EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://misionerosdigitales.com	Checks	9 pruebas
Dominio	misionerosdigitales.com	Hallazgos	45 totales
Fecha	20 de mayo de 2026 a las 19:40	Problemas	16 detectados

D

47/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el sitio web ha arrojado una puntuación de 47/100, lo que corresponde a una calificación de grado D. Durante la auditoría se ejecutaron un total de 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 3 generaron advertencias y 3 fueron fallos críticos. La ausencia total de cabeceras de seguridad y la falta de una redirección obligatoria a HTTPS comprometen la integridad de la plataforma. Debido a la exposición de versiones de software obsoletas y configuraciones de red inadecuadas, se concluye que el sitio es actualmente vulnerable a ataques externos.

Resumen de Riesgos

0	6	8	2	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 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 6.9.4 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 80 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  80 dias restantes (expira: 2026-08-08T14:01:14.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-10T14:01:15.000Z
- 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: cloudflare — 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 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://feeds.feedburner.com/mdc-misionerosdigitales
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://feeds.feedburner.com/mdc-misionerosdigitales

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
  Presente, ? URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de inyección de código y Cross-Site Scripting (XSS).

[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se implementa HSTS, por lo que el navegador no fuerza conexiones seguras, permitiendo ataques de degradación de protocolo.
[HIGH] Redirección HTTP a HTTPS: El sitio permite conexiones HTTP sin redirigir al protocolo seguro, exponiendo el tráfico a interceptaciones.
[HIGH] WordPress version: Se detectó la versión 6.9.4 expuesta públicamente, permitiendo a potenciales atacantes identificar vulnerabilidades conocidas (CVEs).
[MEDIUM] X-Content-Type-Options: Falta la cabecera que evita que el navegador interprete archivos con tipos MIME incorrectos o maliciosos.
[MEDIUM] Referrer-Policy: No existe una política definida, lo que podría filtrar información de navegación a sitios de terceros.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador como la cámara o el micrófono, aumentando el riesgo de privacidad.
[MEDIUM] Contenido Mixto: Se detectaron recursos cargados mediante HTTP (feedburner) en una página HTTPS, rompiendo la cadena de seguridad del sitio.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo puede ser utilizada para acceder a servicios de administración no protegidos.
[MEDIUM] Archivos sensibles expuestos: El archivo readme.html y la ruta de acceso al panel wp-login.php son accesibles, facilitando el reconocimiento y ataques de fuerza bruta.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando información técnica sobre la infraestructura de red.
[LOW] Meta generator: La etiqueta meta expone explícitamente el uso de WordPress 6.9.4.