

샘플 AI 예약 서비스

외부에서 확인 가능한 기본 보안 위험 점검 리포트

82

기본 양호

점검 대상 https://sample-ai-app.example/	서비스 유형 AI 도구로 제작한 예약 웹앱	주요 기능 회원가입, 로그인, 문의폼, 예약
확인 기술 Next.js, Vercel, Supabase, Cursor	점검 일시 2026년 6월 18일 오후 12:00	점검 방식 비로그인 외부 점검 · 17회 요청

요약

HTTPS와 공개 파일 상태는 양호하지만, 보안 헤더와 개인정보 입력 안내를 먼저 보완하는 것이 좋습니다.

PRIORITY

가장 먼저 확인할 항목

위험도와 조치 효과를 기준으로 최대 3개를 정리했습니다.

01 HSTS 주의

HTTPS 재접속을 강제하는 HSTS 헤더가 없습니다.

권장 조치

HSTS 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.

02 Content Security Policy 주의

스크립트 실행 출처를 제한하는 CSP가 없습니다.

권장 조치

Content Security Policy 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.

03 SameSite 속성 주의

인증 쿠키에 SameSite 속성이 없습니다.

권장 조치

SameSite 속성 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.

MANUAL REVIEW

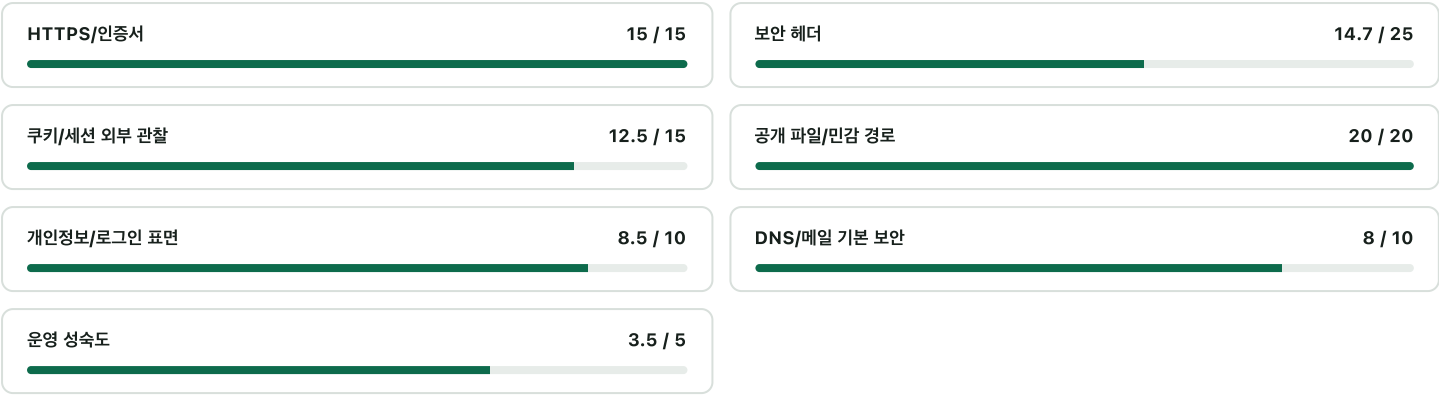
운영자 검토 메모

Supabase 권한은 별도 확인이 필요합니다

외부 도메인 점검만으로 RLS 설정을 확인할 수 없습니다. 실제 사용자 데이터를 받기 전에 프로젝트 콘솔에서 테이블별 RLS 적용 상태를 확인하세요.

영역별 점수

확인할 수 없는 항목은 점수 계산에서 제외했습니다.



DETAILS

점검 결과 상세

항목	결과	관찰 내용과 조치
HTTPS 접속 transport	통과	최종 접속 주소가 HTTPS를 사용합니다. 샘플 관찰값: 설정 확인 조치: HTTPS 접속 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
HTTP에서 HTTPS 이동 transport	통과	HTTP 요청이 HTTPS로 이동합니다. 샘플 관찰값: 설정 확인 조치: HTTP에서 HTTPS 이동 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
인증서 도메인 일치 transport	통과	인증서가 점검 대상 도메인과 일치합니다. 샘플 관찰값: 설정 확인 조치: 인증서 도메인 일치 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
인증서 만료 transport	통과	인증서 만료일까지 67일 남았습니다. 샘플 관찰값: 설정 확인 조치: 인증서 만료 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
HSTS headers	주의	HTTPS 재접속을 강제하는 HSTS 헤더가 없습니다. 샘플 관찰값: 설정 없음 조치: HSTS 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
Content Security Policy headers	주의	스크립트 실행 출처를 제한하는 CSP가 없습니다. 샘플 관찰값: 설정 없음 조치: Content Security Policy 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
클릭재킹 방어 headers	통과	프레임 삽입을 제한하는 정책이 확인되었습니다. 샘플 관찰값: 설정 확인 조치: 클릭재킹 방어 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
MIME 스니핑 방어 headers	주의	X-Content-Type-Options: nosniff가 없습니다. 샘플 관찰값: 설정 없음 조치: MIME 스니핑 방어 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
Referrer 정책 headers	주의	Referrer-Policy가 없습니다. 샘플 관찰값: 설정 없음 조치: Referrer 정책 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.

브라우저 권한 정책 headers	주의	브라우저 권한 제한 정책이 없습니다. 샘플 관찰값: 설정 없음 조치: 브라우저 권한 정책 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
Secure 속성 cookies	통과	확인된 인증 쿠키에 Secure가 적용되어 있습니다. 샘플 관찰값: 설정 확인 조치: Secure 속성 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
HttpOnly 속성 cookies	통과	확인된 인증 쿠키에 HttpOnly가 적용되어 있습니다. 샘플 관찰값: 설정 확인 조치: HttpOnly 속성 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
SameSite 속성 cookies	주의	인증 쿠키에 SameSite 속성이 없습니다. 샘플 관찰값: 설정 없음 조치: SameSite 속성 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
환경변수 파일 노출 exposure	통과	제한된 경로에서 .env 노출 정황을 확인하지 못했습니다. 샘플 관찰값: 설정 확인 조치: 환경변수 파일 노출 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
Git 메타데이터 노출 exposure	통과	제한된 경로에서 Git 메타데이터 노출을 확인하지 못했습니다. 샘플 관찰값: 설정 확인 조치: Git 메타데이터 노출 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
백업/DB 파일 노출 exposure	통과	제한된 경로에서 백업 파일 노출을 확인하지 못했습니다. 샘플 관찰값: 설정 확인 조치: 백업/DB 파일 노출 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
운영체제 메타파일 노출 exposure	통과	제한된 경로에서 메타파일 노출을 확인하지 못했습니다. 샘플 관찰값: 설정 확인 조치: 운영체제 메타파일 노출 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
비밀번호 입력 전송 구간 surface	통과	비밀번호 입력 화면이 HTTPS를 사용합니다. 샘플 관찰값: 설정 확인 조치: 비밀번호 입력 전송 구간 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
개인정보 입력 안내 surface	주의	개인정보 입력 폼 주변에서 안내 링크를 확인하지 못했습니다. 샘플 관찰값: 설정 없음 조치: 개인정보 입력 안내 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
폼 제출 대상 surface	통과	확인된 폼은 동일 출처로 제출됩니다. 샘플 관찰값: 설정 확인 조치: 폼 제출 대상 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
DNS 주소 확인 dns	통과	도메인이 공개 IP 주소로 정상 해석됩니다. 샘플 관찰값: 설정 확인 조치: DNS 주소 확인 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
SPF dns	통과	SPF 레코드가 있습니다. 샘플 관찰값: 설정 확인 조치: SPF 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
DMARC dns	주의	DMARC 정책이 없습니다. 샘플 관찰값: 설정 없음 조치: DMARC 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.
security.txt operations	주의	보안 제보 연락처 파일을 확인하지 못했습니다. 샘플 관찰값: 설정 없음 조치: security.txt 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.

불필요한 서버 식별 헤더가 확인되지 않았습니다.
샘플 관찰값: 설정 확인
조치: 서버 정보 노출 항목을 사용 중인 배포 플랫폼의 설정에서 확인하고 보완하세요.

SCOPE

점검 범위와 한계

- 외부에서 비로그인 상태로 확인 가능한 범위만 점검했습니다.
- 로그인 후 권한, 비즈니스 로직, 소스코드, DB 및 클라우드 설정은 확인하지 않았습니다.
- 관리자 또는 로그인 경로의 존재는 취약점을 의미하지 않습니다.
- 점검 결과는 정식 침투테스트나 보안 인증을 대체하지 않습니다.