EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Hardsoftmair.com	Checks	9 pruebas
Dominio	hardsoftmair.com	Hallazgos	47 totales
Fecha	20 de junio de 2026 a las 08:49	Problemas	16 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio Hardsoftmair.com ha arrojado una puntuación de 53/100, lo que equivale a una calificación de grado D. Durante el análisis, se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 generó una advertencia y 3 fallaron críticamente. Se han identificado brechas importantes en la configuración del servidor y en la exposición de servicios sensibles que comprometen la integridad de la plataforma. Debido a la presencia de puertos de bases de datos abiertos y la falta de cabeceras de seguridad esenciales, el sitio se clasifica actualmente como vulnerable.

Resumen de Riesgos

1	7	5	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 58 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	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.0 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 58 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  58 dias restantes (expira: 2026-08-17T15:34:10.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-19T15:34:11.000Z
- 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: LiteSpeed — 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 200 — 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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 7.0
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (319 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://hardsoftmair.com/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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] Puerto 3306 (MySQL): La base de datos se encuentra abierta al acceso público, lo que permite intentos de conexión externa y ataques de fuerza bruta directos.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos activo sin cifrar, lo que expone credenciales y datos en tránsito a ataques de interceptación.
[HIGH] Redirección HTTPS: El sitio permite conexiones HTTP sin redirigir automáticamente a la versión segura, facilitando ataques de hombre en el medio (MitM).
[HIGH] Versión de WordPress expuesta: Se detecta públicamente la versión del CMS, lo que permite a atacantes identificar y explotar vulnerabilidades específicas conocidas (CVE).
[HIGH] Content-Security-Policy (CSP): La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido o XSS.
[HIGH] X-Frame-Options: La falta de esta configuración hace que el sitio sea susceptible a ataques de clickjacking, donde un atacante puede camuflar la interfaz.
[HIGH] Strict-Transport-Security (HSTS): No existe una política que obligue al navegador a comunicarse siempre a través de canales cifrados.
[MEDIUM] Acceso a /wp-login.php: El panel de administración es accesible para cualquier usuario, aumentando el riesgo de intrusión por fuerza bruta.
[MEDIUM] Archivo /readme.html: Este archivo está disponible públicamente y puede revelar detalles técnicos internos del sistema.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría llevar a la ejecución de archivos no autorizados.
[MEDIUM] Referrer-Policy y Permissions-Policy: Ausencia de controles sobre la información de navegación enviada y sobre el acceso a APIs del navegador como la cámara o el micrófono.
[LOW] Cabecera de servidor expuesta: El servidor se identifica como LiteSpeed, proporcionando información útil para que un atacante perfile la infraestructura.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a rutas de administración, facilitando el mapeo del sitio por parte de agentes maliciosos.