EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Hardsofmair.com	Checks	9 pruebas
Dominio	hardsofmair.com	Hallazgos	15 totales
Fecha	20 de junio de 2026 a las 08:48	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio Hardsofmair.com ha resultado en una puntuación de 73/100, lo que equivale a una nota C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 1 finalizó correctamente, se registraron 0 advertencias y se confirmó 1 fallo directo. Debido a la imposibilidad de verificar parámetros críticos como el cifrado de datos y las cabeceras de protección, el sitio se clasifica actualmente como vulnerable. Es imperativo solucionar los errores de conectividad y configuración detectados para garantizar un entorno de navegación mínimo aceptable.

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] Fallo en conexión SSL/TLS: No se pudo establecer una conexión segura, lo que impide garantizar la confidencialidad de los datos transmitidos entre el usuario y el servidor.
[LOW] Ausencia de archivos de indexación: No se detectaron los archivos robots.txt ni sitemap.xml, lo que compromete la visibilidad estructurada y puede exponer rutas internas de forma no intencionada.
[MEDIUM] Cabeceras de seguridad no verificables: La falta de respuesta en las cabeceras HTTP impide confirmar la protección contra ataques de Clickjacking, XSS o inyección de contenido.
[MEDIUM] Configuración de cookies indeterminada: La imposibilidad de analizar las cookies de sesión impide confirmar si los datos del usuario viajan con los atributos de seguridad necesarios.