1001 Stories

보안 감사 보고서

학습지원 소프트웨어 보안 점검 결과

교육부「학습지원 소프트웨어 선정 기준 및 가이드라인(안)」(2025.12) 대응

문서 유형	보안 감사 보고서
점검 일자	2026년 2월 16일
점검 주체	자동화 보안 감사 시스템 (정적 코드 분석)
대상 시스템	1001 Stories (https://1001stories.seedsofempowerment.org)
운영 주체	Seeds of Empowerment (비영리 교육 플랫폼)
기술 스택	Next.js 15 / PostgreSQL / Prisma ORM / NextAuth.js
점검 범위	인증/인가, 개인정보 처리, AI 연동, 보안 설정

본 보고서는 정적 코드 분석에 기반하며, 동적 침투 테스트를 추가로 권장합니다.

1. 점검 결과 요약

심각도	발견 건수	수정 완료	미수정	비율
CRITICAL	2	0	2	수동 조치 필요
HIGH	6	4	2	67% 수정
MEDIUM	7	1	6	14% 수정
LOW	4	0	4	향후 개선
INFO	3	0	3	참고 사항
합계	22	5	17	23% 수정

2. 즉시 수정된 취약점 (5건)

[F-07] [HIGH] SSE 엔드포인트 CORS 전체 허용

파일: app/api/notifications/sse/route.ts

조치: Access-Control-Allow-Origin을 NEXTAUTH_URL 환경변수로 제한

[F-08] [HIGH] 매직 링크 URL 로그 평문 기록

파일: lib/auth.ts, lib/email.ts

조치: 로그에서 URL 정보 제거, 이메일 주소만 기록

[F-03] [HIGH] 아동 콘텐츠 OpenAI 무단 전송

파일: lib/ai-review-trigger.ts

조치: 미성년자 동의(parentalConsent, aiServiceConsent) 확인 로직 추가

[F-15] [MEDIUM] 도서 직접 등록 API 콘텐츠 미소독

파일: app/api/books/direct-register/route.ts

조치: DOMPurify를 사용한 HTML 소독 적용

[F-18] [HIGH] API 에러 메시지 내부정보 노출

파일: app/api/books/direct-register/route.ts

조치: 에러 응답에서 내부 정보 제거, 일반적 메시지로 교체

3. 추가 조치 필요 사항

[F-01] [CRITICAL] .env.production 내 API 키 하드코딩

권고: 키 교체 및 시크릿 관리 시스템(AWS Secrets Manager 등) 도입 필요

[F-02] [CRITICAL] NEXTAUTH_SECRET 예측 가능한 값

권고: openssl rand -base64 64로 재생성 후 환경변수 업데이트 필요

[F-04] [HIGH] dangerouslySetInnerHTML XSS 위험

권고: 클라이언트 측 렌더링 전 DOMPurify 적용 필요

[F-05] [HIGH] CSP unsafe-inline/unsafe-eval 사용

권고: nonce 기반 CSP 전환 필요 (Next.js 15 지원)

[F-06] [MEDIUM] 리다이렉트 루프 시 인증 우회 가능성

권고: 최대 리다이렉트 횟수 제한 및 에러 페이지 반환으로 변경

[F-09] [MEDIUM] **Rate Limiting 미적용 API 엔드포인트**
권고: 인증, 파일 업로드 API에 Rate Limiting 적용

[F-10] [MEDIUM] **세션 토큰 만료 시간 30일 (과도)**
권고: 교육용 플랫폼 특성상 7일로 단축 권장

[F-11] [MEDIUM] **Prisma raw query 미사용 확인 필요**
권고: 주기적 코드 리뷰로 raw SQL 사용 방지

[F-12] [MEDIUM] **파일 업로드 경로 traversal 검증**
권고: 업로드 파일명 정규화 및 경로 검증 강화

[F-13] [LOW] **HTTP 보안 헤더 추가 권장**
권고: Permissions-Policy, Cross-Origin-* 헤더 추가

[F-14] [LOW] **의존성 패키지 취약점 스캔**
권고: npm audit 정기 실행 및 Dependabot 활성화

[F-16] [LOW] **로그 레벨 프로덕션 설정**
권고: 프로덕션 환경에서 debug 로그 비활성화

[F-17] [LOW] **비밀번호 정책 강화**
권고: 최소 길이, 복잡도 요구사항 추가

[F-19] [INFO] **2FA(다중 인증) 미지원**
권고: 관리자 계정에 TOTP 기반 2FA 도입 권장

[F-20] [INFO] **감사 로그 외부 저장소 백업**
권고: 감사 로그를 별도 저장소에 백업하여 무결성 보장

[F-21] [INFO] **개인정보 접근 로그 분리**
권고: 개인정보 접근 로그를 별도 테이블로 분리 관리

4. 긍정적 보안 소견

COPPA/PIPA 이중 기준 적용
미국 COPPA(만13세)와 한국 개인정보보호법(만14세) 동시 준수

GDPR 제17조 삭제권 완전 구현
소프트삭제 -> 하드삭제 -> 익명화 3단계 구현

bcrypt 해싱 (salt rounds 12)
업계 표준 이상의 패스워드 해싱 강도

Prisma ORM 사용
SQL 인젝션 근본적 방지 (raw query 미사용)

역할 기반 접근 통제 (RBAC)
8개 역할 세분화된 권한 관리

감사 로그 무결성 검증
주요 작업에 대한 감사 로그 기록 및 검증

타이밍 공격 방지
인증 실패 시 일정한 응답 시간 유지

OAuth 계정 연동 보안
기존 계정과 OAuth 자동 연동 차단, 수동 확인 절차

쿠키 보안 설정
HttpOnly, SameSite=Strict, Secure 플래그 설정

CSRF 토큰 검증
NextAuth.js 내장 CSRF 보호 활성화

5. 종합 권고사항

즉시 조치 (CRITICAL)

- API 키 교체 및 시크릿 관리 시스템 도입 (AWS Secrets Manager)
- NEXTAUTH_SECRET 재생성 (openssl rand -base64 64)

단기 조치 (1개월 이내)

- dangerouslySetInnerHTML 사용 부분 DOMPurify 적용
- nonce 기반 CSP 전환
- Rate Limiting 전체 API 적용

중기 조치 (3개월 이내)

- 관리자 계정 2FA 도입
- 감사 로그 외부 백업 시스템 구축
- 동적 침투 테스트 실시
- 의존성 취약점 자동 스캔(Dependabot) 활성화

지속적 관리

- 분기별 보안 감사 실시
- 개인정보 영향 평가(PIA) 정기 수행
- 보안 교육 및 인식 제고

본 보고서는 정적 코드 분석에 기반하며, 동적 침투 테스트를 추가로 권장합니다.
점검 대상: 1001 Stories 플랫폼 소스코드 (Next.js 15, PostgreSQL, Prisma ORM)
점검 기준: OWASP Top 10 (2021), 교육부 학습지원 소프트웨어 가이드라인 (2025.12),
개인정보보호법, 정보통신망법, COPPA, GDPR

문의: Seeds of Empowerment | info@seedsofempowerment.org