

Semana 4

Seguridad y calidad en el desarrollo de software (ISY2202)

Actividad formativa S4

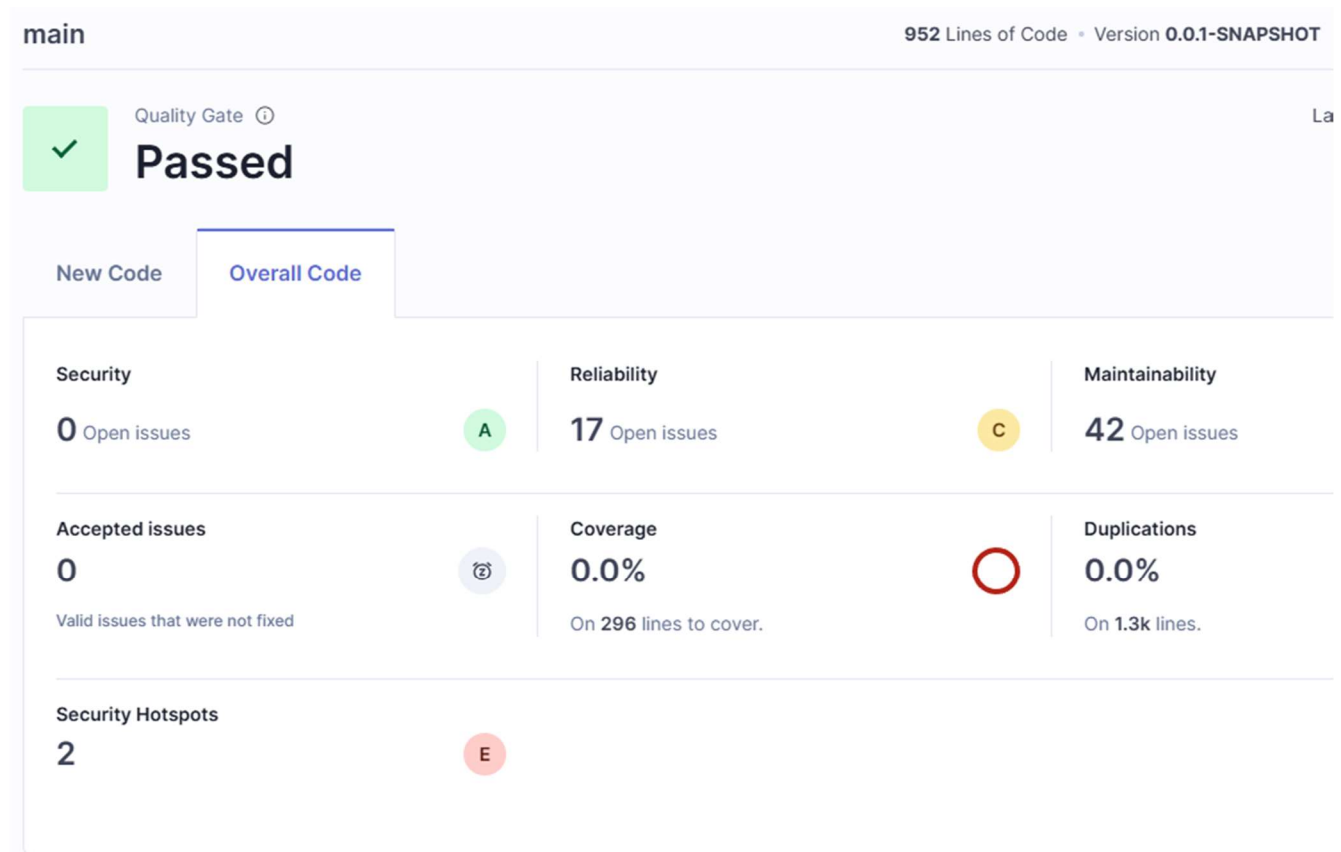
Grupo 1: César Bravo – Víctor Núñez

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

The screenshot shows a security tool interface with a sidebar on the left and a main content area on the right. The sidebar has a header '0.0% Security Hotspots Reviewed' and a filter bar with 'To review', 'Acknowledged', 'Fixed', and 'Safe'. Below this, it shows '2 Security Hotspots' and a 'Review priority: High' section. The first hotspot is 'Authentication' with a status of 'To review'. The main content area shows a message: 'SECRET detected in this expression, review this potentially hard-coded secret.' Below this, it says 'Hard-coded secrets are security-sensitive java:S6418'. There is a 'Review' button and a 'Status: To review' section. The code snippet shown is from 'src/.../com/example/formativa/backend/Constants.java' and contains a red box highlighting a long, complex string value for 'SUPER_SECRET_KEY'.

2) CSRF deshabilitado

The screenshot shows the same security tool interface as before, but now the second hotspot is 'Cross-Site Request Forgery (CSRF)' with a status of 'To review'. The main content area shows a message: 'Make sure disabling Spring Security's CSRF protection is safe here.' Below this, it says 'Hard-coded secrets are security-sensitive java:S6418'. There is a 'Review' button and a 'Status: To review' section. The code snippet shown is from 'src/.../com/example/formativa/config/SecurityConfig.java' and contains a red box highlighting the line where 'csrf.disable()' is called.

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

```
public static final String ISSUER_INFO = "https://www.duocuc.cl/";  
public static final String SUPER_SECRET_KEY = System.getenv(name: "JWT_SECRET");  
public static final long TOKEN_EXPIRATION_TIME = 864 000 000;
```

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

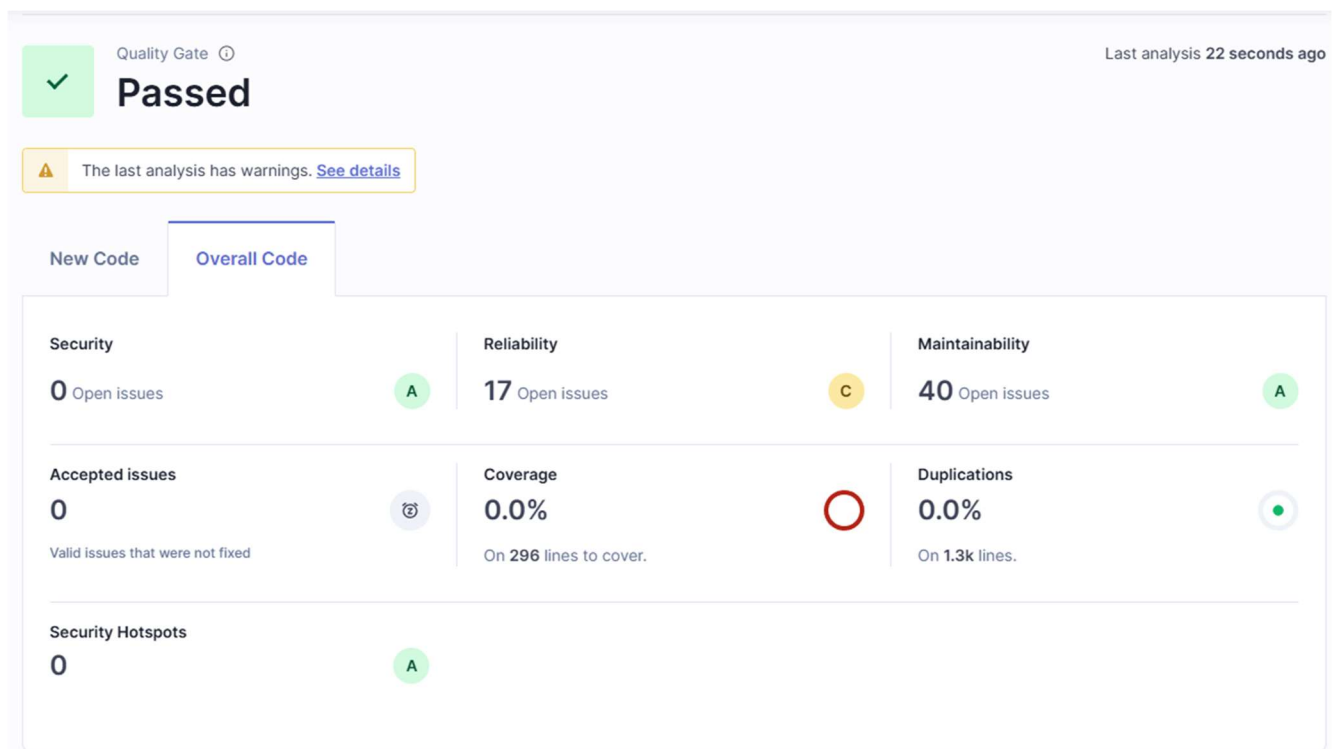
```

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: ZnJhc2VzbGFyZ2FzcGFyYWNvbG9jYXJjb21vY2xhdmV1bnVucHJvamVjdG9kZWVtZXBs3BhcmFqd3Rjb25zcHJpbmc
    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.



Reservados todos los derechos Fundación Instituto Profesional Duoc UC. No se permite copiar, reproducir, reeditar, descargar, publicar, emitir, difundir, de forma total o parcial la presente obra, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otros) sin autorización previa y por escrito de Fundación Instituto Profesional Duoc UC. La infracción de dichos derechos puede constituir un delito contra la propiedad intelectual.