EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://i-t-ai-director-suite.ai.studio	Checks	9 pruebas
Dominio	i-t-ai-director-suite.ai.studio	Hallazgos	48 totales
Fecha	27 de septiembre de 2026 a las 03:38	Problemas	17 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio i-t-ai-director-suite.ai.studio ha resultado en una puntuación de 62/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 fueron satisfactorios, 1 generó advertencias y 3 fallaron de forma crítica. Los resultados indican que, si bien existe una base de seguridad funcional, la ausencia total de cabeceras de protección y la gestión deficiente de cookies representan riesgos significativos. En su estado actual, el sitio se considera vulnerable a ataques de interceptación de datos y manipulación de sesiones.

Resumen de Riesgos

0	6	9	2	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 68 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	0	FALLO	GAESA: falta HttpOnly; GAESA: falta Secure; GAES...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 68 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  68 dias restantes (expira: 2026-12-03T19:21:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-10T19:22:00.000Z
- 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: Google Frontend — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Express — Revela framework/lenguaje
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://i-t-ai-director-suite.ai.studio/
- 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**
  Express

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 0/100

Estado: FALLO

GAESA: falta HttpOnly; GAESA: falta Secure; GAESA: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: GAESA — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: GAESA — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: GAESA — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- INFO **Puerto 22 (SSH)**
  Cerrado — 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] Ausencia de Content-Security-Policy: La falta de esta cabecera permite ataques de inyección de contenido y ejecución de scripts maliciosos (XSS).
[HIGH] Falta de X-Frame-Options: El sitio no previene ataques de clickjacking, lo que podría permitir que atacantes engañen a los usuarios dentro de marcos invisibles.
[HIGH] Strict-Transport-Security no configurado: No se fuerza al navegador a utilizar exclusivamente conexiones HTTPS, facilitando ataques de degradación de SSL.
[HIGH] Cookie GAESA sin flag HttpOnly: Esta cookie de sesión es accesible mediante scripts, aumentando drásticamente el riesgo de robo de identidad en ataques XSS.
[HIGH] Cookie GAESA sin flag Secure: La información de sesión se transmite a través de canales no cifrados, permitiendo su intercepción en redes locales o públicas.
[MEDIUM] Cookie GAESA sin flag SameSite: La ausencia de este atributo hace que el sitio sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] X-Content-Type-Options faltante: El navegador podría intentar adivinar el tipo de contenido, lo que permite la ejecución de archivos maliciosos disfrazados de otros tipos.
[MEDIUM] Referrer-Policy no definida: Se corre el riesgo de filtrar información privada de la URL de origen a sitios externos de terceros.
[MEDIUM] Permissions-Policy ausente: No se restringe el acceso de la aplicación a funciones sensibles del hardware del usuario como cámara o micrófono.
[MEDIUM] Archivos técnicos expuestos: Se detectó acceso público a /readme.html y /README.txt, los cuales pueden revelar detalles internos de la infraestructura.
[MEDIUM] Rutas administrativas accesibles: Los paneles de login en /wp-login.php, /administrator/ y /user/login están expuestos a ataques de fuerza bruta.
[LOW] Exposición de tecnología en cabecera Server: El servidor revela el uso de Google Frontend, proporcionando pistas útiles para un atacante.
[LOW] Cabecera X-Powered-By expuesta: Se confirma el uso del framework Express, lo que permite buscar vulnerabilidades específicas para dicha tecnología.
[LOW] Ausencia de archivos de indexación: No se encontraron robots.txt ni sitemap.xml, lo que dificulta la gestión del rastreo y seguridad de rutas.