EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://infosechub.blog/	Checks	9 pruebas
Dominio	infosechub.blog	Hallazgos	38 totales
Fecha	20 de septiembre de 2026 a las 21:19	Problemas	3 detectados

B

82/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web ha arrojado una puntuación de 82/100, lo que equivale a una nota B según los estándares de auditoría pasiva. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, se identificó 1 advertencia y se registró 1 fallo crítico relacionado con la exposición de software. Aunque la infraestructura base muestra configuraciones sólidas en redirecciones HTTPS, la presencia de versiones de software obsoletas eleva el riesgo de compromiso. En conclusión, el sitio se considera moderadamente seguro, pero es vulnerable a ataques automatizados que busquen explotar debilidades conocidas en el gestor de contenidos.

Resumen de Riesgos

0	1	1	1	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 25 dias
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 1.0.0 expuesta, WordPress 2 expuesta
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 25 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  25 dias restantes (expira: 2026-10-15T19:06:44.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-17T19:06:45.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://infosechub.blog/

- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 dias)
- 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

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1.0.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 1.0.0 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)

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 (1782 bytes)
- INFO **Reglas robots.txt**
  57 Disallow, 2 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, ? URLs

- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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

[HIGH] WordPress version: La versión 1.0.0 se encuentra expuesta públicamente, lo que permite a atacantes buscar y aplicar CVEs conocidos para comprometer el servidor.
[FAIL] WordPress 2 expuesta: La detección de múltiples versiones antiguas del CMS indica una falta crítica de mantenimiento y actualización de seguridad.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede revelar la versión exacta e información técnica del CMS a usuarios malintencionados.
[MEDIUM] SSL/TLS: El certificado de seguridad actual expira en 25 días, lo que representa un riesgo de pérdida de confianza y denegación de acceso en el corto plazo.
[LOW] Ruta sensible en robots.txt: Se detectó una referencia directa a la ruta admin, lo cual facilita el reconocimiento de directorios sensibles por parte de atacantes.
[ERROR] Cabeceras de Seguridad: No se pudieron verificar las cabeceras HTTP, lo que sugiere la ausencia de protecciones esenciales contra ataques de clickjacking e inyección.
[ERROR] Seguridad de Cookies: La falta de verificación en las cookies indica que podrían no tener activados los atributos Secure o HttpOnly, facilitando el robo de sesiones.