EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Solucioneshacs.com	Checks	9 pruebas
Dominio	solucioneshacs.com	Hallazgos	50 totales
Fecha	20 de junio de 2026 a las 08:45	Problemas	10 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a Solucioneshacs.com ha resultado en una puntuación de 85/100 con una nota de grado B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 finalizaron correctamente, 2 generaron advertencias y 1 fue marcado como fallo. A pesar de contar con una base sólida en el cifrado de comunicaciones, se han identificado debilidades críticas relacionadas con la exposición de servicios de infraestructura y versiones de software. Se concluye que el sitio es actualmente vulnerable debido a la exposición directa de su base de datos y puertos de transferencia de archivos. El riesgo de un compromiso exitoso es moderado-alto si no se corrigen los puntos señalados.

Resumen de Riesgos

1	2	3	4	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 45 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
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 4.13.0 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 45 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  45 dias restantes (expira: 2026-08-04T19:41:25.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-06T19:41:26.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

- BAJO **Server header expuesto**
  Server: LiteSpeed — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.30 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://solucioneshacs.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 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
- BAJO **Meta generator**
  Expone: Elementor 4.1.3; features: e_font_icon_svg, additional_custom_breakpoints; settings: css_print_method-external, google_font-enabled, font_display-swap
- INFO **Tecnologias detectadas**
  Next.js, Astro, PHP/8.3.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 4.13.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 4.13.0 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 (321 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://solucioneshacs.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 está abierta a internet, lo que permite ataques directos de fuerza bruta o explotación de vulnerabilidades del motor.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos activo y sin cifrar, facilitando la interceptación de credenciales y datos.
[HIGH] WordPress version: La versión 4.13.0 es visible públicamente, permitiendo a atacantes buscar y aplicar exploits específicos para esa versión.
[MEDIUM] Permissions-Policy: Falta esta cabecera de seguridad, lo que impide restringir el acceso del navegador a funciones sensibles como la cámara o el micrófono.
[MEDIUM] Archivo /readme.html: El archivo es accesible y revela información técnica sobre la instalación y estructura del CMS.
[MEDIUM] Ruta /wp-login.php: El acceso al panel de administración es público, lo que lo hace susceptible a ataques automatizados de adivinación de contraseñas.
[LOW] Server header expuesto: Se detectó el valor LiteSpeed, lo que ayuda a un atacante a perfilar el software del servidor web.
[LOW] X-Powered-By expuesto: El encabezado revela el uso de PHP/8.3.30, facilitando la identificación de posibles vectores de ataque en el lenguaje de programación.
[LOW] Meta generator: La etiqueta expone el uso de Elementor 4.1.3 y detalles sobre la configuración de fuentes y estilos del sitio.
[LOW] Ruta sensible en robots.txt: Se referencia explícitamente la palabra admin, guiando a posibles atacantes hacia directorios de gestión.