

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://www.mundomaletas.com.co/
Dominio www.mundomaletas.com.co
Fecha 6 de mayo de 2026 a las 03:35

Checks 9 pruebas
Hallazgos 47 totales
Problemas 14 detectados

C

64/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoria de seguridad realizada sobre el sitio web arrojo una puntuacion de 64/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron exitosos, 2 generaron advertencias y 2 finalizaron en fallo critico. Los resultados indican que, aunque el sitio cuenta con una base de cifrado valida, carece de las protecciones esenciales en las cabeceras de red y expone informacion tecnica sensible. En su estado actual, el sitio web se considera vulnerable ante ataques de interceptacion de datos y explotacion de software desactualizado.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 69 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 69 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
69 dias restantes (expira: 2026-07-14T02:43:52.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-15T02:43:53.000Z
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- **INFO** **HTTP !' HTTPS redireccion**
HTTP 301 redirige a <https://www.mundomaletas.com.co/>
- **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

1 recurso(s) HTTP en pagina HTTPS

- MEDIO** Recurso HTTP (href (link/stylesheet))
http://gmpg.org/xfn/11

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO** robots.txt
Presente (273 bytes)
- INFO** Reglas robots.txt
4 Disallow, 1 Allow
- BAJO** Ruta sensible en robots.txt
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO** Sitemap en robots.txt
https://www.mundomaletas.com.co/wp-sitemap.xml
- 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 version 6.9.4 esta expuesta publicamente, lo cual permite a atacantes identificar y explotar CVEs conocidos para comprometer el sitio.
- [HIGH] Content-Security-Policy: Falta esta cabecera indispensable que previene ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
- [HIGH] X-Frame-Options: La ausencia de esta cabecera deja el sitio desprotegido contra ataques de clickjacking que podrian enganar a los usuarios.
- [HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce conexiones HTTPS de manera estricta y segura.
- [MEDIUM] X-Content-Type-Options: Falta esta cabecera para evitar que el navegador realice MIME-type sniffing, reduciendo el riesgo de ejecucion de archivos maliciosos.
- [MEDIUM] Referrer-Policy: No existe una politica de referer, lo que podria exponer informacion de navegacion privada al interactuar con enlaces externos.
- [MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el acceso del navegador a APIs sensibles como la camara o el microfono.
- [MEDIUM] Archivo /readme.html: Este archivo es accesible publicamente y puede revelar detalles especificos de la instalacion del CMS a posibles atacantes.
- [MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario, facilitando intentos de ataque por fuerza bruta.
- [MEDIUM] Recurso HTTP: Se detecto un elemento cargado mediante protocolo no seguro (<http://gmpg.org/xfn/11>) dentro de la pagina HTTPS, generando contenido mixto.
- [LOW] Server header expuesto: El servidor revela el uso de LiteSpeed, facilitando el reconocimiento de la infraestructura tecnologica subyacente.
- [LOW] Meta generator: La etiqueta meta expone la version exacta de WordPress 6.9.4, aportando datos innecesarios para la seguridad del sitio.
- [LOW] Ruta sensible en robots.txt: Se hace referencia explicita a la ruta admin, lo que orienta a los atacantes hacia las areas de gestion interna.