EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sia.ailem.app/dashboard/login	Checks	9 pruebas
Dominio	sia.ailem.app	Hallazgos	50 totales
Fecha	25 de mayo de 2026 a las 18:29	Problemas	12 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 57/100, lo que equivale a una nota D. Durante la auditoría se ejecutaron un total de 9 checks pasivos, resultando en 4 verificaciones correctas, 3 advertencias y 2 fallos críticos. Se detectaron deficiencias significativas en la configuración de cabeceras de seguridad y en la redirección obligatoria hacia protocolos cifrados. Debido a la ausencia de protecciones fundamentales contra ataques comunes y la exposición de servicios de administración, el sitio se considera actualmente vulnerable y con un nivel de riesgo moderado-alto.

Resumen de Riesgos

0	6	4	2	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 80 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  80 dias restantes (expira: 2026-08-13T10:39:23.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-15T10:39:24.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: openresty — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 302 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: sia_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: sia_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: sia_session — SameSite**
  SameSite=lax

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- INFO **Puerto 3306 (MySQL)**
  Cerrado — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto

- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Falta de Content-Security-Policy: Facilita la ejecución de ataques XSS y la inyección de contenido malicioso en el navegador del usuario.
[HIGH] Falta de X-Frame-Options: Permite ataques de clickjacking, donde un atacante puede engañar al usuario para que realice acciones no deseadas.
[HIGH] Falta de Strict-Transport-Security: No obliga al navegador a usar siempre conexiones seguras, permitiendo ataques de degradación de protocolo.
[HIGH] Redirección HTTP a HTTPS fallida: El tráfico no cifrado no se redirige automáticamente, dejando los datos expuestos a interceptación en redes públicas.
[HIGH] Cookie XSRF-TOKEN sin flag HttpOnly: Permite que scripts maliciosos lean el token de sesión, aumentando drásticamente el riesgo de secuestro de cuenta.
[MEDIUM] Falta de X-Content-Type-Options: El sitio es susceptible a ataques de sniffing de tipo MIME, lo que podría llevar a la ejecución de archivos maliciosos.
[MEDIUM] Falta de Referrer-Policy: No se controla la información de origen que se envía a terceros, lo que puede filtrar URLs privadas o sensibles.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el acceso de las APIs del navegador a funciones de hardware como cámara o micrófono.
[MEDIUM] Puerto 22 (SSH) abierto: La exposición pública de este puerto invita a ataques de fuerza bruta contra el acceso administrativo del servidor.
[LOW] Server header expuesto (openresty): Revela la tecnología exacta del servidor, ayudando a posibles atacantes a buscar vulnerabilidades específicas.
[LOW] sitemap.xml no encontrado: La ausencia de este archivo dificulta la auditoría de la estructura del sitio y la indexación controlada.