Universidad de Sevilla

Escuela Técnica Superior de Ingeniería Informática

Devising A Project

Herramientas para análisis de código

Grado en Ingeniería Informática – Ingeniería del Software

Ingeniería del Software y Práctica Profesional

Curso 2023 – 2024

Fecha	Versión
16/02/2024	1.0

Grupo de prácticas: 8
Alberto Benitez Morales
Álvaro Carrera Bernal
Álvaro Navarro Rivera
Álvaro Jose Sanchez Flores
Artemio Rodriguez Asensio
Eduardo de Bustamante Lucena
Fernando Barroso Barroso
Francisco Jose Vargas Castro
Gonzalo Santigo Martín
Guillermo Alonso Pacheco Rodrigues
Jaime Caballero Hernandez
Javier Nunes Ruiz
Javier Rodríguez Cordero
Juan Martínez Cano
Marco Antonio Roca Rodríguez
Mario Sanchez Naranjo
Pablo Martínez Valladares

Versiones

Fecha	Versión	Descripción
16/02/2024	1.0	Primera versión del documento

Índice de contenido

Herramientas de análisis de código

Las herramientas de análisis de código son herramientas diseñadas para ayudar a los desarrolladores a mejorar la calidad de su código mediante la identificación de problemas, vulnerabilidades y áreas de mejora. Estas herramientas utilizan técnicas automatizadas para examinar el código fuente y aplicar reglas predefinidas o personalizadas para evaluar su calidad. En nuestro proyecto utilizaremos SonarCloud como principal herramienta de análisis de código.

SonarCloud es un servicio de análisis estático de código basado en la nube y que lo ofrece la empresa responsable de SonarQube, uno de los servicios on-premise más conocidos y utilizados para realizar SAST(Static Application Security Testing), diseñado para detectar problemas de calidad de código en 25 lenguajes de programación diferentes.

Además de medir la seguridad de nuestras aplicaciones, nos ayuda a mejorar la mantenibilidad y confiabilidad de nuestro código. SonarCloud se integra con los siguientes servicios que manejan repositorios con base en git:

- GitHub
- GitLab
- Bitbucket
- Azure DevOps

Hemos decidido utilizar sonarCloud porque es una herramienta de análisis de código con la que hemos trabajado la gran mayoría a lo largo de la carrera, por lo tanto el equipo no tendrá que enfrentarse a la curva de aprendizaje que supone el uso de una herramienta nueva. Utilizaremos sonarCloud con la intención de comprobar que producimos código seguro, mantenible y libre de bugs. Además, sonarCloud es un servicio gratuito para repositorios públicos.

Para usar SonarCloud conectaremos nuestro repositorio de GitHub con la herramienta, que analizará nuestro código sin necesidad de que se ejecute. Los análisis se realizarán de forma automática cada vez que se hace un nuevo commit a la rama principal, teniendo así siempre los datos actualizados.
Los datos que nos devuelve SonarCloud que nos serán útiles son los siguientes:

- Bugs: Errores detectados en el código
- Code Smells: Mala práctica o código que puede derivar en un error
- Vulnerabilidades: Debilidades en el código que pueden ser explotadas, poniendo en riesgo la información que se maneja.
- Puntos calientes de seguridad: Partes de código sensibles de los que puede surgir una vulnerabilidad

SonarCloud nos da todos estos datos marcando tanto en qué parte exacta del código se encuentra, como el grado en el que puede afectar al código desarrollado. Gracias a esta información podremos identificar estos errores o malas prácticas que no fuéramos capaces de identificar sin la herramienta.