EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.ids.alinet.cu	Checks	9 pruebas
Dominio	www.ids.alinet.cu	Hallazgos	15 totales
Fecha	1 de junio de 2026 a las 14:34	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha arrojado una puntuación de 73/100, obteniendo una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 1 resultó satisfactorio y 1 fue clasificado como fallo técnico directo. El análisis se vio severamente limitado por errores de conexión que impidieron validar componentes críticos como el cifrado y las cabeceras de seguridad. Debido a la imposibilidad de verificar la integridad del protocolo SSL y la configuración del servidor, el sitio se considera vulnerable en su estado actual. Se requiere una intervención técnica inmediata para normalizar la visibilidad y seguridad de la plataforma.

Resumen de Riesgos

1	0	0	2	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder
- BAJO **sitemap.xml**
  Error al acceder

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — 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

[CRITICAL] Conexion SSL: No se pudo establecer una conexión SSL/TLS válida, lo que impide el cifrado de la información y expone los datos de los usuarios.
[LOW] Ausencia de archivos de indexación: No se detectó acceso a robots.txt ni sitemap.xml, lo que dificulta la gestión de rastreo y transparencia del sitio.
[ERROR] Cabeceras de seguridad: El escáner no pudo verificar la presencia de políticas de seguridad en las cabeceras, aumentando el riesgo de ataques XSS o inyecciones.
[ERROR] Redirección HTTPS: No se ha podido confirmar si el tráfico no cifrado se redirige automáticamente a una conexión segura.
[ERROR] Seguridad de Cookies: La falta de acceso a la configuración de cookies impide validar si contienen los atributos Secure y HttpOnly necesarios para proteger sesiones.