웹사이트 보안 진단 경영 요약 보고서

GitHub · Change is constant. GitHub keeps you ahead. · GitHub

github.com · 진단 ID 2 · 보고서 생성 2026-11-03 15:48

1. 한눈에 보는 진단 결과

SECURITY SCORE

92 / 100

A 등급

치명적	높음	보통	낮음	정보
1	1	6	5	0

분석 결과 웹 보안 종합 점수는 92/100(A 등급)입니다. 기본적인 보안 설정은 대체로 갖추어져 있습니다. 특히 우선순위가 높은 2 개 문제를 먼저 조치하는 것을 권장합니다. 본 결과는 외부 공개정보 기반 비파괴 진단이며, 공개 스캔으로 확인 불가한 6 개 항목은 '확인 불가(NOT_TESTED)'로 별도 표기했습니다.

2. 핵심 리스크와 사업적 의미

순위	발견된 문제	위험도	사업적 의미
1	NULL/EXPORT Cipher 비활성화	치명적	고객 정보 유출·서비스 중단으로 직결될 수 있는 위험
2	취약 Cipher 비활성화	높음	공격 표적이 될 경우 피해 가능성이 높은 위험
3	CSP unsafe-inline	보통	누적 시 신뢰도·검색 노출에 영향을 주는 개선 항목
4	HttpOnly 속성	보통	누적 시 신뢰도·검색 노출에 영향을 주는 개선 항목
5	Source Map 공개	보통	누적 시 신뢰도·검색 노출에 영향을 주는 개선 항목

3. 조치 시 기대 효과

우선순위 상위 3 개 문제를 조치하면 보안 점수는 92 점(A 등급) → 100 점(A 등급)으로 개선될 것으로 예상됩니다.

4. 권고 실행 로드맵 (30 일)

시기	단계	핵심 과제
1 주차	즉시 조치 (높은 위험)	NULL/EXPORT Cipher 비활성화
2 주차	보안 헤더·설정 강화	취약 Cipher 비활성화
3 주차	정보 노출·의존성 정리	CSP unsafe-inline
4 주차	재점검·유지관리	30 일 후 재진단

5. 진단 개요

항목	내용
진단 대상	https://github.com
도메인	github.com
진단 모드	간편 진단 (Public Scan)
진단 일시	2026-09-01 23:54:01
진단 방식	Public Security Scan (비파괴)
진단 페이지 수	6
점검 Rule 수	160 개 (평가 154 · 확인불가 6)
적용 기준	OWASP Top10:2025 / WSTG / CWE / CVE / CVSS 4.0
진단 ID	2

검사 범위 및 한계

본 진단은 인터넷을 통해 공개적으로 접근 가능한 웹사이트 영역을 대상으로 비파괴적 방식으로 수행되었습니다. 관리자 로그인 이후 영역, 계정·권한 취약점, 서버 내부 소스코드·DB·내부 네트워크, SQL Injection·XSS 등 능동 공격, 인증 우회, 파일 업로드 공격, 비즈니스 로직 취약점은 본 Public Scan 의 범위에 포함되지 않습니다. 본 결과는 전체 보안성을 보증하는 인증서가 아니며, 상세 검증이 필요한 경우 별도의 정밀진단을 권장합니다.

보안 개선 상담: ckyoo@web2002.co.kr · 주식회사 쓰리웨이