CODESCAN

보안 진단 리포트

B

74점

/ 100

0	0	2	1
CRITICAL	HIGH	MEDIUM	LOW

https://example-shop.com

진단일: 2026-07-15 12:35 KST | 리포트 ID: CS-BAD70E2B | 총 발견: 4건

양호 — 일부 보안 헤더/설정 개선이 필요합니다.

본 문서는 리포트 형식 안내용 샘플입니다. 실제 유료 리포트에는 발견된 모든 취약점의 정확한 위치 · 단계별 수정 가이드 · AI 수정 프롬프트가 포함됩니다.

경영진 요약 — Executive Summary

기술적 세부사항 없이 30초 안에 보안 상태를 파악할 수 있도록 작성했습니다.

0	0	2	1
Critical	High	Medium	Low

이 사이트는 B 등급입니다. 양호 — 일부 보안 헤더/설정 개선이 필요합니다.

즉시 조치가 필요한 Critical/High 항목이 없습니다.

방치 시 예상 리스크: 공격 표면 노출 — 복합 공격 위험

핵심 지표 요약

즉시 조치 필요	0건
공격 용이도	낮음 (자동화 공격 도구로 즉시 가능)
예상 영향	공격 표면 노출 — 복합 공격 위험
최우선 위험 항목	Content-Security-Policy 미설정

한 줄 진단

→ 전반적으로 양호하나, 일부 취약점이 고객 신뢰에 영향을 줄 수 있습니다.

카테고리별 점수 분석 — Security Score Breakdown

각 카테고리 점수와 취약점 발견 건수입니다. 80점 이상은 안전, 50점 미만은 즉시 검토가 필요합니다.

카테고리	가중치	점수	바 차트	상태	설명
HTTP 보안 헤더	14%	-		-	미설정 헤더가 XSS·클릭재킹·스니핑 공격 경로가 됩니다.
SSL/TLS 인증서	14%	-		-	만료·취약 암호화는 중간자 공격(MITM) 위험을 높입니다.
시크릿/API키 유출	12%	-		-	소스·응답에서 API키·토큰 노출 여부를 탐지합니다.
Supabase RLS	10%	-		-	Row Level Security 미적용 시 데이터 무단 열람이 가능합니다.
포트 보안	8%	-		-	불필요하게 열린 포트는 서버 침투의 진입점이 됩니다.
디렉토리 노출	8%	-		-	디렉토리 목록 노출은 내부 파일 경로를 그대로 드러냅니다.
에러 정보 노출	8%	-		-	Stack trace 노출은 시스템 구조를 공격자에게 알려줍니다.
쿠키 보안	6%	-		-	HttpOnly·Secure·SameSite 미설정은 세션 탈취 위험입니다.
CORS 설정	6%	-		-	Wildcard CORS는 외부 사이트에서 API 무단 호출을 허용합니다.
API 엔드포인트	6%	-		-	인증 없는 API 엔드포인트는 데이터 유출 위험이 있습니다.
이메일 보안(SPF/DMARC)	4%	-		-	SPF·DMARC 미설정은 피싱 메일 발송 위험을 높입니다.
WAF 탐지	4%	-		-	WAF 부재는 기본적인 공격 필터링이 없음을 의미합니다.
CT 로그/인증서 투명성	0%	-		-	악성 인증서 발급 여부를 모니터링합니다.
유사 도메인 사칭	0%	-		-	브랜드 피싱을 위한 유사 도메인 존재 여부를 탐지합니다.

점수는 해당 카테고리 내 탐지된 취약점 수와 심각도를 기반으로 계산됩니다. 0점은 스캔 불가 또는 해당 없음을 의미할 수 있습니다.

취약점 상세 (4건) — Detailed Findings

각 항목이 유료 리포트에서 어떤 형식으로 제공되는지 보여주는 샘플입니다.

MEDIUM (2건)

1. Content-Security-Policy 미설정

MEDIUM | 긴급도: 단기(1주)

무엇이 문제인가: XSS 공격을 완화하는 CSP 헤더가 없습니다.

유료 리포트에만 포함되는 내용

- 정확한 발견 위치 (URL · 포트 · 경로)
- 실제 위험 시나리오 · 비즈니스 영향
- 단계별 수정 체크리스트
- AI 수정 프롬프트 (Cursor · Claude Code 복붙용)

2. 쿠키 SameSite 속성 미설정

MEDIUM | 긴급도: 단기(1주)

무엇이 문제인가: CSRF 공격에 취약할 수 있습니다.

유료 리포트에만 포함되는 내용

- 정확한 발견 위치 (URL · 포트 · 경로)
- 실제 위험 시나리오 · 비즈니스 영향
- 단계별 수정 체크리스트
- AI 수정 프롬프트 (Cursor · Claude Code 복붙용)

LOW (1건)

3. 서버 버전 정보 노출

LOW | 긴급도: 단기(1주)

무엇이 문제인가: 응답 헤더에 소프트웨어 버전이 노출됩니다.

유료 리포트에만 포함되는 내용

- 정확한 발견 위치 (URL · 포트 · 경로)
- 실제 위험 시나리오 · 비즈니스 영향
- 단계별 수정 체크리스트
- AI 수정 프롬프트 (Cursor · Claude Code 복붙용)

INFO (1건)

4. SSL 인증서 유효

INFO | 긴급도: 단기(1주)

무엇이 문제인가: SSL 인증서가 정상적으로 발급되어 있습니다.

유료 리포트에만 포함되는 내용

- 정확한 발견 위치 (URL · 포트 · 경로)
- 실제 위험 시나리오 · 비즈니스 영향
- 단계별 수정 체크리스트
- AI 수정 프롬프트 (Cursor · Claude Code 복붙용)

수정 우선순위 — Remediation Priority

이번 주에 처리할 5개 항목입니다. 이것만 수정해도 보안 점수가 크게 개선됩니다.

#	취약점 항목	Severity	긴급도	예상 수정 시간	영향도
1	Content-Security-Policy 미설정	중간	단기(1주)	반일~1일	중간
2	쿠키 SameSite 속성 미설정	중간	단기(1주)	반일~1일	중간
3	서버 버전 정보 노출	낮음	단기(1주)	반일~1일	낮음
4	SSL 인증서 유효	정보	단기(1주)	반일~1일	참고

다음 단계 — Next Steps

STEP 1 — 즉시 조치

실제 유료 리포트에서는 발견된 모든 취약점의 정확한 위치와 AI 수정 프롬프트(복붙용)를 제공합니다. 결제 후 바로 조치를 시작할 수 있습니다.

STEP 2 — 재스캔으로 확인

수정 후 codescan.kr에서 같은 URL을 다시 스캔하세요. 무료입니다. 점수 변화를 즉시 확인할 수 있습니다.

STEP 3 — 지속 모니터링 (Pro 구독)

CodeScan Pro는 매일 자동 스캔 후 등급이 떨어지면 즉시 이메일로 알려드립니다. 월 29,900원 · codescan.kr/security/pricing/

STEP 4 — 전문가 심층 진단

자동 스캔으로 찾기 어려운 비즈니스 로직 취약점은 전문가 모의해킹으로 정밀 진단하세요. sentrix.co.kr 문의

리포트 정보

리포트 ID	CS-BAD70E2B
대상 URL	https://example-shop.com
진단일	2026-07-15
재스캔	codescan.kr/security/scan/
문의	support@sentrix.co.kr

CodeScan v2.0 | 21개 보안 카테고리 점검 | 생성: 2026-07-15 21:35 KST