EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://humbertoherrera.com	Checks	9 pruebas
Dominio	humbertoherrera.com	Hallazgos	48 totales
Fecha	16 de junio de 2026 a las 19:54	Problemas	18 detectados

D

49/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre humbertoherrera.com arroja una puntuación de 49/100, lo que corresponde a una calificación de grado D. Se ejecutaron 9 comprobaciones pasivas, de las cuales 5 resultaron satisfactorias y 4 presentaron fallos críticos que comprometen la integridad del sitio. El principal riesgo reside en la exposición de servicios sensibles como la base de datos y la falta de protocolos de endurecimiento en las cabeceras HTTP. No se detectaron advertencias intermedias, lo que indica una polaridad entre elementos correctamente configurados y vulnerabilidades graves. Bajo las condiciones actuales, el sitio se considera vulnerable y requiere intervención inmediata para mitigar riesgos de intrusión.

Resumen de Riesgos

1	7	7	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 193 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 6.9.1 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	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 193 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  193 dias restantes (expira: 2026-12-26T10:21:32.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-24T10:21:32.000Z
- 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: Apache — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.1.34 — Revela framework/lenguaje
- 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 6.9.1
- INFO **Tecnologias detectadas**
  Next.js, Astro, PHP/8.1.34

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.1 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 (28 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **sitemap.xml**
  Presente, ? URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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) abierto: La base de datos es accesible desde internet, lo que permite ataques de fuerza bruta y posibles fugas de información masiva.
[HIGH] Redirección HTTP a HTTPS ausente: El servidor no fuerza el cifrado de la conexión, permitiendo que los usuarios naveguen por canales inseguros propensos a la interceptación.
[HIGH] Versión de WordPress 6.9.1 expuesta: El uso de una versión desactualizada y visible permite a los atacantes identificar y explotar vulnerabilidades conocidas (CVEs) específicas del CMS.
[HIGH] Cabeceras de seguridad faltantes (CSP, X-Frame-Options, HSTS): La ausencia de estas protecciones facilita ataques de Cross-Site Scripting (XSS) y Clickjacking.
[HIGH] Puerto 21 (FTP) abierto: El uso de este protocolo implica la transferencia de credenciales y archivos en texto plano, sin cifrado de ningún tipo.
[MEDIUM] Puerto 22 (SSH) abierto: La exposición de la interfaz de acceso remoto aumenta la superficie de ataque frente a intentos de inicio de sesión no autorizados.
[MEDIUM] X-Content-Type-Options ausente: La falta de esta cabecera permite que el navegador realice "MIME-type sniffing", lo que puede derivar en la ejecución de scripts maliciosos.
[MEDIUM] Ruta /wp-login.php y archivo /readme.html accesibles: Estos elementos revelan rutas administrativas y detalles técnicos que facilitan el reconocimiento del sitio por parte de terceros.
[MEDIUM] Referrer-Policy y Permissions-Policy ausentes: No se limita la información de navegación enviada a otros sitios ni se restringen APIs del navegador como la cámara o el micrófono.
[MEDIUM] Configuración de robots.txt: El archivo bloquea la indexación de todo el contenido del sitio, lo cual podría ser una desconfiguración que afecta la visibilidad.
[LOW] Cabeceras de servidor expuestas (Apache y PHP/8.1.34): Se revela información técnica detallada sobre la infraestructura, ayudando a los atacantes a personalizar sus vectores de ataque.
[LOW] Meta generator visible: La etiqueta en el código fuente confirma públicamente el uso de WordPress 6.9.1.