EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://iamantis.com	Checks	9 pruebas
Dominio	iamantis.com	Hallazgos	39 totales
Fecha	28 de abril de 2026 a las 15:13	Problemas	8 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio iamantis.com ha resultado en una puntuación de 71/100, obteniendo una nota de C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 generó una advertencia y 2 presentaron fallos críticos. Aunque el sitio cuenta con elementos base de seguridad, la ausencia de capas de protección modernas y errores en la configuración de cifrado comprometen su integridad. Se concluye que el sitio es vulnerable ante ataques de inyección y suplantación de identidad debido a estas carencias técnicas.

Resumen de Riesgos

0	2	3	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 29 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	100	OK	No se encontraron cookies
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	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 29 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  29 dias restantes (expira: 2026-05-28T01:53:30.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-27T01:53:31.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.29.3 — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- 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.)

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

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 — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

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

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 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)**
  Cerrado — 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

[WARN] SSL/TLS: El certificado de seguridad expira en 29 días, lo que representa un riesgo de pérdida de confianza y acceso si no se renueva a corto plazo.
[HIGH] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de esta política deja el sitio desprotegido contra ataques de clickjacking, permitiendo que sea cargado en marcos externos.
[MEDIUM] X-Content-Type-Options: No se detectó esta cabecera, lo que permite que los navegadores realicen MIME-type sniffing y ejecuten archivos con formatos incorrectos.
[MEDIUM] Referrer-Policy: Falta esta configuración, lo que implica un control nulo sobre la información de navegación que se envía a sitios terceros.
[MEDIUM] Permissions-Policy: Ausente, lo que significa que no se restringe el acceso de las APIs del navegador a funciones sensibles como cámara o geolocalización.
[ERROR] Redirección HTTPS: No se pudo verificar la redirección automática de tráfico no cifrado, lo que podría exponer datos de usuarios en tránsito.
[LOW] Server header expuesto: El servidor revela la versión exacta de nginx/1.29.3, facilitando a posibles atacantes la búsqueda de exploits específicos para ese software.
[LOW] Archivos de indexación faltantes: No se encontraron robots.txt ni sitemap.xml, lo que dificulta la gestión del rastreo y puede exponer rutas internas a motores de búsqueda.