DB 침입 탐지 시스템(DB-IDS) System Test Results 보고

202211252 컴퓨터공학부 고승우

Executive Summary

테스트 성과 및 결함 요약

핵심 기능

시스템 테스트(ST-01~06) 시나리오 **모두 Pass**

성능 목표

처리량(102/sec), 동시성(100명) **100% 달성**

데이터 정합성

UI-API-DB 간 데이터 일관성 확인 **(ST-06)**

식별된 결함

'로그 아카이브(D-01)' 등 3건의 미구현 기능 식별

Unit Test Analysis

단위 테스트(UT) 분석: 방어 로직 및 정확성 검증

01

쿼리 처리 검증

비정상 UTF-8, SQL 예외 (SQLException) 발생 시 정상 처리 확인 (UT-01, UT-02)

02

정규화 로직 검증

1=1 → 0=0 리터럴 마스킹, 주석 제거 등 우회 시도 무력화 검증 (UT-03-RE)

03

패턴 탐지 검증

정규화된 SQL에 대해 패턴 탐지 이벤트 생성 및 심각도 산정 로직 검증 (UT-03-DS / UT-04-DS)

04

행동 탐지 검증

단위 시간 당 질의 폭주 등의 행동 패턴의 이벤트를 생성하는 로직 검증 (UT-05 / UT-06)

05

권한 탐지 검증

룰 기반 권한정책에 따라 권한 위반 이벤트를 생성하는 로직 검증 (UT-07 / UT-08)

06

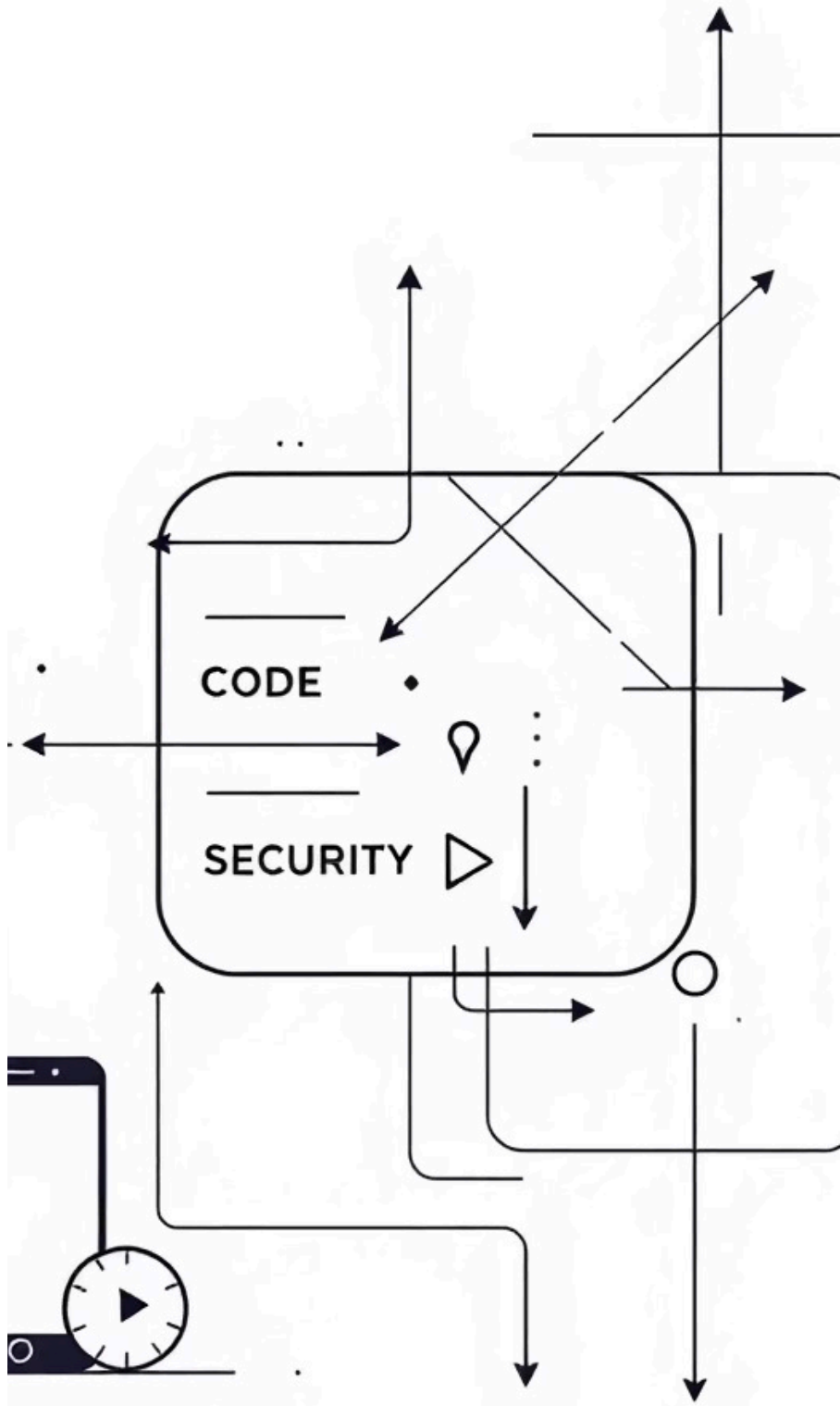
알림 전송 검증

이메일과 슬랙 알림 전송에 대한 검증 (UT-09 / UT-10)

07

쿼리 로그 저장 검증

쿼리 로그 저장 로직의 유효성 검증/정규화/저장 연동을 단위 수준에서 검증 (UT-11)



Integration Test Analysis

통합 테스트(IT) 분석: End-to-End 시나리오 연계 검증

데이터 파이프라인

로그 수집(POST)부터 조회(GET)까지 데이터 일관성 및 ID 일치 확인 (IT-01)

탐지-알림 연계

DROP TABLE 수집(POST) → PATTERN/HIGH 이벤트 생성 → **Mailhog(Email)** 및 **WireMock(Slack)** 동시 발송 성공 (IT-05)

대시보드(UI) 연동 검증

백엔드에 생성된 데이터가 대시보드에 정확히 반영

탐지 3종 연계

패턴(IT-02), 행동(IT-03), 권한(IT-04) 이벤트 모두 API 레벨에서 정상 생성 및 조회 확인

System Test Analysis

시스템 테스트(ST) 분석: 실운영(EC2) 환경 검증

1

핵심 시나리오 6종 Pass

로깅, 패턴, 행동, 권한, 알림, UI 정합성 모두 통과

2

데이터 정합성(ST-06)

EC2 대시보드 UI ↔️ API 응답 ↔️ DB 데이터 간 불일치 없음 확인

3

검증 완료

사용자 요구사항(FR-1~6)의 핵심 기능이 실제 환경에서 정상 동작함을 입증

Non-Functional Test Analysis

비기능(NFT) 테스트 분석: 성능 및 보안

102/sec

처리량(NFT-02)

목표 100/sec, **실측 102.0/sec (목표 달성)**

100

동시성(NFT-03)

관리자 100명 동시 접속, **오류 0%**, 최대 응답 822ms (성공)

SHA-256

보안(NFT-06)

관리자 비밀번호, **SHA-256 해시** 저장 방식 DB에서 확인 (평문 저장 없음)

신뢰성(NFT-07)

정상 쿼리 1000, 공격쿼리 50, 오탐≤5%, 미탐≤2% 확인

신뢰성(NFT-08)

Event 100건 생성, 슬랙과 이메일 100건 전송 확인

Test Results Summary

결론 및 식별된 결함

결론

핵심 탐지 로직(패턴, 행동, 권한) 정상 동작 및 성능 목표 달성

주요 결함 (D-01)

로그 아카이브 기능 미구현 (UT-12, IT-08, ST-08 Fail)

기타 결함 (D-02, D-03)

로그인 실패 처리, 알림 실패 처리 등 세부 예외 처리 미구현 (ST-07, IT-06 Fail)

Future Plans

향후 계획

식별된 결함 보완

D-01, D-02, D-03 결함 수정

미실시 테스트 진행

기능 미구현에 대한 테스트 진행

시스템 고도화

추가 기능 개발 및 최적화

Detailed Defect Analysis

결함 상세 분석

1	**D-01:** 로그 아카이브 기능 미구현 • 영향 범위: UT-12, IT-08, ST-08 • 우선순위: High • 장기 로그 관리 및 스토리지 최적화 필요
2	**D-02:** 로그인 실패 처리 미구현 • 영향 범위: ST-07 • 우선순위: Medium • 사용자 인증 예외 처리 강화 필요
3	**D-03:** 알림 실패 처리 미구현 • 영향 범위: IT-06 • 우선순위: Medium • 알림 전송 실패 시 재시도 로직 추가 필요