



PRÁCTICA SONARLINT

Sonar es una herramienta que nos permite analizar problemas en nuestro código desde nuestro IDE. Aporta más recomendaciones que las que nos puede dar cualquier IDE, entre ellas:

 Vulnerability





 Bug

 Security Hotspot

 Code Smell

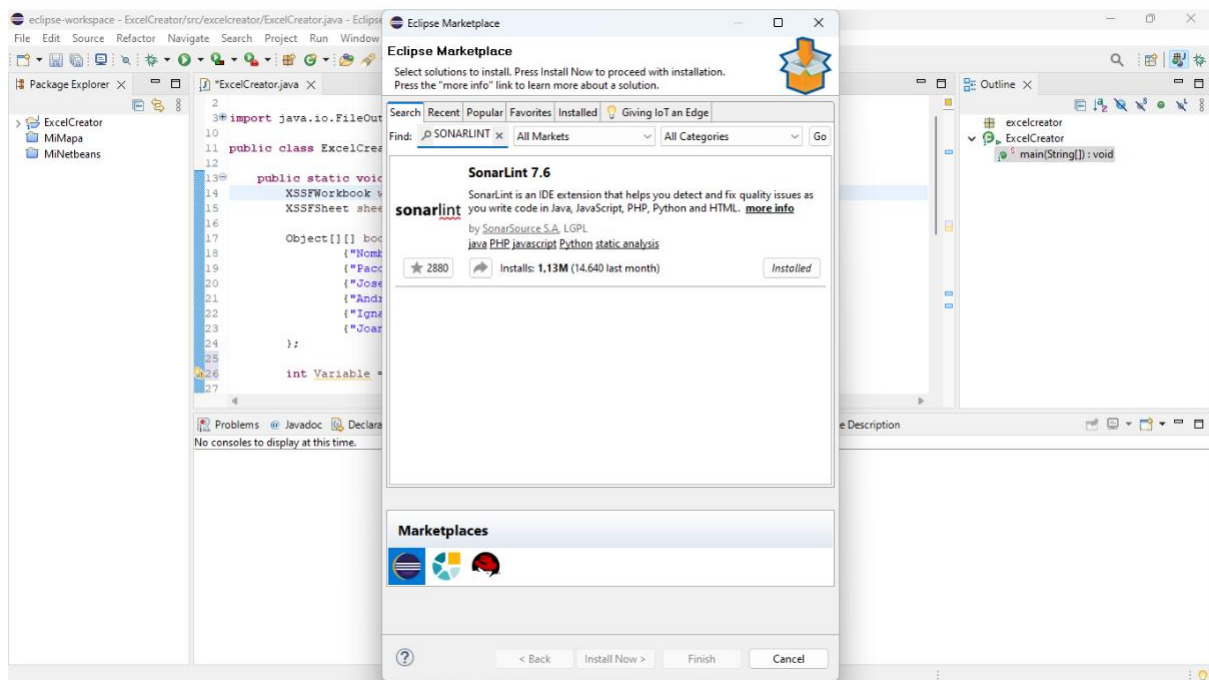
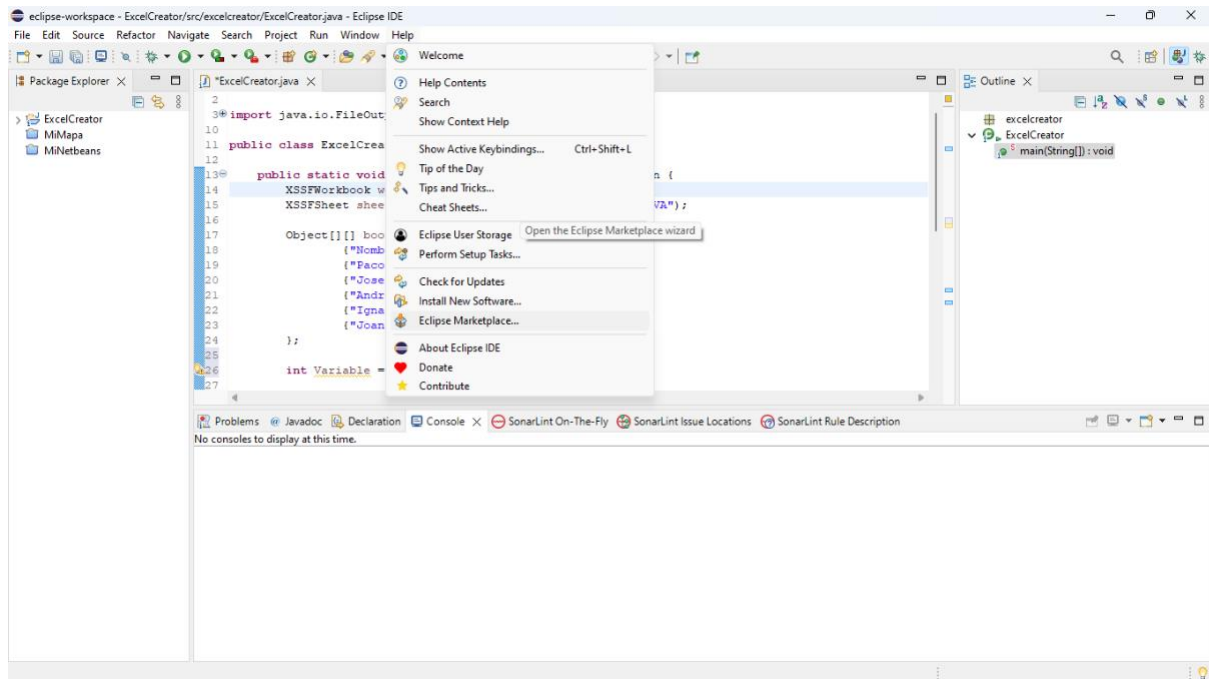
- **Vulnerabilidades:** un problema relacionado con la seguridad que representa una puerta trasera para los atacantes
- **Bugs:** un problema que representa algo incorrecto en el código. Si esto no ha provocado un error todavía, lo provocará y probablemente en el peor momento posible.
- **Punto de acceso de seguridad:** piezas de código sensibles a la seguridad que deben revisarse manualmente. Tras la revisión, descubrirá que no hay ninguna amenaza o que hay un código vulnerable que debe repararse.
- **Código apestoso (code smell):** un problema relacionado con la mantenibilidad en el código. Dejarlo como está significa que, en el mejor de los casos, los desarrolladores que mantienen el código tendrán más dificultades de las que deberían al realizar cambios. En el peor de los casos, estarán tan confundidos por el estado del código que introducirán errores adicionales a medida que realicen cambios.

Cada una de estas reglas se pueden ordenar por la siguiente severidad:

	 Blocker	 Critical	 Major	 Minor
Impact	High	High	Low	Low
Likelihood	High	Low	High	Low

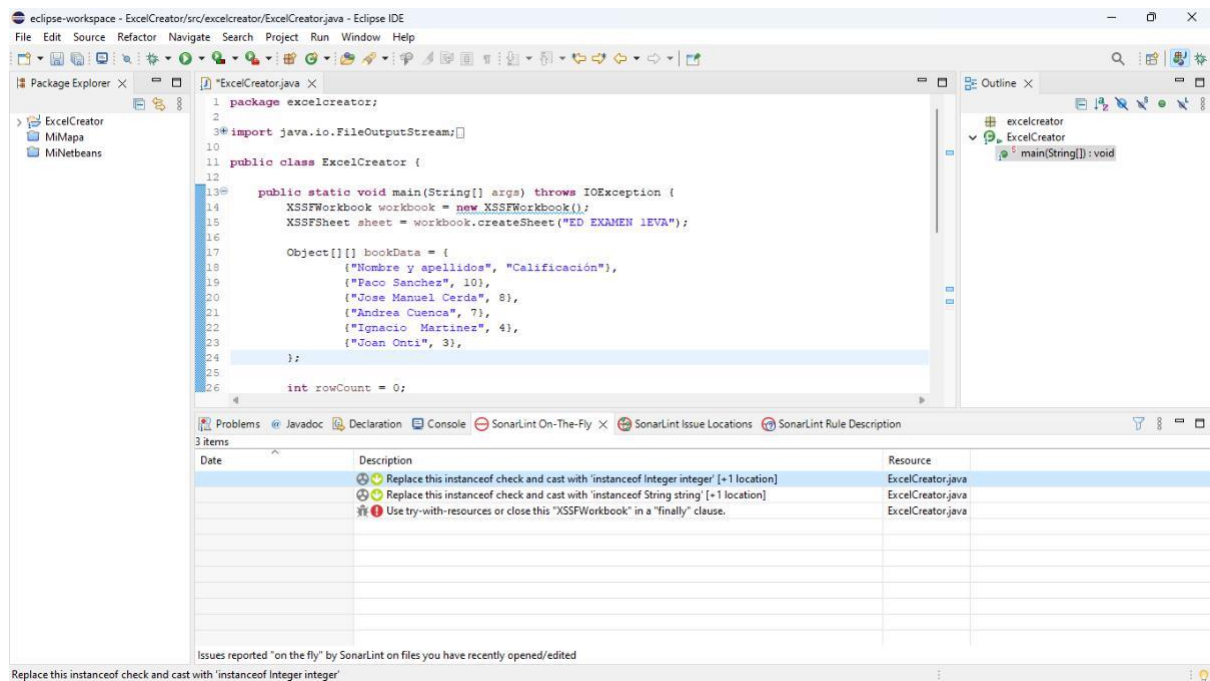
INSTALACIÓN DE SONARLINT EN ECLIPSE

Accedemos a 'Eclipse Marketplace' y buscamos 'SonarLint'. Procedemos con la instalación del plugin.

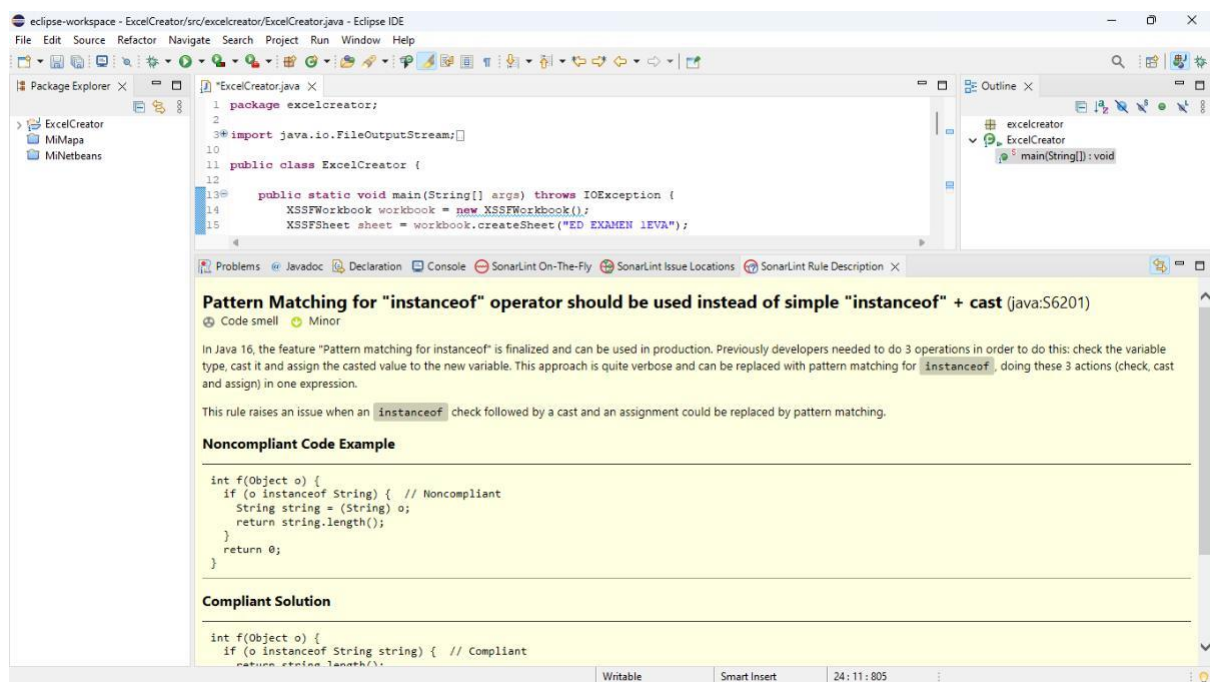


FUNCIONAMIENTO DE SONAR LINT

En la pestaña inferior 'SonarLint On-The-Fly' aparecen todas las mejoras que podemos hacer en nuestro código:



Clicando con el botón derecho del ratón en cada una de las recomendaciones podemos acceder a la descripción de la regla con un ejemplo de mal funcionamiento y de solución del error:



Ejercicio 1

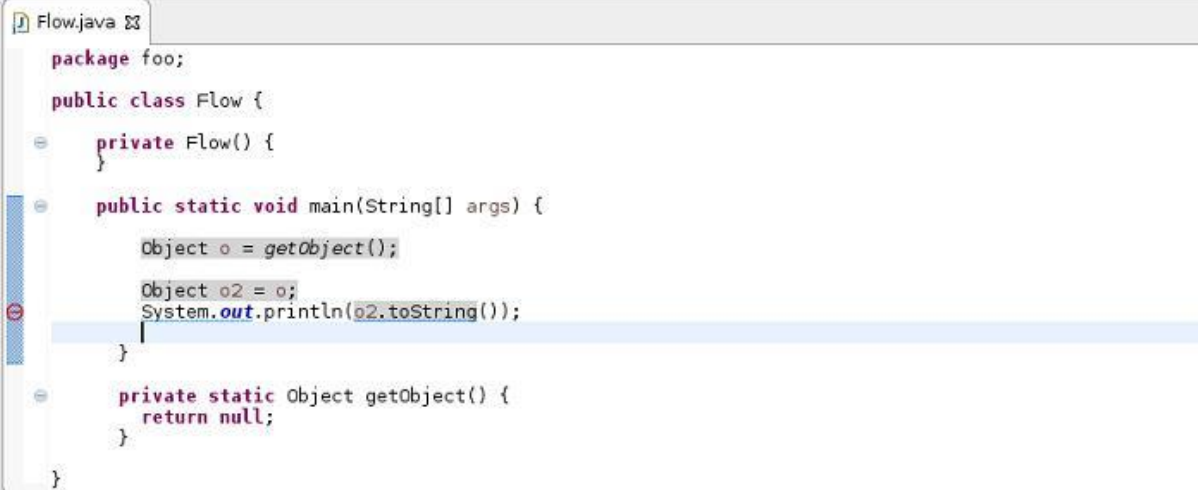
Crea un documento word con tres vulnerabilidades, tres bugs, tres security hotspot y tres code smell en JAVA sacados de la web oficial (y que entiendas que significan).

Explica cada uno de ellos.

Web oficial: <https://rules.sonarsource.com/java/>

Ejercicio 2

Crea un proyecto con el siguiente código:



```
Flow.java
package foo;

public class Flow {

    private Flow() {
    }

    public static void main(String[] args) {
        Object o = getObject();

        Object o2 = o;
        System.out.println(o2.toString());
    }

    private static Object getObject() {
        return null;
    }
}
```

Analiza las recomendaciones que aporta SonarLint, corrégelas y documéntalas en un Word.