정적 코드 분석

■ 검토 배경

- 아모레몰 모둠 체제의 출범으로 소스코드 전체 볼륨이 증가하고 있으며, 전략과제 수행 결과 테스트케이스 수 대비 결함이 5.45%(최대 15.6%) 발견됨
- 테스트 단계에서는 사용자 관점의 블랙박스 형태의 테스트이기 때문에 모든 결함을 발견하는 데에는 한계점이 있음
- BY23 경영 진단 결과 아모레몰의 서비스 품질에 대한 필요성이 대두됨

소스코드 정적 분석을 통해 개발 단계에서 조기에 결함을 발견하고 보완하여 소스코드 품질을 강화하기 위한 방안을 수립하고자 함

🥊 정적 분석이란? 소스 코드의 실행 없이 정적으로 코드를 검사하여 잠재적으로 발생이 가능한 버그 및 취약점을 발견하는 과정을 의미

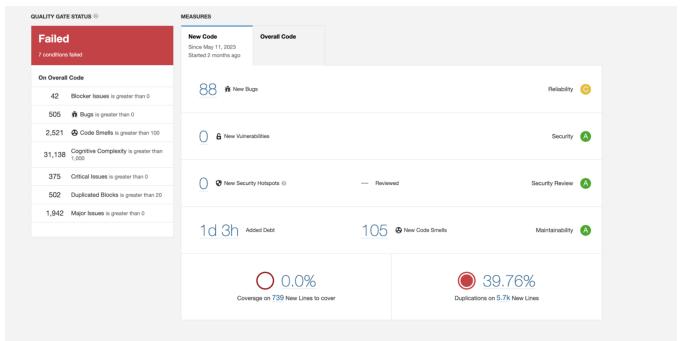
■ 추진 목표

아모레몰 서비스 품질 강화 - 정적 분석 도구(Sonarqube) 도입 및 배포 프로세스에 적용하여 소스코드 품질을 상시 모니터링이 가능토록 함

- b 소스코드 품질 강화 테스트 단계보다 더 빠른 시점인 빌드 시점에 잠재적인 버그와 취약점을 식별 및 보완 → 테스트 수행 전 소스코드의 기본 품질 확보
- 기술적 부채 관리 이슈 별로 심각도를 제공하여 중요한 문제부터 점진적으로 처리하여 기술적 부채 개선
- 🖕 실시간 품질 모니터링 Jira 대시보드를 통해 아모레몰 소스코드 품질 통계 및 추이를 제공하여 서비스 품질 상태를 실시간으로 파악 가능

■ To-Be

SonarQube 정적분석 결과 예시



- 결함 (Bugs): 런타임 오류 또는 예기치 않은 동작으로 이어질 수 있는 결함
 - Blocker: 최악의 경우 어플리케이션이 중단되거나 저장된 데이터가 손상될 수 있는 이슈
 - Critical: 보안 결함을 나타내는 이슈
- 코드 스멜(Code Smells): 코드 품질을 저하시키거나 유지보수성을 낮추는 코드
- 복잡도 (Complexity): 코드 복잡도를 측정하고, 너무 복잡한 코드를 감지
- 중복 코드(Duplicated Blocks): 중복 코드를 찾아내고, 중복 코드의 비율을 평가
- Lines of Code: 전체 소스코드 라인 수

정적분석 테스트 프레임워크 구조



Jira 대시보드

Jira 대시보드를 통해 전체 아모레몰 프로젝트의 품질기준(Quality Gate) 합격 현황, 보안취약점 및 크리티컬 이슈 현황을 실시간으로 조회할 수 있도록 구성함. 대시보드 링크: http://jira-digit.amorepacific.com:8080/secure/Dashboard.jspa?selectPageId=17800

