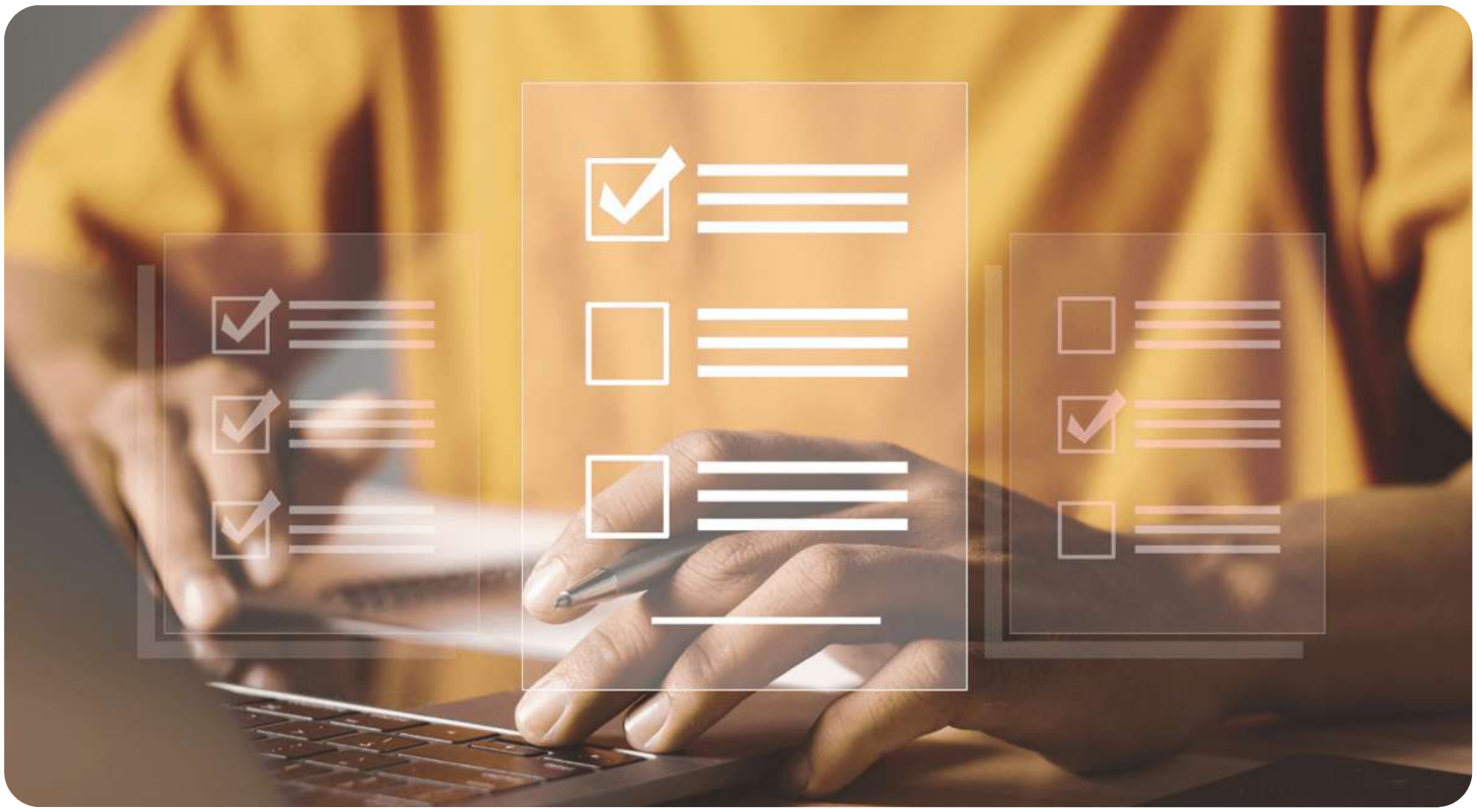
DuocUC | ONLINE



Semana 4
Seguridad y calidad en el desarrollo de software (ISY2202)

Actividad formativa S4

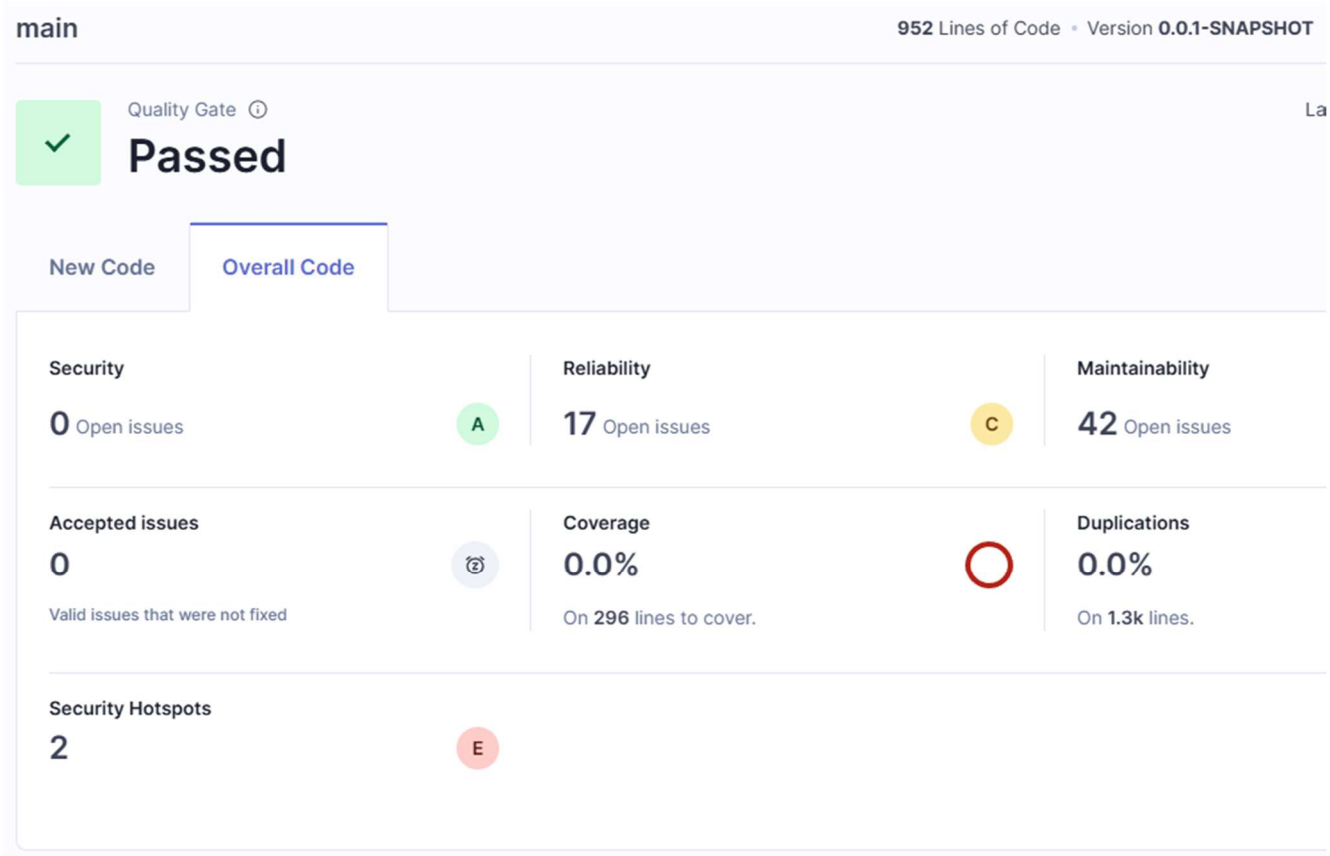
Grupo 1: César Bravo – Víctor Núñez

Introducción

En esta cuarta semana, ejecutaremos un análisis de código estático sobre la actividad desarrollada en las últimas entregas, y resolveremos los problemas más graves encontrados.

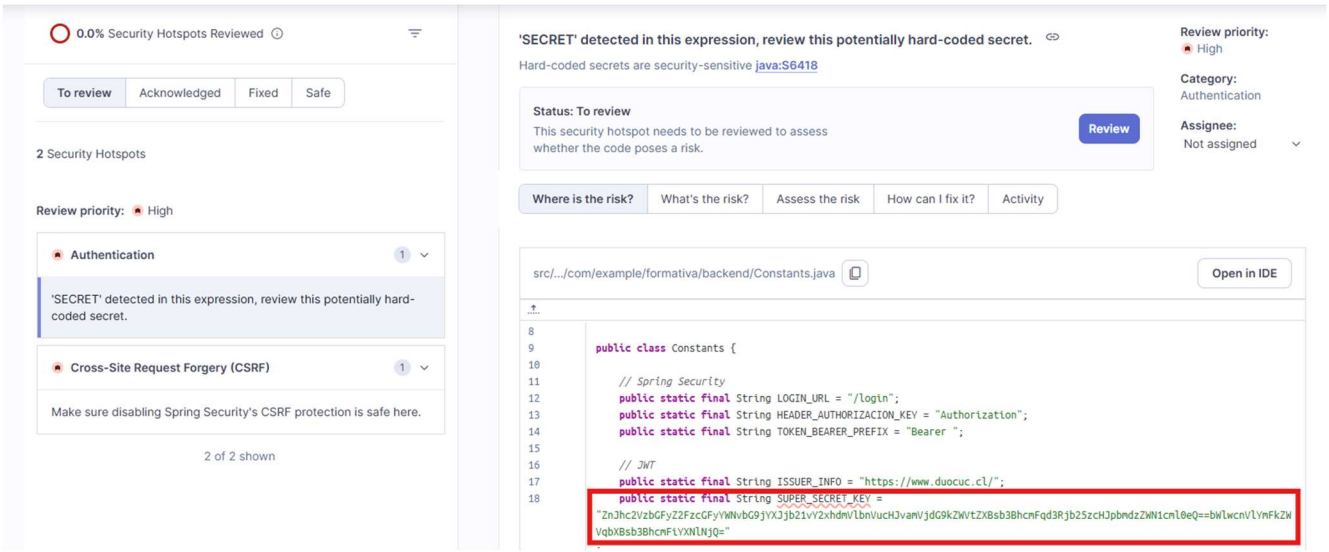
Desarrollo

Instalamos SonarQube vía Docker y ejecutamos el comando de mvn desde la carpeta del proyecto. Los resultados fueron los siguientes:

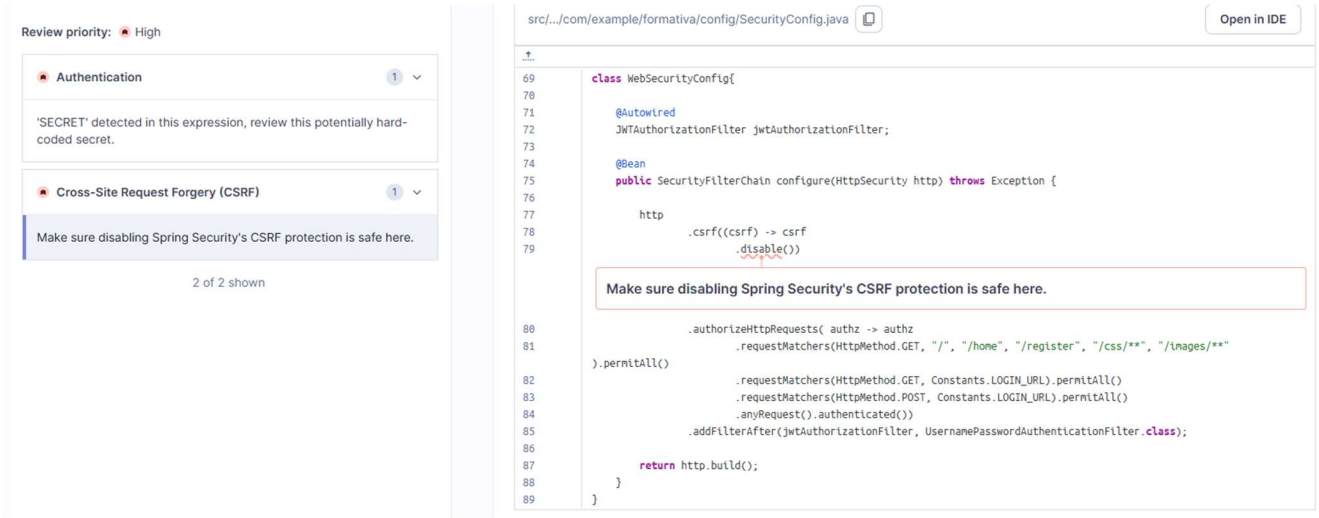


Podemos ver que el código pasa el quality gate, y que casi todos los issues encontrados son de mantenibilidad y no requieren atención inmediata. Sin embargo, hay dos issues de seguridad que deberíamos abordar con prioridad:

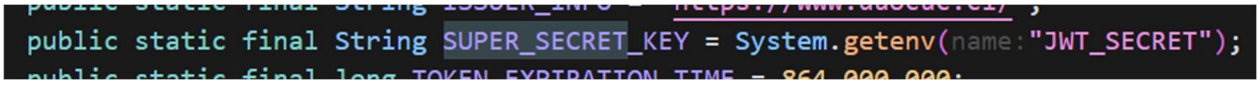
1) Secreto en código



2) CSRF deshabilitado



Resolvimos el primer issue leyendo una variable de ambiente en vez de tener el secreto directamente en el código.

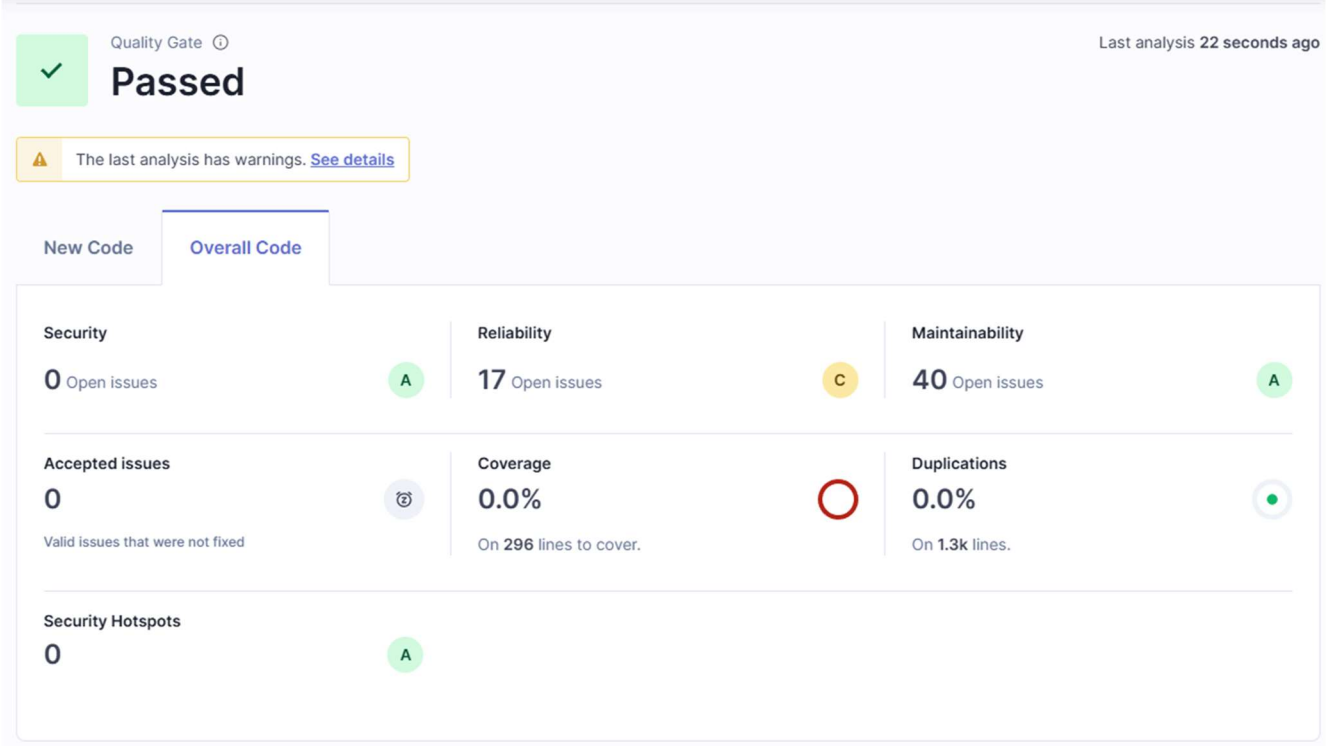


Agregamos la variable de ambiente JWT_SECRET al archivo docker-compose.yml:

```
services:
  app:
    build: .
    ports:
      - "80:8080"
    depends_on:
      - mysql
    environment:
      SPRING_DATASOURCE_URL: jdbc:mysql://mysql:3306/formativa
      SPRING_DATASOURCE_USERNAME: root
      SPRING_DATASOURCE_PASSWORD: root
      JWT_SECRET: ZnJhc2VzbGFyZ2FzcGFyYWNvbG9jYXJjb21vY2xhdmVlbnVucHJvamVjdG9kZWVtZXBsb3BhcmFqd3Rjb25zcHJpbmc
    networks:
      - app-network
```

El segundo issue lo resolvimos quitando la llamada a csrf.disable().

Ejecutamos el análisis de SonarQube nuevamente y obtuvimos estos resultados:



Conclusión

En esta actividad aprendimos el flujo básico de uso de SonarQube: su instalación, configuración y uso vía línea de comandos. Ejecutamos dos análisis de código estático y resolvimos los problemas de seguridad que encontró.

Aprendimos también las distintas categorías de issues que tiene SonarQube.