Desarrollo de Software Seguro

Adriana Liceth Fontecha Cañas

ID: 943450

Brayan Ferney Forero Vega

ID:946416

Julian David Rodriguez Cortes

ID:957778

Ingeniería de Sistemas

Corporación Universitaria Minuto de Dios

NRC-50-61831 Desarrollo de Software Seguro

Docente: Edwin Albeiro Ramos Villamil

2025

Informe de Análisis de Vulnerabilidades y Calidad del Código

Herramienta utilizada: SonarCloud

Fecha del análisis: 05/10/2025

Introducción

El presente informe describe los resultados obtenidos tras el análisis de calidad del código fuente del proyecto utilizando la plataforma SonarCloud.
El objetivo de este análisis es identificar vulnerabilidades, problemas de mantenibilidad, confiabilidad y duplicaciones en el código, con el fin de mejorar la calidad del software y reducir los riesgos en su operación.

Resumen General del Análisis

Métrica	Valor	Calificación	Observaciones
Seguridad	**0 issues**	**A**	**No se detectaron vulnerabilidades o riesgos de seguridad.**
Confiabilidad (Reliability)	**1 issue**	**C**	**Se identificó un problema menor que puede afectar el comportamiento en tiempo de ejecución.**
Mantenibilidad (Maintainability)	**7 issues**	**A**	**Los problemas son menores y no comprometen la estructura del código.**
Cobertura de pruebas (Coverage)	**No analizada**	**—**	**Es necesario configurar la cobertura para obtener métricas de pruebas unitarias.**
Duplicaciones	**0.2%**	**—**	**Excelente nivel, prácticamente sin código duplicado.**
Security Hotspots	**3**	**—**	**Se identificaron tres áreas que requieren revisión manual por**

			posibles riesgos de seguridad.

Análisis Detallado

Seguridad

- Resultados: 0 vulnerabilidades abiertas.
- Calificación: A (Excelente).
- Conclusión: El proyecto no presenta fallas de seguridad detectadas automáticamente. Los *Security Hotspots* identificados deben revisarse manualmente para confirmar que no representan un riesgo.

3.2 Confiabilidad

- Resultados: 1 problema abierto (nivel C).
- Descripción: Este tipo de hallazgo generalmente está relacionado con posibles errores lógicos, excepciones no controladas o condiciones límite no verificadas.
- Recomendación: Revisar el reporte detallado en SonarCloud para identificar el archivo afectado y aplicar las correcciones sugeridas.

3.3 Mantenibilidad

- Resultados: 7 issues menores.
- Calificación: A (Buena mantenibilidad).
- Descripción: Se detectaron ligeras oportunidades de mejora, posiblemente relacionadas con complejidad ciclomática, comentarios faltantes o código innecesariamente complejo.
- Recomendación: Aplicar refactorización ligera para mantener un código limpio y legible.

3.4 Duplicación de Código

- Resultados: 0.2% de duplicación.

- Conclusión: Excelente práctica de reutilización de código. No se observan fragmentos redundantes significativos.

3.5 Cobertura de Pruebas

- Resultados: No disponible.
- Observación: SonarCloud indica que es necesario configurar la integración para medir la cobertura de pruebas unitarias.
- Recomendación: Implementar pruebas automatizadas (por ejemplo, con Jest, Mocha, o JUnit según el lenguaje) y configurar el reporte para integrarlo con SonarCloud.

3.6 Security Hotspots

- Resultados: 3 puntos identificados.
- Descripción: Los *hotspots* no son vulnerabilidades confirmadas, pero representan fragmentos de código que deben ser revisados manualmente, como el uso de funciones criptográficas, manejo de tokens o validaciones de entrada.
- Recomendación: Revisar manualmente cada hotspot y documentar si el riesgo es aceptable o requiere mitigación.

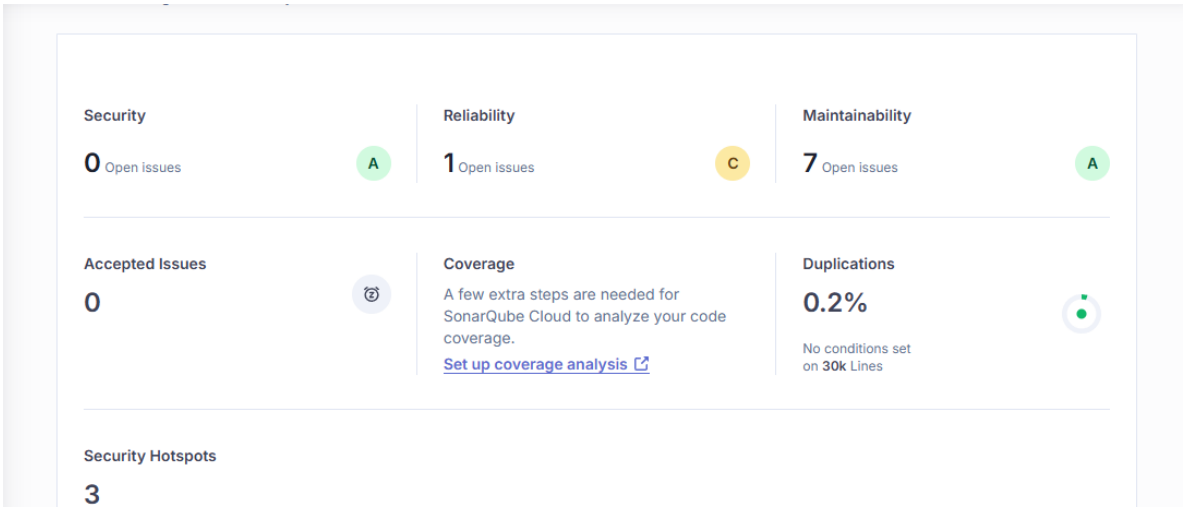
Conclusiones Generales

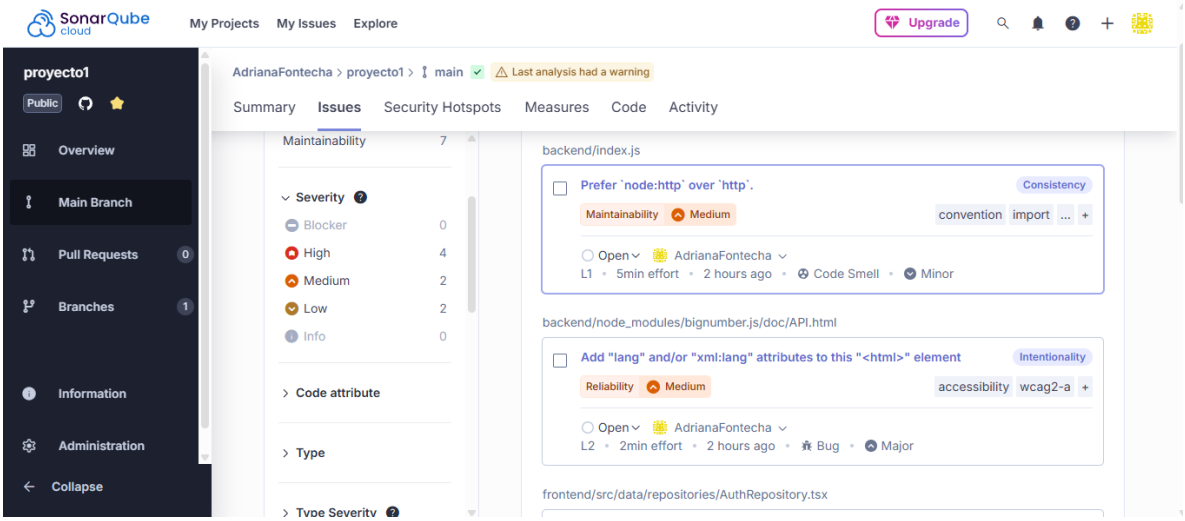
El análisis de SonarCloud muestra que el proyecto tiene una muy buena calidad de código, con cero vulnerabilidades críticas y mínimos problemas de confiabilidad y mantenibilidad. El nivel de duplicación es muy bajo (0.2%), lo que demuestra buenas prácticas de programación.
Se recomienda realizar las siguientes acciones:

1. Revisar los *Security Hotspots* para confirmar que no representan riesgos.
2. Corregir el único problema de confiabilidad identificado.
3. Implementar la cobertura de pruebas unitarias para monitorear la calidad del código en futuras versiones.

Recomendaciones Finales

- Mantener un análisis continuo con SonarCloud en cada *commit* o *pull request*.
- Aplicar las correcciones sugeridas en los archivos marcados.
- Implementar una política de calidad que establezca métricas mínimas de cobertura y mantenibilidad.
- Documentar las revisiones de seguridad y los cambios realizados tras este informe.





	Lines of Code	Security	Reliability	Maintainability	Security Hotspots	Coverage	Duplications
proyecto1							
backend	2,424	0	1	1	2	—	0.0%
database	0	0	0	0	0	—	0.0%
frontend	519	0	0	6	1	—	0.6%
USUARIOS.postman_...	—	0	0	0	0	—	0.0%

4 of 4 shown

Enlace de github : https://github.com/AdrianaFontecha/proyecto1.git