

보안 진단 결과 보고서

STRICTLY CONFIDENTIAL

대외비 · 지정 수신자 한정

고객사 A

진단 대상: 고객사 A

작성: FELSEN Security

발행일: 2026.10.14

공개용 익명 발췌본

비밀유지 및 정보보호

WARNING · 무단 열람·복제·배포 금지

본 보고서는 **고객사 A와 고객사 A가 승인한 담당자만 열람할 수 있는 기밀 자료**입니다. 시스템 구성, 취약점 및 재현 절차 등 외부에 공개되어서는 안 되는 정보를 포함하고 있습니다.

고객사 A의 사전 서면 승인 없이 본 보고서의 전부 또는 일부를 복제하거나, 제3자에게 전달·공유·공개하는 행위를 금합니다. 내용을 발췌하여 배포하거나 외부 서비스에 업로드하는 행위도 이에 포함됩니다.

무단 공개나 목적 외 사용으로 손해가 발생할 경우 관련 법령 및 계약에 따라 책임을 질 수 있습니다. 수신 권한이 없다면 열람과 사용을 중단하고, 발신자에게 알린 뒤 모든 사본을 삭제해 주십시오.

※ 본 파일은 고객 정보를 삭제한 공개용 익명 발췌본입니다. 위 안내는 정식 보고서의 기밀 취급 문구입니다.

목차

비밀유지 및 정보보호	2
목차	3
경영진 요약	4
1.1 개요	4
1.2 주요 점검 결과	4
1.3 개선 사항	4
점검 범위 및 방법	5
2.1 점검 대상	5
2.2 점검 방법	5
점검 항목 및 결과	6
1. 기본 구성 및 설정	6
기술 상세 분석	7
FLS-WEB-001: HSTS 헤더 미설정	7
위험도 · 영향 · 개선 권고	8
FLS-WEB-002: 입력 형식 검증 미흡	8

상세 결과와 증적 중 공개하지 않은 부분은 본문에 “...중략...”으로 표시했습니다.

경영진 요약

1.1 개요

고객사 A의 공개 웹 애플리케이션을 외부 사용자 관점에서 점검했습니다. 웹 응답, 입력값 처리, 관리 화면과 인증 절차를 살펴봤으며, 관리자 계정과 소스 코드 없이 블랙박스 방식으로 진행했습니다.

1.2 주요 점검 결과

점검한 범위에서 다음 사항을 확인했습니다.

- **HTTPS 전환:** HTTP 접속은 HTTPS로 전환되었습니다.
- **관리자 인증:** 로그인 화면은 외부에 노출되어 있었습니다. 비로그인 상태에서 관리자 기능을 실행하거나 인증을 우회한 사례는 확인되지 않았습니다.
- **오류 메시지:** 입력 오류 응답에 내부 경로나 스택 정보는 노출되지 않았습니다.

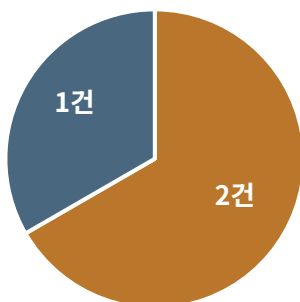
...중략...

1.3 개선 사항

낮은 위험도의 취약점 2건과 참고 사항 1건을 수록했습니다. HSTS 헤더 미설정, 잘못된 자료형 입력 시 HTTP 500/503 오류, 관리 화면의 외부 노출에 관한 내용입니다.

입력값 검증과 예외 처리를 보완하고, HTTPS가 정상 운영되는지 확인한 뒤 HSTS를 적용하도록 권고했습니다. 관리 화면의 외부 공개가 필요한지도 검토할 수 있습니다.

공개본 수록 결과



취약점 2건 · 참고 사항 1건

- **낮음 2건 · 66.7%**
HSTS 미설정, 입력 형식 검증 미흡
- **참고 1건 · 33.3%**
관리 화면의 외부 노출

발체본에 수록한 3건 기준이며, 참고 사항은 취약점 수에 포함하지 않았습니다.

점검 범위 및 방법

2.1 점검 대상

점검 대상 정보는 다음과 같으며, 주소와 시스템명은 익명 처리했습니다.

- **대상 URL:** <https://portal.example.invalid/>
- **대상 구성:** 공개 웹 애플리케이션, 웹서버, 콘텐츠 관리 기능
- **점검 조건:** 외부 사용자 관점 / 관리자 계정과 소스 코드 미제공

제외 항목: 이 발책본의 점검 범위에는 서비스 거부·부하 테스트, 내부망 점검, 소스 코드 분석, 사회공학, 제 3자 운영 시스템을 포함하지 않았습니다.

2.2 점검 방법

정상 요청의 응답 코드와 헤더, 화면 동작을 기록한 뒤 입력값과 접근 경로를 하나씩 바꿔 결과를 비교했습니다. 자동화 도구가 탐지한 항목은 수동으로 재확인하고, 현상만 확인한 경우와 실제 영향을 입증한 경우를 구분했습니다.

- 대표 페이지와 정적 파일의 HTTP·HTTPS 응답 및 보안 헤더 확인
- 폼과 파라미터에 자료형이 다른 값을 입력했을 때 오류 처리 확인
- 로그인하지 않고 볼 수 있는 관리 화면의 정보와 기능 확인

...중략...

※ 위 주소는 설명용 예시입니다. 실제 주소, 계정과 진단 일정은 공개하지 않습니다.

점검 항목 및 결과

주요 점검 항목과 방법, 결과를 아래 표에 정리했습니다.

1. 기본 구성 및 설정

점검 항목	설명	방법 / 도구	상태 / 결과
HTTPS 전환	HTTP 요청이 HTTPS로 전환되는지 확인.	브라우저, HTTP 요청 비교	확인: HTTP 요청은 HTTPS 주소로 전환됨.
HSTS 정책	대표 페이지와 정적 파일의 HSTS 헤더 확인.	응답 헤더 분석	낮음: HSTS 헤더 미설정. 상세 분석: FLS-WEB-001
입력값 자료형	문자열 입력 필드에 배열 등 다른 자료형 전송.	폼 요청 수정, 응답 비교	낮음: 일부 입력에 HTTP 500/503 오류 반환. 지속적인 장애는 확인되지 않음.
관리 화면	로그인 전 관리 화면에 접근할 수 있는지 확인.	브라우저, 수동 요청	참고: 로그인 화면과 일부 기능 정보 노출. 관리자 인증 우회는 확인되지 않음.

...중략...

“확인되지 않음”은 이번 점검에서 해당 영향을 입증하지 못했다는 뜻입니다. 시스템 전체가 안전하다거나 점검하지 않은 항목에 문제가 없다는 의미는 아닙니다.

기술 상세 분석

FLS-WEB-001: HSTS 헤더 미설정

해당 위치:

- 공개 웹 페이지: [/, /company/, /downloads/](/company/)
- 정적 파일: </assets/> 경로의 공개 파일

설명

일부 HTTPS 응답에 Strict-Transport-Security 헤더가 설정되어 있지 않았습니다. HSTS는 브라우저가 일정 기간 해당 호스트에 HTTPS로만 접속하도록 지정하는 정책입니다.

HTTP에서 HTTPS로의 전환은 정상 작동했습니다. 다만 HSTS 정책이 저장되지 않은 브라우저에서는 최초 접속 시 HTTP 요청이 먼저 전송될 수 있습니다. 공격자가 통신 경로를 제어할 수 있다면, HTTPS 전환 전의 HTTP 통신을 방해하거나 변조할 가능성이 있습니다.

...중략...

상세 분석 및 재현 예시

1단계: 대표 페이지의 HTTPS 응답 확인

정상 응답의 헤더에서 HSTS 설정 여부를 확인했습니다. 아래는 고객 정보를 제거하고 재구성한 응답 예시입니다.

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: private, no-store
X-Content-Type-Options: nosniff

Strict-Transport-Security: 헤더 없음
```

...중략...

기술 상세 분석 (계속)

위험도 평가

위험도: 낮음

영향

HSTS 정책이 저장되지 않은 브라우저가 HTTP로 처음 접속할 때, 통신 경로를 제어하는 공격자가 HTTPS 전환을 방해할 수 있습니다. HSTS 미설정만으로 HTTPS 암호화가 무력화되거나 실제 정보가 유출됐다고 판단할 수는 없습니다.

개선 권고

- **HSTS 설정:** 웹서버 또는 리버스 프록시에서 대상 HTTPS 응답에 HSTS 헤더가 빠짐없이 포함되도록 설정합니다.
- **하위 도메인 점검:** 모든 하위 도메인에서 HTTPS가 정상 동작하는지 확인한 뒤 includeSubDomains를 적용합니다.
- **HTTPS 전환 유지:** HSTS 적용 후에도 기존 HTTP → HTTPS 전환을 유지합니다.

...중략...

FLS-WEB-002: 입력 형식 검증 미흡

설명

문자열 입력 필드에 배열을 전송하자 HTTP 503 오류가 반환되었습니다. 일부 잘못된 형식의 입력에서는 HTTP 500 오류도 발생했습니다. 오류 응답에 내부 경로나 스택 정보는 노출되지 않았으며, 지속적인 서비스 장애는 확인되지 않았습니다.

서버에서 입력값의 자료형과 허용 범위를 먼저 검증하고, 잘못된 요청에는 정해진 4xx 응답을 반환하도록 권고했습니다.

...중략...