

CodeScan

# 보안 진단 리포트

**https://shop.example.com**

진단 시각: 2026.09.13 09:00 KST

문서 번호: CS-13951B37 / 문서 양식: 2026.09.13

이 문서는 가상 사이트의 설명용 샘플입니다. 실제 진단 결과나 보안 인증이 아닙니다.

| 기록 등급 | 기록 점수    | 발견 기록 |
|-------|----------|-------|
| B     | 74 / 100 | 2건    |

## 이 문서로 할 일

발견 위치와 진단 기록을 확인하고, 실제 서비스에 적용되는지 검토한 뒤 수정 계획을 정합니다. 변경 후에는 재 진단과 정상 기능 테스트를 함께 진행하세요.

등급과 점수는 자동 진단이 기록한 값입니다. 침해 사실, 실제 악용 가능성 또는 서비스 전체의 안전을 증명하지 않습니다. 진단 범위 밖의 로그인 권한·업무 흐름과 점검하지 못한 항목을 함께 고려하세요.

작성·서비스

SENTRIX / codescan.kr

## 경영진 요약

결정에 필요한 범위와 다음 조치를 정리합니다. 검토 순서는 진단에서 부여한 심각도를 기준으로 하며 실제 노출·권한·업무 중요도에 따라 조정하세요.

| 심각 | 높음 | 중간 | 낮음 | 정보 |
|----|----|----|----|----|
| 0  | 0  | 2  | 0  | 0  |

| 확인할 내용         | 현재 기록                   |
|----------------|-------------------------|
| 조치 검토 대상       | 2건 — 실제 영향 확인 후 우선순위 결정 |
| 점검 미완료로 식별된 기록 | 0건 — 연결·실행 문제 복구 후 재점검  |
| 실제 악용 가능성      | 이 자동 진단만으로 확인하지 않음      |
| 법적 적합성·제재 여부   | 이 문서에서 판단하지 않음          |

## 먼저 검토할 항목

조치 계획 · Content-Security-Policy 헤더 미설정

조치 계획 · 쿠키 SameSite 속성 미설정

심각도와 기록만으로 피해가 발생했다고 판단하거나 서비스를 중단하지 마세요. 근거와 업무 영향을 책임자·개발자와 확인해 대응 범위를 정하세요.

## 수정 우선순위와 담당자 결정

1. 우선 검토: 실제 노출·권한·키 유효성 등 영향 조건을 확인합니다.
2. 조치 계획: 변경 담당자, 검증 방법과 되돌리는 방법을 정합니다.
3. 재검증: 재진단 완료 여부와 정상 사용자 기능을 확인하고 결과를 기록합니다.

## 카테고리별 점수 · 기록 범위

기록이 없는 항목은 '기록 없음'으로 표시합니다. 0점은 기록된 점수이며 미점검으로 바꾸지 않습니다. 반대로 높은 점수가 전체 점검 완료나 안전을 보장하지 않습니다.

| 점검 분류          | 기록 점수    |
|----------------|----------|
| HTTP 보안 헤더     | 55 / 100 |
| SSL/TLS        | 95 / 100 |
| 시크릿·API 키      | 기록 없음    |
| Supabase 접근 정책 | 기록 없음    |
| 외부 포트          | 기록 없음    |
| 디렉토리           | 기록 없음    |
| 오류 정보          | 기록 없음    |
| 쿠키             | 50 / 100 |
| CORS           | 기록 없음    |
| API            | 기록 없음    |
| 메일 인증          | 기록 없음    |
| WAF 식별         | 기록 없음    |
| 인증서 공개 기록      | 기록 없음    |
| 유사 도메인         | 기록 없음    |

### 범위 확인

연결 실패·시간 초과·차단으로 진단이 끝나지 않은 항목은 취약점이 없다는 뜻이 아닙니다. 발견 기록의 위치와 시각을 확인하고 필요한 재점검을 진행하세요.

## 취약점 상세 · 발견 기록 2건

진단 엔진이 남긴 기록과 검토용 조치 안내를 구분합니다. 원문 기록의 결론도 실제 환경에서 다시 확인해야 합니다.

### 1. Content-Security-Policy 헤더 미설정

진단 심각도: 중간 / 처리 구분: 조치 계획

#### 발견 위치

https://shop.example.com/ (HTML response header)

#### 진단 기록 (원문)

예시 응답에서 CSP 헤더를 확인하지 못했습니다. 이 관찰만으로 XSS 공격 가능 여부나 다른 방어 수단의 부재를 판단할 수는 없습니다.

#### 진단 엔진의 권장 조치 (원문)

외부 스크립트와 결제·로그인 동선을 확인한 뒤, 보고 전용 정책부터 검증하세요.

#### 검토할 위험 조건

CSP 헤더 미관찰만으로 XSS가 성립한다고 판단할 수 없습니다. 입력 처리와 스크립트 출처를 함께 확인해야 합니다.

#### 업무 영향 검토

보호 설정을 바꾸면 정상 로그인·결제·외부 연동에도 영향을 줄 수 있습니다. 필요한 방어와 정상 기능을 함께 확인하고 변경·복구 범위를 정하세요.

#### 수정·확인 체크리스트

- 실제 스크립트·스타일·폰트·API 출처와 인라인 코드를 정리합니다.
- 시험 환경에서 Report-Only 정책으로 위반을 확인하고 필요한 출처와 nonce/hash 사용을 검토합니다.
- 로그인·결제 기능을 확인한 정책을 적용하고 되돌릴 설정을 준비합니다.

#### 변경 후 검증

정책 헤더와 브라우저 위반 로그를 확인하고 로그인·결제·관리자 동선을 다시 시험합니다.

#### FIX PROMPT · 개발 도구에 전달할 변경 요청

내 웹 서비스의 콘텐츠 보안 정책 항목을 검토해 주세요.

먼저 현재 구현과 관찰 근거를 대조하고, 확인된 사실과 추가 검증이 필요한 가정을 구분해 주세요. 변경 파일과 이유, 영향 받는 정상 동선, 시험 방법, 되돌리는 방법을 제시해 주세요. 운영 배포 전 검토할 수 있는 변경안으로 작성하고 비밀키·쿠키·개인정보 원문은 요청하거나 포함하지 마세요.

검토 방향: 실제 스크립트·스타일·폰트·API 출처와 인라인 코드를 정리합니다. 시험 환경에서 Report-Only 정책으로 위반을 확인하고 필요한 출처와 nonce/hash 사용을 검토합니다. 로그인·결제 기능을 확인한 정책을 적용하고 되돌릴 설정을 준비합니다.

변경 후 확인: 정책 헤더와 브라우저 위반 로그를 확인하고 로그인·결제·관리자 동선을 다시 시험합니다.

## 2. 쿠키 SameSite 속성 미설정

진단 심각도: 중간 / 처리 구분: 조치 계획

### 발견 위치

https://shop.example.com/ (Set-Cookie; value omitted)

### 진단 기록 (원문)

예시 응답 쿠키에 SameSite 속성이 명시되지 않았습니다. 실제 전송 동작은 브라우저 정책과 쿠키 용도에 따라 달라지므로 CSRF 취약점으로 단정하지 않습니다.

### 진단 엔진의 권장 조치 (원문)

세션 쿠키의 용도와 사이트 간 이동을 확인하고 CSRF 방어를 함께 검토하세요.

### 검토할 위험 조건

쿠키의 용도와 브라우저 기본 동작에 따라 영향이 다릅니다. 속성 미설정만으로 세션 탈취나 CSRF를 단정하지 않습니다.

### 업무 영향 검토

보호 설정을 바꾸면 정상 로그인·결제·외부 연동에도 영향을 줄 수 있습니다. 필요한 방어와 정상 기능을 함께 확인하고 변경·복구 범위를 정하세요.

### 수정·확인 체크리스트

1. 세션·분석 등 쿠키별 용도와 발급 지점을 확인합니다.
2. 용도에 맞춰 Secure·HttpOnly·SameSite·Domain·Path를 설정합니다.
3. 외부 로그인과 결제 복귀 흐름, 세션 만료·회전을 함께 검토합니다.

### 변경 후 검증

대상 브라우저에서 쿠키 전송 범위와 로그인·로그아웃·결제 복귀를 확인합니다.

### FIX PROMPT · 개발 도구에 전달할 변경 요청

내 웹 서비스의 쿠키와 세션 설정 항목을 검토해 주세요.

먼저 현재 구현과 관찰 근거를 대조하고, 확인된 사실과 추가 검증이 필요한 가정을 구분해 주세요. 변경 파일과 이유, 영향 받는 정상 동선, 시험 방법, 되돌리는 방법을 제시해 주세요. 운영 배포 전 검토할 수 있는 변경안으로 작성하고 비밀키·쿠키·개인정보 원문은 요청하거나 포함하지 마세요.

검토 방향: 세션·분석 등 쿠키별 용도와 발급 지점을 확인합니다. 용도에 맞춰 Secure·HttpOnly·SameSite·Domain·Path를 설정합니다. 외부 로그인과 결제 복귀 흐름, 세션 만료·회전을 함께 검토합니다.

변경 후 확인: 대상 브라우저에서 쿠키 전송 범위와 로그인·로그아웃·결제 복귀를 확인합니다.

## 수정 우선순위 · 작업 전달

아래 목록을 바탕으로 담당자·기한·검증 결과를 기록하세요. 우선순위는 서비스의 실제 영향과 변경 위험을 검토해 정합니다.

### 1. 조치 계획 / Content-Security-Policy 헤더 미설정

담당자: \_\_\_\_\_ 확인 기한: \_\_\_\_\_  
검증 결과·근거: \_\_\_\_\_

### 2. 조치 계획 / 쿠키 SameSite 속성 미설정

담당자: \_\_\_\_\_ 확인 기한: \_\_\_\_\_  
검증 결과·근거: \_\_\_\_\_

## 다음 단계 · 검증 범위 결정

### 개발팀에서 수정할 수 있는 경우

원문 근거와 환경을 확인하고 검토된 변경안을 시험 환경에서 적용하세요. 재진단에서 점검이 완료됐는지와 로그인·결제 등 정상 동작을 함께 확인하세요.

### 전문가의 검증이 필요한 경우

로그인 이후 권한·결제 흐름: SENTRIX AI 모의해킹(AI 탐색 + 레드팀 검증, 범위별 견적). 진단 근거 검토 후 범위·산출물·일정 합의하고 착수.

[SENTRIX AI 모의해킹 범위 상담 신청](#)

### 기업 외부 자산을 계속 관리해야 하는 경우

회사 도메인 전체 외부 자산: SENTRIX ASM. 등록된 자산의 반복 점검·담당자·조치 기한 관리는 Continuous에서 이어감.

[SENTRIX ASM 안내 보기](#)

[등록 자산의 반복 점검 · Continuous →](#)

### 공유와 해석

문서에는 내부 경로·구성·민감한 발견 위치가 포함될 수 있습니다. 필요한 담당자에게만 전달하고 공개 링크나 개발 도구에 비밀값을 붙이지 마세요. 이 문서는 보안 인증, 법률 의견, 침해 사고 판정 또는 모든 취약점의 부재를 보증하는 문서가 아닙니다.

### 판단·검증 참고 문서

MDN CSP: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP>

MDN CORS: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CORS>

Supabase RLS: <https://supabase.com/docs/guides/database/postgres/row-level-security>

OWASP Authorization: [https://cheatsheetseries.owasp.org/cheatsheets/Authorization\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html)

FIRST CVSS: <https://www.first.org/cvss/user-guide>