

DL-vScanly

보안 취약점 진단 리포트

자동화 취약점 분석 보고서

프로젝트: 보고서 형식 예시

대상 URL: https://example.com/

스캔 ID: 00000000-0000-4000-8000-000000000001

생성 일시: 2026-10-12T03:00:00Z

리포트 유형: 종합 보고서

통합 위험도 점수

2.0 /100

위험 등급

일부 미평가

CVSS 점수 미평가 2건 · 산정된 부분의 등급: 점수화된 위험 신호 없음. 개별 심각도 · 증적을 함께 확인하세요.

총 발견 항목 수

2

치명·높음

0

수집 페이지

1

URL 위험도 행

1

심각도별 분포



- 치명
- 높음
- 중간
- 낮음
- 참고

0 (0.0%)
0 (0.0%)
1 (50.0%)
1 (50.0%)
0 (0.0%)

요약 · 경영 요약

보고서 형식을 설명하기 위한 가상 데이터 예시이며 실제 사이트의 진단 결과가 아닙니다. 두 가지 보안 헤더의 설정 신호와 조치 방향을 보여줍니다. 실제 운영 적용 전 서비스 구성과 호환성을 확인해야 합니다.

점검 범위와 한계

스캔 유형: 빠른 점검 · 상태: 완료

점검 시각: 2026-10-12T02:59:50Z ~ 2026-10-12T03:00:00Z

발견 항목은 검증이 필요한 자동 탐지 신호입니다. 탐지 신뢰도와 심각도는 다릅니다. 미발견은 안전을 보장하지 않으며, 접근하지 못한 페이지와 설정 범위 밖 항목은 미평가입니다.

위험도 점수는 제품의 참고 지표로 CVSS 점수와 다릅니다. 기준 매핑·비율은 인증이나 준수 판정이 아닙니다. AI 설명은 증거와 함께 검토하세요. 내보내기에서 민감 헤더·인증정보 필드를 마스킹하지만 공유 전 나머지 증거도 확인해야 합니다.

경영 요약

자동 탐지 발견 항목 2건을 정리했습니다. 치명·높음으로 분류된 항목은 없습니다. 2건은 CVSS 점수가 미평가되어 통합 등급을 일부 미평가로 표시합니다. 증거를 확인한 뒤 조치를 계획하세요. 스테이징에서 수정과 주요 기능을 검증하고 해당 항목을 다시 점검하세요.

우선 조치 (Top 2)

아래 순서대로 먼저 처리하세요. 심각도·영향 기준이며, 상세는 본문 취약점 항목을 참고하세요.

#1

[MEDIUM] Content-Security-Policy

필요한 리소스를 목록화하고 스테이징에서 Content-Security-Policy-Report-Only 정책을 검증하세요. 로그인·결제·외부 스크립트 동작을 확인한 후 점진적으로 적용하고 재점검하세요.

#2

[LOW] Strict-Transport-Security

전체 서비스의 HTTPS 지원을 확인하고 짧은 max-age로 검증하세요. 모든 하위 도메인의 HTTPS 준비 없이 includeSubDomains나 preload를 적용하지 마세요.

발견 항목 상세 분석

발견 항목 2건을 증거 기준 2개 그룹으로 정리했습니다. 이 PDF는 심각도순 2개 그룹을 표시합니다. 전체 항목은 JSON 보고서에서 확인하세요.

MEDIUM

#1 Content-Security-Policy

영향 URL

example.com

- https://example.com/

파라미터

Content-Security-Policy

자동 탐지 · 검증 필요 · 탐지 신뢰도: 0.8

1. 요약

수집한 응답에서 CSP 헤더가 확인되지 않았습니다. 브라우저의 리소스 실행 정책을 검토할 필요가 있습니다.

2. 영향도

비즈니스 영향도: MEDIUM

일부 스크립트 삽입 공격에 대한 추가 방어가 부족할 수 있습니다. 이 결과만으로 XSS 취약점이나 공격 성공을 확인한 것은 아닙니다.

3. 다음에 할 일

필요한 리소스를 목록화하고 스테이징에서 Content-Security-Policy-Report-Only 정책을 검증하세요. 로그인 · 결제 · 외부 스크립트 동작을 확인한 후 점진적으로 적용하고 재점검하세요.

4. 기술 상세

탐지 · 점검 방법

수집한 응답 헤더의 설정 점검

5. 점검 근거 · 증거

소스 / 증거 발췌

[response-header] Content-Security-Policy: absent

LOW

#2 Strict-Transport-Security

영향 URL

example.com

- https://example.com/

파라미터

Strict-Transport-Security

자동 탐지 · 검증 필요 · 탐지 신뢰도: 0.8

1. 요약

수집한 HTTPS 응답에서 HSTS 헤더가 확인되지 않았습니다.

2. 영향도

비즈니스 영향도: LOW

브라우저에 HTTPS 연결 정책을 저장하는 추가 방어가 없을 수 있습니다. 실제 영향은 리다이렉트 · 도메인 · 클라이언트 환경에 따라 다릅니다.

3. 다음에 할 일

전체 서비스의 HTTPS 지원을 확인하고 짧은 max-age로 검증하세요. 모든 하위 도메인의 HTTPS 준비 없이 includeSubDomains나 preload를 적용하지 마세요.

4. 기술 상세

탐지·점검 방법

수집한 응답 헤더의 설정 점검

5. 점검 근거·증적

소스 / 증적 발취

[response-header] Strict-Transport-Security: absent

부록

심각도별 분포

치명		0 (0.0%)
높음		0 (0.0%)
중간		1 (50.0%)
낮음		1 (50.0%)
참고		0 (0.0%)

URL 위험도 요약

URL	위험도 %	발견 건수
https://example.com/	—	2

URL 1행 중 1행을 표시합니다. —는 점수 미기록입니다. 전체 행은 JSON 보고서에서 확인하세요.

리포트 본문 구성

각 취약점은 요약 / 위험·영향 / 다음 조치 / (부록) 기술·증적 순입니다. 선택하신 리포트 언어로만 출력합니다.

- 1. 요약 — 무엇인지, 왜 중요한지
- 2. 위험·영향 — 비즈니스 관점
- 3. 조치 — 다음에 할 일(앞쪽 우선 조치 목록)
- 4. 기술 상세 — 개발·보안팀 검토용
- 5. 증적 — 확인 근거
- 6. 부록 — 분포·URL·컴플라이언스