Derby, no recomendable para entornos de producción.

```
sonar.jdbc.url:
jdbc:mysql://localhost:3306/sonar?useUnicode=true&characterEncoding=utf
8
sonar.jdbc.driverClassName: com.mysql.jdbc.Driver
sonar.jdbc.validationQuery: select 1
sonar.jdbc.username=sonar
sonar.jdbc.password=sonar
```

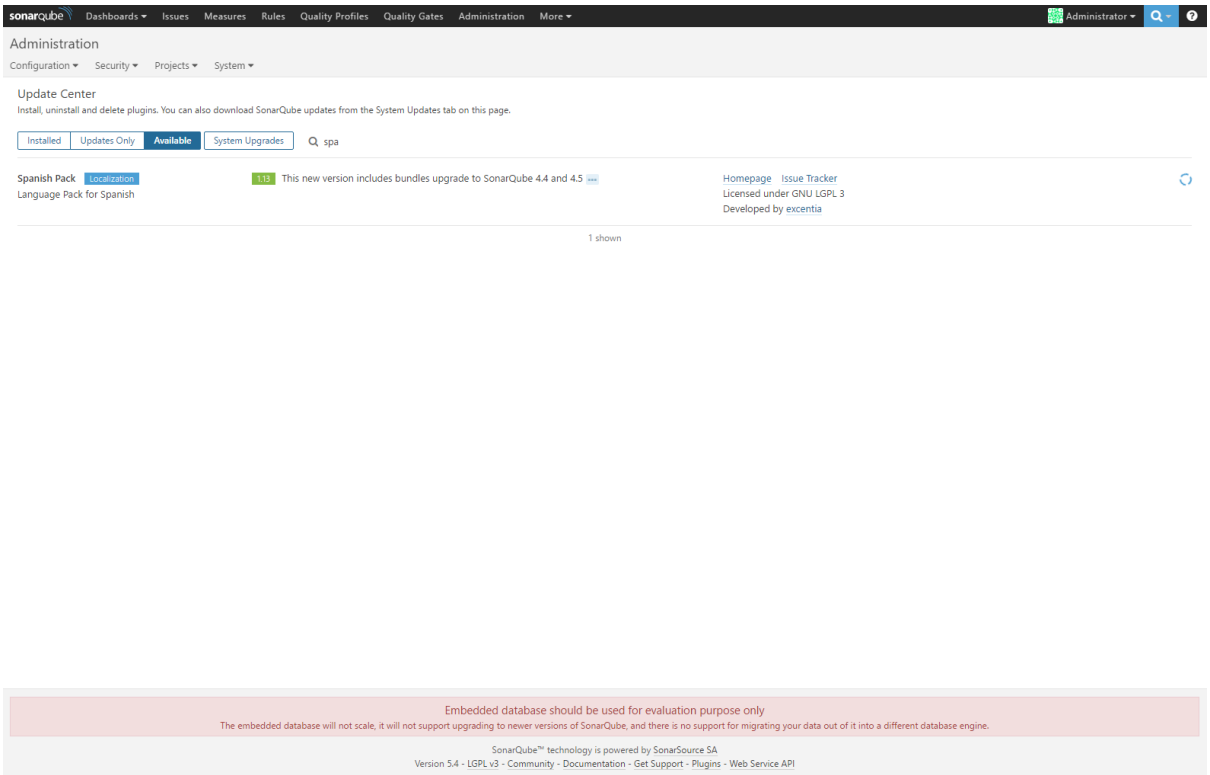
Arrancar el servidor con el comando para el sistema operativo correspondiente que se encuentra en

```
SONAR_HOME/bin/<sistema operativo>/<comando>
```

Esta opción arranca Sonar en el puerto **9000**, el puerto tambien se puede configurar en el anterior fichero de configuración.

Existe un usuario administrador creado por defecto con **admin/admin**

Se puede instalar un plugin para el idioma español, para ello acceder a **Administration/System/Update Center/Available Plugins** y buscar el **Spanish Pack**



2.3. Conceptos

Deuda tecnica: Es un calculo basado únicamente en **reglas** y **evidencias**. La deuda técnica en Sonar, se calcula con la metodología SQALE (Software Quality Assessment based on Lifecycle Expectations). Se mide en dias.

Reglas: Representan aquellos puntos que se desean vigilar en los proyectos. Se pueden definir con un perfil de calidad. Se pueden obtener mas reglas a partir de nuevos Plugins. Se pueden definir nuevas reglas basadas en plantillas.

Evidencias: Son los incumplimientos de las Reglas de calidad que se presentan en el código. Tendrán asociada una severidad. Con las evidencias se pued hacer: Comentar, Asignar, Planificar, Confirmar, Cambiar Severidad, Resolver y Falso Positivo. Todas estas tareas se pueden realizar de forma individual o conjunta. Se pueden definir evidencias manuales.

2.4. Organizacion

La interface web de sonar, se divide en tres partes

- Menu superior
- Menu lateral

- Zona de visualizacion de datos

En el menu superior aparecen los siguientes items

- **Cuadros de mando**: para volver en cualquier momento a la página de inicio
- **Proyectos**: para acceder al listado completo de proyectos, vistas, desarrolladores, etc. o para acceder de forma rápida a proyectos recientemente accedidos
- **Medidas**: permite definir consultas sobre las medidas, se pueden guardar para visualizarlas en un cuadro de mando.
- **Evidencias**: para acceder al servicio de evidencias
- **Reglas**: para acceder a la página de reglas
- **Perfiles**: navegar y gestionar perfiles de calidad
- **Configuración**: para acceder a la configuración del sistema (acceso restringido a administradores de sistema)
- *Conectarse: / <Nombre> para conectarse con tu usuario. Dependiendo de tus permisos de usuario, tendrás acceso a diferentes servicios y cuadros de mando. Autenticarte en el sistema te permitirá tener acceso a tu propia interfaz web personalizada. Desde aquí puedes modificar tu perfil y desconectarte.
- **Buscar un componente**: proyecto, fichero, vista, desarrollador, etc. para acceder rápidamente a él. Pulsa 's' para acceso directo a la caja de búsqueda.

El menú lateral ira cambiando sus opciones dependiendo del área en la que nos encuentremos, de los permisos de usuario y de las extensiones que se hayan incorporado en la instalación. Proporciona acceso a diferentes cuadros de mando y servicios.

2.5. Carga de datos

Para cargar los datos de un proyecto, se puede hacer de varias formas

- Plugin de Maven
- Sonar scanner

2.5.1. Sonar Scanner

Se puede descargar de aquí

Se debe incluir en la variable de entorno **PATH** el directorio **<SONAR_SCANNER_HOME>\bin**.

Y para analizar un proyecto, se debe ejecutar el comando

```
> sonar-scanner.bat -Dsonar.projectKey=hello_world_jasmine
-Dsonar.sources=. -Dsonar.host.url=http://localhost:9000
-Dsonar.login=d2e43f1a438391b6aaafab9ad5cf0bb9eed98721
```

2.5.2. Maven

La mas habitual es a través de un plugin de Maven.

```
<plugin>
    <groupId>org.codehaus.mojo</groupId>
    <artifactId>sonar-maven-plugin</artifactId>
    <version>2.7</version>
</plugin>
```

Y su goal

```
mvn sonar:sonar
```

Para la seleccion de un perfil de Sonar a emplear, se ha de indicar el parametro **sonar.profile**

```
-Dsonar.profile="Mi Perfil"
```

Si se desea publicar la cobertura en Sonar, se ha de seguir los pasos que se pueden encontrar en **https://github.com/SonarSource/sonar-examples/blob/master/projects/languajes/java/code-coverage**

2.6. Gestion de Usuarios y Seguridad

Se pueden añadir nuevos usuarios, grupos, definir permisos a nivel global o de proyecto, desde **Administration/Security/Users**

2.7. Cuadro de mando

Los cuadros de mando, son los componentes principales de Sonar, ya que son los que nos permiten configurar que información de que proyecto queremos visualizar y como visualizarlo.

Se organizan en columnas, pudiendo seleccionar entre 5 distribuciones distintas.

Se dividen en **Widget**, habiendo **Widget** orientados a distintos propositos, si se busca un Widget concreto se pueden filtrar los Widget mostrados por categorias.

Los Widget a parte de mostrar información, permiten acceder a vistas mas avanzadas, ya que en general los Widget ofrecen resumenes de la información.

Existen Widget que ofrecen información sobre

- Tamaño de los ficheros
- Bloques duplicados
- Mala distribución de la complejidad
- Codigo Spaguetti
- Falta de pruebas unitarias
- Cumplimiento de estandares y defectos potenciales
- Contabilizacion de comentarios
- Eventos en cuanto a la calidad.
- Treemap
- Evidencias y deuda técnica.
- Piramide de deuda técnica. Muestra la deuda tecnica organizada de abajo arriba por prioridad en su resolución.
- Resumen de deuda tecnica. Ofrece un Ratio entre lo que se necesita invertir para solventar la deuda tecnica y lo que se necesita invertir para crear el proyecto desde cero.

Calidad Estatica con Sonar