웹사이트 보안 진단 보고서

Threeway CMS

new.threeway.co.kr · 진단 ID 7 · 보고서 생성 2026-11-03 15:49

1. 진단 개요

항목	내용
진단 대상	https://new.threeway.co.kr
도메인	new.threeway.co.kr
진단 모드	정밀 진단 (Deep Scan · 서버+소스)
진단 일시	2026-09-02 00:53:24
진단 방식	Public Security Scan (비파괴)
진단 페이지 수	31
점검 Rule 수	183 개 (평가 171 · 확인불가 12)
적용 기준	OWASP Top10:2025 / WSTG / CWE / CVE / CVSS 4.0
진단 ID	7

2. 종합 진단 결과

SECURITY SCORE

74 / 100

C 등급

치명적	높음	보통	낮음	정보
3	8	7	9	0

3. 종합 평가

분석 결과 웹 보안 종합 점수는 74/100(C 등급)입니다. 기본 통신 보안은 적용되어 있으나 여러 개선 항목이 확인되었습니다. 특히 우선순위가 높은 11 개 문제를 먼저 조치하는 것을 권장합니다. 본 결과는 외부 공개정보 기반 비파괴 진단이며, 공개 스캔으로 확인 불가한 12 개 항목은 '확인 불가(NOT_TESTED)'로 별도 표기했습니다.

4. 분야별 점수 및 검사 커버리지

진단 분야	점수	평가	커버리지
DNS · 도메인	84 점	양호	14/15
전송 · TLS	55 점	취약	18/20
HTTP 프로토콜	99 점	매우 양호	19/20
보안 응답 헤더	91 점	매우 양호	19/25
쿠키	100 점	매우 양호	10/10
웹 표준 · 공개파일	100 점	매우 양호	9/10
기술스택 · 의존성	99 점	매우 양호	15/15
JavaScript	95 점	매우 양호	15/15

입력 폼	100 점	매우 양호	9/10
정보 노출	96 점	매우 양호	10/10
서드파티 · 공급망	99 점	매우 양호	10/10
서버 환경 (정밀)	81 점	양호	13/13
소스코드 (정밀)	0 점	취약	10/10

※ 커버리지 = 공개 스캔으로 실제 평가한 항목 / 전체 항목. 확인 불가 항목은 점수에서 제외.

5. 주요 발견사항 (우선 조치)

순위	Rule	항목	위험도	결과	근거
1	SRC-001	하드코딩된 Secret/자격증명	치명적	발견 2 건 — index.php:9 일반 API/Secret Key(3d4***	A04:2025 · CWE-798
2	SRC-004	SQL Injection 위험 패턴	치명적	1 곳: index.php:3	A03:2025 · CWE-89
3	TLS-013	NULL/EXPORT Cipher 비활성화	치명적	NULL/EXPORT 지원됨	OWASP A04:2025 · WSTG Weak Cryptography · CWE-327
4	SRC-002	의존성 알려진 취약점(SCA)	높음	express 4.16.0(CVE 3 건, 최고 7.5); jquery 1.12.	A06:2025 · CWE-1035
5	SRC-003	명령 실행 위험 함수	높음	1 곳: index.php:6	A03:2025 · CWE-78
6	SRV-008	호스트 방화벽 활성화	높음	방화벽 상태: inactive	A05:2025 · CWE-284
7	SRC-009	저장소 내 .env/환경 설정 파일	높음	.env (3 개 값: DB_PASSWORD, APP_DEBUG, AWS_KEY.	A04:2025 · CWE-538
8	SRC-005	XSS 위험 패턴	높음	1 곳: index.php:5	A03:2025 · CWE-79

6. 조치 후 예상 점수

현재 **74** 점**(C)** → 우선 **3** 건 조치 후 **100** 점**(A)** **(+26** 점**)**

7. 분야별 상세 점검 결과

DNS · 도메인 — 84 점 · 양호 (평가 14/15)

Rule	항목	상태	위험도	확인된 값	근거
DNS-001	도메인 DNS 조회 가능	통과	-	A/AAAA 4 개	OWASP A02:2025 · WSTG Information Gathering
DNS-002	사설 IP 노출 여부	통과	-	공인 IP 만 반환	OWASP A02:2025 · WSTG Information Gathering · CWE-200
DNS-003	DNSSEC 적용	문제	낮음	DNSKEY 없음	OWASP

	여부			(DNSSEC 미적용)	A08:2025 · WSTG Configuration Testing
DNS-004	SPF 레코드 존재	문제	보통	SPF 없음	OWASP A02:2025 · WSTG Configuration Testing
DNS-005	SPF 과도한 허용	확인 불가	-	SPF 없음	OWASP A02:2025 · WSTG Configuration Testing · CWE-284
DNS-006	DMARC 레코드 존재	문제	보통	DMARC 없음	OWASP A02:2025 · WSTG Configuration Testing
DNS-007	DMARC 보호수준	문제	낮음	policy=없음	OWASP A02:2025 · WSTG Configuration Testing
DNS-008	CAA 레코드 존재	문제	낮음	CAA 없음	OWASP A04:2025 · WSTG Cryptography Testing
DNS-009	NS 이중화	문제	보통	NS 이중화 부족	OWASP A06:2025 · WSTG Configuration Testing
DNS-010	MX 설정 정상	참고	-	MX 없음(메일 미사용 추정)	OWASP A02:2025 · WSTG Information Gathering
DNS-011	와일드카드 DNS 노출	통과	-	와일드카드 없음	OWASP A02:2025 · WSTG Information Gathering
DNS-012	WWW/루트 도메인 일관성	문제	낮음	root/www 응답 불일치	OWASP A02:2025 · WSTG Configuration Testing
DNS-013	CNAME 체인 과다	통과	-	CNAME 체인 0	OWASP A06:2025 · WSTG Information Gathering
DNS-014	Dangling CNAME 징후	통과	-	Dangling CNAME 없음	OWASP A01:2025 · WSTG Configuration Testing · CWE-284

DNS-015	IPv6 서비스 일관성	참고	-	IPv6(AAAA) 있음	OWASP A02:2025 · WSTG Configuration Testing

전송 · **TLS — 55** 점 · 취약 **(평가 18/20)**

Rule	항목	상태	위험도	확인된 값	근거
TLS-001	HTTPS 지원	통과	-	HTTPS(443) 정상	OWASP A04:2025 · WSTG Weak Cryptography · CWE-319
TLS-002	HTTP→HTTPS 강제전환	문제	높음	평문 HTTP 응답	OWASP A04:2025 · WSTG Weak Cryptography · CWE-319
TLS-003	인증서 유효성	통과	-	인증서 유효·신뢰	OWASP A04:2025 · WSTG Weak Cryptography · CWE-295
TLS-004	인증서 만료 임박	통과	-	만료 81 일 전	OWASP A04:2025 · WSTG Weak Cryptography
TLS-005	Hostname 일치	통과	-	hostname 일치	OWASP A04:2025 · WSTG Weak Cryptography · CWE-297
TLS-006	TLS 1.0 비활성화	통과	-	TLS1.0 비활성	OWASP A04:2025 · WSTG Weak Cryptography · CWE-326
TLS-007	TLS 1.1 비활성화	통과	-	TLS1.1 비활성	OWASP A04:2025 · WSTG Weak Cryptography · CWE-326
TLS-008	TLS 1.2 지원	통과	-	TLS1.2/1.3 지원	OWASP A04:2025 · WSTG Weak Cryptography
TLS-009	TLS 1.3 지원	통과	-	TLS1.3 지원	OWASP A04:2025 · WSTG Weak Cryptography
TLS-010	취약 Cipher 비활성화	문제	높음	취약 cipher 지원	OWASP A04:2025 · WSTG Weak Cryptography · CWE-327
TLS-011	RC4 비활성화	확인 불가	-	RC4 테스트 불가 (클라이언트 미지원)	OWASP A04:2025 · WSTG Weak Cryptography · CWE-327

TLS-012	3DES 비활성화	확인 불가	-	3DES 테스트 불가(클라이언트 미지원)	OWASP A04:2025 · WSTG Weak Cryptography · CWE-327
TLS-013	NULL/EXPORT Cipher 비활성화	문제	치명적	NULL/EXPORT 지원됨	OWASP A04:2025 · WSTG Weak Cryptography · CWE-327
TLS-014	인증서 체인 완전성	통과	-	체인 완전	OWASP A04:2025 · WSTG Weak Cryptography · CWE-295
TLS-015	자가서명 인증서 여부	통과	-	자가서명 아님	OWASP A04:2025 · WSTG Weak Cryptography · CWE-295
TLS-016	약한 서명 알고리즘	통과	-	서명 알고리즘 sha256	OWASP A04:2025 · WSTG Weak Cryptography · CWE-327
TLS-017	약한 공개키 크기	통과	-	EC 256bit	OWASP A04:2025 · WSTG Weak Cryptography · CWE-326
TLS-018	OCSP/상태 정보	주의	-	폐기 상태 확인 불가(OCSP 미수집)	OWASP A04:2025 · WSTG Weak Cryptography · CWE-295
TLS-019	SNI 정상 처리	통과	-	SNI 정상	OWASP A02:2025 · WSTG Configuration Testing
TLS-020	Mixed Content	통과	-	혼합 콘텐츠 없음	OWASP A04:2025 · WSTG Client-side Testing · CWE-319

HTTP 프로토콜 — 99 점 · 매우 양호 (평가 19/20)

Rule	항목	상태	위험도	확인된 값	근거
HTTP-001	서버 버전 노출	통과	-	버전 미노출	OWASP A02:2025 · WSTG Information Gathering · CWE-200
HTTP-002	X-Powered-By 노출	문제	낮음	X-Powered-By: PHP/8.4.25, PleskLin	OWASP A02:2025 · WSTG Information Gathering · CWE-200
HTTP-003	TRACE	통과	-	TRACE 비활성	OWASP

	Method				A02:2025 · WSTG Configuration Testing · CWE-749
HTTP-004	불필요 HTTP Method 노출	확인 불가	-	Allow 헤더 없음	OWASP A02:2025 · WSTG Configuration Testing · CWE-749
HTTP-005	HTTP 응답 압축	참고	-	압축 설정 참고	OWASP A06:2025 · WSTG Configuration Testing
HTTP-006	민감 페이지 캐시 방지	통과	-	민감 페이지 미검출	OWASP A02:2025 · WSTG Configuration Testing · CWE-525
HTTP-007	오류 페이지 상태 코드	통과	-	404 상태=404	OWASP A10:2025 · WSTG Error Handling
HTTP-008	5xx 상세정보 노출	통과	-	상세정보 미노출	OWASP A10:2025 · WSTG Error Handling · CWE-209
HTTP-009	Content-Type 명시	통과	-	text/html; charset=UTF-8	OWASP A02:2025 · WSTG Configuration Testing · CWE-436
HTTP-010	Charset 명시	통과	-	charset 명시	OWASP A02:2025 · WSTG Configuration Testing
HTTP-011	Canonical HTTPS URL	참고	-	canonical 없음	OWASP A02:2025 · WSTG Information Gathering
HTTP-012	리다이렉트 체인 과다	통과	-	리다이렉트 과다 아님	OWASP A06:2025 · WSTG Configuration Testing
HTTP-013	외부 오픈 리다이렉트 징후	참고	-	특이 패턴 없음	OWASP A01:2025 · WSTG Input Validation · CWE-601
HTTP-014	Directory Listing 노출	통과	-	디렉터리 리스팅 없음	OWASP A02:2025 · WSTG Configuration

					Testing · CWE-548
HTTP-015	기본 서버 페이지 노출	통과	-	기본 페이지 아님	OWASP A02:2025 · WSTG Configuration Testing · CWE-200
HTTP-016	HTTP/2 또는 최신 프로토콜	참고	-	HTTP/1.1	OWASP A06:2025 · WSTG Configuration Testing
HTTP-017	잘못된 MIME 응답	통과	-	MIME 실행형 불일치 미검출	OWASP A02:2025 · WSTG Configuration Testing · CWE-430
HTTP-018	민감 응답의 public cache	통과	-	민감 응답 public cache 미검출	OWASP A02:2025 · WSTG Configuration Testing · CWE-525
HTTP-019	Referrer 내 민감 Query 징후	통과	-	외부 요청 45 건의 Referer 에 민감 query 없음	OWASP A02:2025 · WSTG Client-side Testing · CWE-598
HTTP-020	robots.txt 민감 경로 노출	통과	-	robots 민감경로 없음	OWASP A02:2025 · WSTG Information Gathering · CWE-200

보안 응답 헤더 — 91 점 · 매우 양호 (평가 19/25)

Rule	항목	상태	위험도	확인된 값	근거
HDR-001	Content-Security-Policy 존재	문제	보통	CSP 없음	OWASP A02:2025 · WSTG Client-side Testing · CWE-693
HDR-002	CSP unsafe-inline	확인 불가	-	CSP 없음	OWASP A02:2025 · WSTG Client-side Testing · CWE-693
HDR-003	CSP unsafe-eval	확인 불가	-	CSP 없음	OWASP A02:2025 · WSTG Client-side Testing · CWE-693
HDR-004	CSP wildcard source	확인 불가	-	CSP 없음	OWASP A02:2025 · WSTG Client-side Testing · CWE-693
HDR-005	CSP object-src 제한	확인 불가	-	CSP 없음	OWASP A02:2025 ·

					WSTG Client-side Testing · CWE-693
HDR-006	CSP base-uri 제한	확인 불가	-	CSP 없음	OWASP A02:2025 · WSTG Client-side Testing · CWE-693
HDR-007	CSP frame-ancestors	확인 불가	-	CSP 없음	OWASP A01:2025 · WSTG Client-side Testing · CWE-1021
HDR-008	HSTS 적용	문제	보통	HSTS 없음	OWASP A04:2025 · WSTG Configuration Testing · CWE-319
HDR-009	HSTS max-age 충분	문제	낮음	max-age 부족 (0)	OWASP A04:2025 · WSTG Configuration Testing
HDR-010	HSTS includeSubDomains	참고	-	includeSubDomains 검토	OWASP A04:2025 · WSTG Configuration Testing
HDR-011	X-Content-Type-Options	통과	-	nosniff	OWASP A02:2025 · WSTG Client-side Testing · CWE-693
HDR-012	Clickjacking 보호	통과	-	SAMEORIGIN	OWASP A01:2025 · WSTG Client-side Testing · CWE-1021
HDR-013	Referrer-Policy	통과	-	strict-origin-when-cross-origin	OWASP A02:2025 · WSTG Client-side Testing · CWE-200
HDR-014	Permissions-Policy	참고	-	Permissions-Policy 없음	OWASP A02:2025 · WSTG Client-side Testing · CWE-693
HDR-015	COOP 설정	참고	-	COOP 없음	OWASP A02:2025 · WSTG Client-side Testing
HDR-016	CORP 설정	참고	-	CORP 없음	OWASP A02:2025 · WSTG Client-side Testing
HDR-017	COEP 설정	참고	-	COEP 없음	OWASP A02:2025 · WSTG Client-side Testing

HDR-018	CORS wildcard	통과	-	와일드카드 아님	OWASP A01:2025 · WSTG Client-side Testing · CWE-942
HDR-019	CORS credentials + wildcard 징후	통과	-	안전	OWASP A01:2025 · WSTG Client-side Testing · CWE-942
HDR-020	CORS Origin 반사 징후	통과	-	Origin 반사 안 함	OWASP A01:2025 · WSTG Client-side Testing · CWE-942
HDR-021	Cache-Control 민감정보	통과	-	민감 응답 캐시 미검출	OWASP A02:2025 · WSTG Configuration Testing · CWE-525
HDR-022	Pragma/ Expires 상충	통과	-	cache 헤더 상충 없음	OWASP A02:2025 · WSTG Configuration Testing
HDR-023	X-XSS-Protection 구형 정책	주의	-	구형 X-XSS-Protection: 1; mode=block	OWASP A02:2025 · WSTG Client-side Testing
HDR-024	Cross-origin isolation 일관성	통과	-	일관	OWASP A02:2025 · WSTG Client-side Testing
HDR-025	보안 헤더 페이지별 일관성	통과	-	페이지 31 개 헤더 일관	OWASP A02:2025 · WSTG Configuration Testing · CWE-693

쿠키 — **100** 점 · 매우 양호 (평가 **10/10**)

Rule	항목	상태	위험도	확인된 값	근거
CK-001	Secure 속성	통과	-	Secure 적용	OWASP A07:2025 · WSTG Session Management · CWE-614
CK-002	HttpOnly 속성	통과	-	HttpOnly 적용	OWASP A07:2025 · WSTG Session Management · CWE-1004
CK-003	SameSite 속성	통과	-	SameSite 설정	OWASP A01:2025 · WSTG Session Management · CWE-1275
CK-004	SameSite=None + Secure	통과	-	정상	OWASP A07:2025 · WSTG Session

					Management · CWE-614
CK-005	Cookie Domain 과다	통과	-	Domain 미지정 (현재 호스트 한정)	OWASP A07:2025 · WSTG Session Management · CWE-565
CK-006	Cookie Path 과다	참고	-	Path=/ 쿠키 1개(관찰)	OWASP A07:2025 · WSTG Session Management
CK-007	Cookie 만료기간 과다	통과	-	쿠키 수명 적정	OWASP A07:2025 · WSTG Session Management · CWE-613
CK-008	Cookie 값 노출 마스킹	통과	-	쿠키 값 마스킹	OWASP A02:2025 · WSTG Session Management · CWE-532
CK-009	세션 쿠키 명명 노출	참고	-	twcms_session	OWASP A02:2025 · WSTG Information Gathering · CWE-200
CK-010	중복/상충 Cookie	통과	-	중복 없음	OWASP A10:2025 · WSTG Session Management

웹 표준 · 공개파일 — **100** 점 · 매우 양호 (평가 **9/10**)

Rule	항목	상태	위험도	확인된 값	근거
WEB-001	robots.txt 존재	통과	-	robots status=200	OWASP A02:2025 · WSTG Information Gathering
WEB-002	sitemap.xml 존재	참고	-	sitemap 없음	OWASP A02:2025 · WSTG Information Gathering
WEB-003	security.txt 존재	참고	-	security.txt 없음	OWASP A06:2025 · WSTG Information Gathering
WEB-004	security.txt 연락처 유효성	확인 불가	-	security.txt 없음	OWASP A06:2025 · WSTG Configuration Testing
WEB-005	외부 링크 HTTPS 비율	통과	-	외부 링크 없음	OWASP A04:2025 · WSTG Client-side Testing · CWE-319
WEB-006	폼 action	통과	-	폼 action https	OWASP

	HTTPS				A04:2025 · WSTG Client-side Testing · CWE-319
WEB-007	비밀번호 입력 페이지 HTTPS	통과	-	정상	OWASP A04:2025 · WSTG Authentication Testing · CWE-319
WEB-008	iframe HTTP 콘텐츠	통과	-	iframe http 없음	OWASP A04:2025 · WSTG Client-side Testing · CWE-319
WEB-009	mailto 공개 이메일	참고	-	공개 이메일 0 개	OWASP A02:2025 · WSTG Information Gathering · CWE-200
WEB-010	페이지 크롤링 오류율	통과	-	크롤 오류율 낮음	OWASP A10:2025 · WSTG Error Handling

기술스택 · 의존성 — 99 점 · 매우 양호 (평가 15/15)

Rule	항목	상태	위험도	확인된 값	근거
TECH-001	웹서버 기술 식별	참고	-	cloudflare (90%)	OWASP A02:2025 · WSTG Information Gathering
TECH-002	백엔드 기술 식별	참고	-	PHP 8.4.25, PleskLin(85%)	OWASP A02:2025 · WSTG Information Gathering
TECH-003	CMS 식별	참고	-	미식별	OWASP A03:2025 · WSTG Information Gathering
TECH-004	프론트엔드 Framework 식별	참고	-	jQuery 3.6.0(95%)	OWASP A03:2025 · WSTG Information Gathering
TECH-005	정확한 버전 노출	문제	낮음	버전 노출: PHP 8.4.25, PleskLin, jQuery 3.6.0	OWASP A02:2025 · WSTG Information Gathering · CWE-200
TECH-006	지원 종료 기술 징후	통과	-	버전 확인된 기술의 지원종료 미검출	OWASP A03:2025 · WSTG Configuration Testing · CWE-1104
TECH-007	Known CVE 정	통과	-	NVD 조회 결과	OWASP

	확매치			영향 CVE 없음 (jQuery 3.6.0)	A03:2025 · WSTG Configuration Testing · CWE-1104
TECH-008	Potential CVE 매치	참고	-	Potential CVE 는 버전 확정 후 정밀진단에서 매칭	OWASP A03:2025 · WSTG Configuration Testing · CWE-1104
TECH-009	오래된 jQuery 징후	통과	-	jQuery 3.6.0	OWASP A03:2025 · WSTG Client-side Testing · CWE-1104
TECH-010	오래된 Bootstrap 징후	통과	-	Bootstrap 미검출/버전불명	OWASP A03:2025 · WSTG Client-side Testing · CWE-1104
TECH-011	Source Map 공개	통과	-	Source Map 미공개	OWASP A02:2025 · WSTG Client-side Testing · CWE-200
TECH-012	Dependency 버전 URL 노출	통과	-	버전 URL 과다 노출 미검출	OWASP A02:2025 · WSTG Information Gathering · CWE-200
TECH-013	CDN 라이브러리 SRI	통과	-	SRI 적용/외부 없음	OWASP A08:2025 · WSTG Client-side Testing · CWE-353
TECH-014	외부 라이브러리 버전 고정	통과	-	외부 의존성 버전 고정	OWASP A08:2025 · WSTG Client-side Testing · CWE-829
TECH-015	Third-party 패키지 과다	참고	-	외부 스크립트 공급자 0 곳	OWASP A03:2025 · WSTG Client-side Testing · CWE-829

JavaScript — 95 점 · 매우 양호 (평가 15/15)

Rule	항목	상태	위험도	확인된 값	근거
JS-001	인라인 Secret 패턴	통과	-	인라인 시크릿 미검출	OWASP A02:2025 · WSTG Client-side Testing · CWE-798
JS-002	API Endpoint 공개 목록	참고	-	공개 JS 내 API 엔드포인트 참고	OWASP A01:2025 · WSTG Information Gathering
JS-003	내부 IP 문자열	통과	-	내부 IP 미검출	OWASP

	노출				A02:2025 · WSTG Information Gathering · CWE-200
JS-004	내부 Hostname 노출	통과	-	내부 호스트명 미검출	OWASP A02:2025 · WSTG Information Gathering · CWE-200
JS-005	개발환경 URL 노출	통과	-	개발 URL 미검출	OWASP A02:2025 · WSTG Information Gathering · CWE-200
JS-006	Console debug 로그	통과	-	콘솔 debug 출력 0 건, 민감정보 없음	OWASP A02:2025 · WSTG Error Handling · CWE-532
JS-007	JavaScript 오류	통과	-	런타임 오류 없음	OWASP A10:2025 · WSTG Error Handling
JS-008	eval 사용 징후	문제	보통	eval() 사용	OWASP A05:2025 · WSTG Client-side Testing · CWE-95
JS-009	document.write 사용	문제	낮음	document.write 사용	OWASP A05:2025 · WSTG Client-side Testing · CWE-79
JS-010	innerHTML 동적 사용 징후	주의	-	innerHTML 동적 사용	OWASP A05:2025 · WSTG Client-side Testing · CWE-79
JS-011	postMessage wildcard 징후	통과	-	postMessage 안전	OWASP A01:2025 · WSTG Client-side Testing · CWE-346
JS-012	localStorage 민감정보 키 징후	통과	-	localStorage 항목 0 건, 민감정보 징후 없음	OWASP A07:2025 · WSTG Client-side Testing · CWE-922
JS-013	sessionStorage 민감정보 징후	통과	-	sessionStorage 항목 0 건, 민감정보 징후 없음	OWASP A07:2025 · WSTG Client-side Testing · CWE-922
JS-014	외부 script HTTP	통과	-	외부 script http 없음	OWASP A04:2025 · WSTG Client-side Testing · CWE-319

JS-015	외부 script 과도 권한	통과	-	외부 script 적정	OWASP A03:2025 · WSTG Client-side Testing · CWE-829

입력 폼 — 100 점 · 매우 양호 (평가 9/10)

Rule	항목	상태	위험도	확인된 값	근거
FORM-001	Password autocomplete 정책	참고	-	autocomplete 정책 참고	OWASP A07:2025 · WSTG Authentication Testing
FORM-002	민감정보 GET 전송	통과	-	GET 민감전송 없음	OWASP A04:2025 · WSTG Input Validation · CWE-598
FORM-003	외부 Domain Form Action	통과	-	외부 action 없음	OWASP A01:2025 · WSTG Client-side Testing · CWE-441
FORM-004	HTTP Form Action	통과	-	form action https	OWASP A04:2025 · WSTG Client-side Testing · CWE-319
FORM-005	Password field HTTP 페이지	통과	-	정상	OWASP A04:2025 · WSTG Authentication Testing · CWE-319
FORM-006	파일 업로드 Form 노출	참고	-	파일 업로드 폼 없음	OWASP A05:2025 · WSTG Input Validation
FORM-007	CSRF token 구조 징후	확인 불가	-	POST 폼 없음	OWASP A01:2025 · WSTG Session Management · CWE-352
FORM-008	민감 Input 이름 노출	참고	-	입력 필드 분류 참고	OWASP A06:2025 · WSTG Information Gathering
FORM-009	Form target=_blank 보호	통과	-	정상	OWASP A06:2025 · WSTG Client-side Testing
FORM-010	입력 제한 속성	참고	-	클라이언트 입력 제한 참고	OWASP A05:2025 · WSTG Input Validation · CWE-20

정보 노출 — 96 점 · 매우 양호 (평가 10/10)

Rule	항목	상태	위험도	확인된 값	근거

EXP-001	Stack Trace 노출	통과	-	스택 트레이스 없음	OWASP A10:2025 · WSTG Error Handling · CWE-209
EXP-002	절대 서버경로 노출	통과	-	서버 경로 미노출	OWASP A02:2025 · WSTG Error Handling · CWE-200
EXP-003	내부 IP 노출	통과	-	내부 IP 없음	OWASP A02:2025 · WSTG Information Gathering · CWE-200
EXP-004	내부 Hostname 노출	통과	-	내부 호스트명 없음	OWASP A02:2025 · WSTG Information Gathering · CWE-200
EXP-005	Debug Mode 징후	통과	-	디버그 징후 없음	OWASP A02:2025 · WSTG Configuration Testing · CWE-489
EXP-006	HTML 주석 민감정보	통과	-	주석 민감정보 없음	OWASP A02:2025 · WSTG Information Gathering · CWE-615
EXP-007	Generator 버전 노출	통과	-	generator 버전 미노출	OWASP A02:2025 · WSTG Information Gathering · CWE-200
EXP-008	공개 Source Map	문제	보통	Source Map 공개	OWASP A02:2025 · WSTG Client-side Testing · CWE-200
EXP-009	개발/테스트 배너 노출	통과	-	배너 없음	OWASP A02:2025 · WSTG Configuration Testing · CWE-489
EXP-010	민감한 공개 문서 링크	통과	-	민감 파일 링크 없음	OWASP A02:2025 · WSTG Configuration Testing · CWE-552

서드파티 · 공급망 — **99** 점 · 매우 양호 (평가 **10/10**)

Rule	항목	상태	위험도	확인된 값	근거
3RD-001	외부 JavaScript	참고	-	외부 JS 0 개	OWASP

	인벤토리				A03:2025 · WSTG Client-side Testing · CWE-829
3RD-002	외부 CSS 인벤토리	참고	-	외부 CSS 2 개	OWASP A03:2025 · WSTG Client-side Testing · CWE-829
3RD-003	외부 iframe 인벤토리	참고	-	외부 iframe 0 개	OWASP A03:2025 · WSTG Client-side Testing · CWE-829
3RD-004	외부 Script SRI	통과	-	SRI 적용/외부 없음	OWASP A08:2025 · WSTG Client-side Testing · CWE-353
3RD-005	외부 CSS SRI	문제	낮음	외부 CSS SRI 누락 2	OWASP A08:2025 · WSTG Client-side Testing · CWE-353
3RD-006	HTTP 외부 리소스	통과	-	http 외부 리소스 없음	OWASP A04:2025 · WSTG Client-side Testing · CWE-319
3RD-007	분석/마케팅 서비스 목록	참고	-	없음	OWASP A06:2025 · WSTG Information Gathering
3RD-008	외부 폰트 서비스	참고	-	fonts.googleapis.com	OWASP A06:2025 · WSTG Information Gathering
3RD-009	외부 Resource Provider 과다	통과	-	공급자 1 곳	OWASP A03:2025 · WSTG Client-side Testing · CWE-829
3RD-010	알 수 없는 외부 Script 출처	통과	-	출처 분류됨	OWASP A03:2025 · WSTG Client-side Testing · CWE-829

서버 환경 (정밀) — 81 점 · 양호 (평가 13/13)

Rule	항목	상태	위험도	확인된 값	근거
SRV-001	운영체제 지원 (EOL) 상태	통과	-	ubuntu 26.04 (지원 중)	A06:2025 · CWE-1104
SRV-002	OS·커널 정보	참고	-	OS ubuntu 26.04 / Kernel 7.0.0-30-generic	-
SRV-003	보안 업데이트 대기	통과	-	대기 중인 보안 업데이트 없음	A06:2025 · CWE-1104

SRV-004	웹서버 버전 알려진 취약점(CVE)	통과	-	nginx 1.30.4: NVD 영향 CVE 없음	A06:2025 · CWE-1035
SRV-005	런타임(PHP/Node/Python) 지원 상태	통과	-	런타임 지원 중: php 8.5.4, python 3.14.4	A06:2025 · CWE-1104
SRV-006	데이터베이스 포트 외부 노출	통과	-	DB 포트 외부 노출 없음	A05:2025 · CWE-284
SRV-007	외부 노출 서비스 수	주의	-	외부 바인딩 포트 17 개	A05:2025 · CWE-1327
SRV-008	호스트 방화벽 활성화	문제	높음	방화벽 상태: inactive	A05:2025 · CWE-284
SRV-009	SSH 안전 설정	통과	-	키 인증 전용 (PasswordAuthentication=no, PermitRootLogin=prohibit-password)	A07:2025 · CWE-309
SRV-010	웹루트 world-writable 파일	통과	-	world-writable 파일 0 개	A05:2025 · CWE-732
SRV-011	컨테이너 위험 설정(privileged)	통과	-	컨테이너 4 개, privileged 0 개	A05:2025 · CWE-250
SRV-012	시간 동기화 (NTP)	통과	-	NTP 동기화: 활성	A09:2025 · CWE-778
SRV-013	디스크 사용률	통과	-	루트 디스크 사용률 71%	CWE-400

소스코드 (정밀) — 0 점 · 취약 (평가 10/10)

Rule	항목	상태	위험도	확인된 값	근거
SRC-001	하드코딩된 Secret/자격증명	문제	치명적	발견 2 건 — index.php:9 일반 API/Secret Key(3d4**********n4"); .env:3 AWS Access Key(AKI**********PLE)	A04:2025 · CWE-798
SRC-009	저장소 내 .env/환경 설정 파일	문제	높음	.env (3 개 값: DB_PASSWORD, APP_DEBUG, AWS_KEY...)	A04:2025 · CWE-538
SRC-003	명령 실행 위험 함수	문제	높음	1 곳: index.php:6	A03:2025 · CWE-78
SRC-004	SQL Injection 위험 패턴	문제	치명적	1 곳: index.php:3	A03:2025 · CWE-89
SRC-005	XSS 위험 패턴	문제	높음	1 곳: index.php:5	A03:2025 · CWE-79
SRC-006	안전하지 않은 역직렬화	문제	높음	1 곳: index.php:7	A08:2025 · CWE-502
SRC-007	약한 해시로 비밀번호 처리	주의	-	1 곳: index.php:8	A02:2025 · CWE-327
SRC-008	디버그 모드 흔적	주의	-	1 곳: .env:1	A05:2025 · CWE-489
SRC-002	의존성 알려진 취약점(SCA)	문제	높음	express 4.16.0(CVE 3 건, 최고 7.5); jquery 1.12.4(CVE 4	A06:2025 · CWE-1035

				건, 최고 6.9)	
SRC-010	SBOM 구성요소 명세	참고	-	SBOM 구성요소 2 개 (composer/npm/pip lock 기준)	A06:2025

8. 서버 및 기술환경

구분	기술	버전	신뢰도	탐지 방식(근거)
web_server	cloudflare	-	90%	Server: cloudflare
backend	PHP	8.4.25, PleskLin	85%	X-Powered-By: PHP/8.4.25, PleskLin
frontend	jQuery	3.6.0	95%	스크립트 경로에서 jQuery 감지

※ 외부 공개정보 기반 추정. (근거: OWASP WSTG 정보수집)

9. 외부 연결 서비스 (서드파티)

서비스	용도	도메인	근거(방식)
Google	Fonts	fonts.googleapis.com	외부 리소스 URL 수집 · OWASP A03:2025

10. 정상적으로 적용된 항목

항목	근거	분야
도메인 DNS 조회 가능	OWASP A02:2025 · WSTG Information Gathering	DNS · 도메인
사설 IP 노출 여부	OWASP A02:2025 · WSTG Information Gathering · CWE-200	DNS · 도메인
와일드카드 DNS 노출	OWASP A02:2025 · WSTG Information Gathering	DNS · 도메인
CNAME 체인 과다	OWASP A06:2025 · WSTG Information Gathering	DNS · 도메인
Dangling CNAME 징후	OWASP A01:2025 · WSTG Configuration Testing · CWE-284	DNS · 도메인
HTTPS 지원	OWASP A04:2025 · WSTG Weak Cryptography · CWE-319	전송 · TLS
인증서 유효성	OWASP A04:2025 · WSTG Weak Cryptography · CWE-295	전송 · TLS
인증서 만료 임박	OWASP A04:2025 · WSTG Weak Cryptography	전송 · TLS
Hostname 일치	OWASP A04:2025 · WSTG Weak Cryptography · CWE-297	전송 · TLS
TLS 1.0 비활성화	OWASP A04:2025 · WSTG Weak Cryptography · CWE-326	전송 · TLS
TLS 1.1 비활성화	OWASP A04:2025 · WSTG Weak Cryptography · CWE-326	전송 · TLS
TLS 1.2 지원	OWASP A04:2025 · WSTG Weak Cryptography	전송 · TLS
TLS 1.3 지원	OWASP A04:2025 · WSTG Weak Cryptography	전송 · TLS
인증서 체인 완전성	OWASP A04:2025 · WSTG Weak Cryptography · CWE-295	전송 · TLS
자가서명 인증서 여부	OWASP A04:2025 · WSTG Weak	전송 · TLS

	Cryptography · CWE-295	
약한 서명 알고리즘	OWASP A04:2025 · WSTG Weak Cryptography · CWE-327	전송 · TLS
약한 공개키 크기	OWASP A04:2025 · WSTG Weak Cryptography · CWE-326	전송 · TLS
SNI 정상 처리	OWASP A02:2025 · WSTG Configuration Testing	전송 · TLS
Mixed Content	OWASP A04:2025 · WSTG Client-side Testing · CWE-319	전송 · TLS
서버 버전 노출	OWASP A02:2025 · WSTG Information Gathering · CWE-200	HTTP 프로토콜
TRACE Method	OWASP A02:2025 · WSTG Configuration Testing · CWE-749	HTTP 프로토콜
민감 페이지 캐시 방지	OWASP A02:2025 · WSTG Configuration Testing · CWE-525	HTTP 프로토콜
오류 페이지 상태코드	OWASP A10:2025 · WSTG Error Handling	HTTP 프로토콜
5xx 상세정보 노출	OWASP A10:2025 · WSTG Error Handling · CWE-209	HTTP 프로토콜
Content-Type 명시	OWASP A02:2025 · WSTG Configuration Testing · CWE-436	HTTP 프로토콜
Charset 명시	OWASP A02:2025 · WSTG Configuration Testing	HTTP 프로토콜
리다이렉트 체인 과다	OWASP A06:2025 · WSTG Configuration Testing	HTTP 프로토콜
Directory Listing 노출	OWASP A02:2025 · WSTG Configuration Testing · CWE-548	HTTP 프로토콜
기본 서버 페이지 노출	OWASP A02:2025 · WSTG Configuration Testing · CWE-200	HTTP 프로토콜
잘못된 MIME 응답	OWASP A02:2025 · WSTG Configuration Testing · CWE-430	HTTP 프로토콜
민감 응답의 public cache	OWASP A02:2025 · WSTG Configuration Testing · CWE-525	HTTP 프로토콜
Referrer 내 민감 Query 징후	OWASP A02:2025 · WSTG Client-side Testing · CWE-598	HTTP 프로토콜
robots.txt 민감 경로 노출	OWASP A02:2025 · WSTG Information Gathering · CWE-200	HTTP 프로토콜
X-Content-Type-Options	OWASP A02:2025 · WSTG Client-side Testing · CWE-693	보안 응답 헤더
Clickjacking 보호	OWASP A01:2025 · WSTG Client-side Testing · CWE-1021	보안 응답 헤더
Referrer-Policy	OWASP A02:2025 · WSTG Client-side Testing · CWE-200	보안 응답 헤더
CORS wildcard	OWASP A01:2025 · WSTG Client-side Testing · CWE-942	보안 응답 헤더
CORS credentials + wildcard 징후	OWASP A01:2025 · WSTG Client-side Testing · CWE-942	보안 응답 헤더
CORS Origin 반사 징후	OWASP A01:2025 · WSTG Client-side Testing · CWE-942	보안 응답 헤더
Cache-Control 민감정보	OWASP A02:2025 · WSTG Configuration Testing · CWE-525	보안 응답 헤더

Pragma/Expires 상충	OWASP A02:2025 · WSTG Configuration Testing	보안 응답 헤더
Cross-origin isolation 일관성	OWASP A02:2025 · WSTG Client-side Testing	보안 응답 헤더
보안 헤더 페이지별 일관성	OWASP A02:2025 · WSTG Configuration Testing · CWE-693	보안 응답 헤더
Secure 속성	OWASP A07:2025 · WSTG Session Management · CWE-614	쿠키
HttpOnly 속성	OWASP A07:2025 · WSTG Session Management · CWE-1004	쿠키
SameSite 속성	OWASP A01:2025 · WSTG Session Management · CWE-1275	쿠키
SameSite=None + Secure	OWASP A07:2025 · WSTG Session Management · CWE-614	쿠키
Cookie Domain 과다	OWASP A07:2025 · WSTG Session Management · CWE-565	쿠키
Cookie 만료기간 과다	OWASP A07:2025 · WSTG Session Management · CWE-613	쿠키
Cookie 값 노출 마스킹	OWASP A02:2025 · WSTG Session Management · CWE-532	쿠키
중복/상충 Cookie	OWASP A10:2025 · WSTG Session Management	쿠키
robots.txt 존재	OWASP A02:2025 · WSTG Information Gathering	웹 표준 · 공개파일
외부 링크 HTTPS 비율	OWASP A04:2025 · WSTG Client-side Testing · CWE-319	웹 표준 · 공개파일
폼 action HTTPS	OWASP A04:2025 · WSTG Client-side Testing · CWE-319	웹 표준 · 공개파일
비밀번호 입력 페이지 HTTPS	OWASP A04:2025 · WSTG Authentication Testing · CWE-319	웹 표준 · 공개파일
iframe HTTP 콘텐츠	OWASP A04:2025 · WSTG Client-side Testing · CWE-319	웹 표준 · 공개파일
페이지 크롤링 오류율	OWASP A10:2025 · WSTG Error Handling	웹 표준 · 공개파일
지원 종료 기술 징후	OWASP A03:2025 · WSTG Configuration Testing · CWE-1104	기술스택 · 의존성
Known CVE 정확매치	OWASP A03:2025 · WSTG Configuration Testing · CWE-1104	기술스택 · 의존성
오래된 jQuery 징후	OWASP A03:2025 · WSTG Client-side Testing · CWE-1104	기술스택 · 의존성
오래된 Bootstrap 징후	OWASP A03:2025 · WSTG Client-side Testing · CWE-1104	기술스택 · 의존성
Source Map 공개	OWASP A02:2025 · WSTG Client-side Testing · CWE-200	기술스택 · 의존성
Dependency 버전 URL 노출	OWASP A02:2025 · WSTG Information Gathering · CWE-200	기술스택 · 의존성
CDN 라이브러리 SRI	OWASP A08:2025 · WSTG Client-side Testing · CWE-353	기술스택 · 의존성
외부 라이브러리 버전 고정	OWASP A08:2025 · WSTG Client-side Testing · CWE-829	기술스택 · 의존성
인라인 Secret 패턴	OWASP A02:2025 · WSTG Client-side Testing · CWE-798	JavaScript
내부 IP 문자열 노출	OWASP A02:2025 · WSTG Information Gathering ·	JavaScript

	CWE-200	
내부 Hostname 노출	OWASP A02:2025 · WSTG Information Gathering · CWE-200	JavaScript
개발환경 URL 노출	OWASP A02:2025 · WSTG Information Gathering · CWE-200	JavaScript
Console debug 로그	OWASP A02:2025 · WSTG Error Handling · CWE-532	JavaScript
JavaScript 오류	OWASP A10:2025 · WSTG Error Handling	JavaScript
postMessage wildcard 징후	OWASP A01:2025 · WSTG Client-side Testing · CWE-346	JavaScript
localStorage 민감정보 키 징후	OWASP A07:2025 · WSTG Client-side Testing · CWE-922	JavaScript
sessionStorage 민감정보 징후	OWASP A07:2025 · WSTG Client-side Testing · CWE-922	JavaScript
외부 script HTTP	OWASP A04:2025 · WSTG Client-side Testing · CWE-319	JavaScript
외부 script 과도 권한	OWASP A03:2025 · WSTG Client-side Testing · CWE-829	JavaScript
민감정보 GET 전송	OWASP A04:2025 · WSTG Input Validation · CWE-598	입력 폼
외부 Domain Form Action	OWASP A01:2025 · WSTG Client-side Testing · CWE-441	입력 폼
HTTP Form Action	OWASP A04:2025 · WSTG Client-side Testing · CWE-319	입력 폼
Password field HTTP 페이지	OWASP A04:2025 · WSTG Authentication Testing · CWE-319	입력 폼
Form target=_blank 보호	OWASP A06:2025 · WSTG Client-side Testing	입력 폼
Stack Trace 노출	OWASP A10:2025 · WSTG Error Handling · CWE-209	정보 노출
절대 서버경로 노출	OWASP A02:2025 · WSTG Error Handling · CWE-200	정보 노출
내부 IP 노출	OWASP A02:2025 · WSTG Information Gathering · CWE-200	정보 노출
내부 Hostname 노출	OWASP A02:2025 · WSTG Information Gathering · CWE-200	정보 노출
Debug Mode 징후	OWASP A02:2025 · WSTG Configuration Testing · CWE-489	정보 노출
HTML 주석 민감정보	OWASP A02:2025 · WSTG Information Gathering · CWE-615	정보 노출
Generator 버전 노출	OWASP A02:2025 · WSTG Information Gathering · CWE-200	정보 노출
개발/테스트 배너 노출	OWASP A02:2025 · WSTG Configuration Testing · CWE-489	정보 노출
민감한 공개 문서 링크	OWASP A02:2025 · WSTG Configuration Testing · CWE-552	정보 노출
외부 Script SRI	OWASP A08:2025 · WSTG Client-side Testing · CWE-353	서드파티 · 공급망
HTTP 외부 리소스	OWASP A04:2025 · WSTG Client-side Testing · CWE-319	서드파티 · 공급망

외부 Resource Provider 과다	OWASP A03:2025 · WSTG Client-side Testing · CWE-829	서드파티 · 공급망
알 수 없는 외부 Script 출처	OWASP A03:2025 · WSTG Client-side Testing · CWE-829	서드파티 · 공급망
운영체제 지원(EOL) 상태	A06:2025 · CWE-1104	서버 환경 (정밀)
보안 업데이트 대기	A06:2025 · CWE-1104	서버 환경 (정밀)
웹서버 버전 알려진 취약점(CVE)	A06:2025 · CWE-1035	서버 환경 (정밀)
런타임(PHP/Node/Python) 지원 상태	A06:2025 · CWE-1104	서버 환경 (정밀)
데이터베이스 포트 외부 노출	A05:2025 · CWE-284	서버 환경 (정밀)
SSH 안전 설정	A07:2025 · CWE-309	서버 환경 (정밀)
웹루트 world-writable 파일	A05:2025 · CWE-732	서버 환경 (정밀)
컨테이너 위험 설정(privileged)	A05:2025 · CWE-250	서버 환경 (정밀)
시간 동기화(NTP)	A09:2025 · CWE-778	서버 환경 (정밀)
디스크 사용률	CWE-400	서버 환경 (정밀)

11. 이번(무료 공개) 진단으로 확인할 수 없는 항목

아래는 공개 스캔으로 확인 불가한 항목입니다. '문제 없음'이 아니라 '미확인'이며 정밀진단에서 점검합니다. (스펙 원칙: NOT_TESTED 는 PASS 로 계산하지 않음)

항목	분야	관련 기준
SPF 과도한 허용	DNS · 도메인	OWASP A02:2025 · WSTG Configuration Testing · CWE-284
RC4 비활성화	전송 · TLS	OWASP A04:2025 · WSTG Weak Cryptography · CWE-327
3DES 비활성화	전송 · TLS	OWASP A04:2025 · WSTG Weak Cryptography · CWE-327
불필요 HTTP Method 노출	HTTP 프로토콜	OWASP A02:2025 · WSTG Configuration Testing · CWE-749
CSP unsafe-inline	보안 응답 헤더	OWASP A02:2025 · WSTG Client-side Testing · CWE-693
CSP unsafe-eval	보안 응답 헤더	OWASP A02:2025 · WSTG Client-side Testing · CWE-693
CSP wildcard source	보안 응답 헤더	OWASP A02:2025 · WSTG Client-side Testing · CWE-693
CSP object-src 제한	보안 응답 헤더	OWASP A02:2025 · WSTG Client-side Testing · CWE-693
CSP base-uri 제한	보안 응답 헤더	OWASP A02:2025 · WSTG Client-side Testing · CWE-693
CSP frame-ancestors	보안 응답 헤더	OWASP A01:2025 · WSTG Client-side Testing · CWE-1021
security.txt 연락처 유효성	웹 표준 · 공개파일	OWASP A06:2025 · WSTG Configuration Testing
CSRF token 구조 징후	입력 폼	OWASP A01:2025 · WSTG Session Management · CWE-352

12. 국제 보안기준

기준	적용	참고 사이트
OWASP Top 10:2025	취약점 상위 위험 분류	https://owasp.org/Top10/2025/
OWASP WSTG Stable	테스트 방법론 연결	https://owasp.org/www-project-web-security-testing-guide/stable/
CWE	취약점 유형 분류	https://cwe.mitre.org/
CVE / NVD	알려진 제품 취약점(정밀진단 연동)	https://www.cve.org/
CVSS 4.0	확인된 CVE 위험도	https://www.first.org/cvss/

13. 진단 결과 요약

양호한 부분

항목	근거
도메인 DNS 조회 가능	OWASP A02:2025 · WSTG Information Gathering
사설 IP 노출 여부	OWASP A02:2025 · WSTG Information Gathering · CWE-200
와일드카드 DNS 노출	OWASP A02:2025 · WSTG Information Gathering
CNAME 체인 과다	OWASP A06:2025 · WSTG Information Gathering
Dangling CNAME 징후	OWASP A01:2025 · WSTG Configuration Testing · CWE-284
HTTPS 지원	OWASP A04:2025 · WSTG Weak Cryptography · CWE-319
인증서 유효성	OWASP A04:2025 · WSTG Weak Cryptography · CWE-295
인증서 만료 임박	OWASP A04:2025 · WSTG Weak Cryptography
Hostname 일치	OWASP A04:2025 · WSTG Weak Cryptography · CWE-297
TLS 1.0 비활성화	OWASP A04:2025 · WSTG Weak Cryptography · CWE-326

개선이 필요한 부분

항목	근거
SPF 레코드 존재	OWASP A02:2025 · WSTG Configuration Testing
DMARC 레코드 존재	OWASP A02:2025 · WSTG Configuration Testing
NS 이중화	OWASP A06:2025 · WSTG Configuration Testing
Content-Security-Policy 존재	OWASP A02:2025 · WSTG Client-side Testing · CWE-693
HSTS 적용	OWASP A04:2025 · WSTG Configuration Testing · CWE-319
eval 사용 징후	OWASP A05:2025 · WSTG Client-side Testing · CWE-95
공개 Source Map	OWASP A02:2025 · WSTG Client-side Testing · CWE-200
DNSSEC 적용 여부	OWASP A08:2025 · WSTG Configuration Testing
DMARC 보호수준	OWASP A02:2025 · WSTG Configuration Testing
CAA 레코드 존재	OWASP A04:2025 · WSTG Cryptography Testing

우선 확인이 필요한 부분

항목	근거
하드코딩된 Secret/자격증명	A04:2025 · CWE-798
SQL Injection 위험 패턴	A03:2025 · CWE-89
NULL/EXPORT Cipher 비활성화	OWASP A04:2025 · WSTG Weak Cryptography · CWE-327
의존성 알려진 취약점(SCA)	A06:2025 · CWE-1035
명령 실행 위험 함수	A03:2025 · CWE-78
호스트 방화벽 활성화	A05:2025 · CWE-284
저장소 내 .env/환경 설정 파일	A04:2025 · CWE-538
XSS 위험 패턴	A03:2025 · CWE-79
안전하지 않은 역직렬화	A08:2025 · CWE-502
HTTP→HTTPS 강제전환	OWASP A04:2025 · WSTG Weak Cryptography · CWE-319

14. 30일 실행 플랜

주차	단계	할 일	상세
1 주차	즉시 조치 (높은 위험)	하드코딩된 Secret/자격증	코드에서 비밀값을 제거하

		명	고 환경변수/Vault 로 이전한 뒤, 노출된 키는 폐기·재발급하세요.
2 주차	보안 헤더·설정 강화	SQL Injection 위험 패턴	문자열 연결 대신 Prepared Statement(바인딩)를 사용하세요.
3 주차	정보 노출·의존성 정리	NULL/EXPORT Cipher 비활성화	NULL/EXPORT Cipher 를 즉시 제거합니다.
4 주차	재점검·유지관리	30 일 후 재진단	동일 기준으로 재진단해 개선폭을 확인하고 설정 유지 여부를 점검하세요.

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