EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://casa-mundo-es.com/categoria/mini-frigorifico-edicion-exclusiva/?utm_source=gkpoke&utm_campaign=MONSTER%20ES&utm_medium=paid&ttclid=E_C_P_Ct0B-SQOwbISsExQXp9HXNBCwy4YKBMy3_W3yqkPMB_9C9jLaQTfiTJk08MJ7HJGzqmJYc9G7UXMHJ2dDfx6Qvx_g52abt6-QfV_hnecJ7Cx4JU1EPu07ZeI44COqvuMBikk6QHg6kWyPJ3nYab8aUQT4qellnuLEZIGaswHcOujQiNAqDDgjFzWnCN-VQYqTb--_ukRiQTVWEmEjiSSNCZ9M0EgAgBDLQVXJd0drrmdh1qL6CCDgAGPaeomgPYa1OCvaojD_p5-&utm_id=1863482717946897&utm	Checks	9 pasados
Dominio	casa-mundo-es.com	Hallazgos	47 totales
Fecha	4 de mayo de 2026 a las 21:37	Problemas	16 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 60/100, lo que equivale a una calificación de grado C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 generó una advertencia y 3 fallaron debido a configuraciones críticas. A pesar de contar con un cifrado SSL válido, la exposición de bases de datos y la ausencia total de cabeceras de seguridad representan un riesgo significativo. En su estado actual, el sitio se considera vulnerable a ataques externos que podrían comprometer la integridad de la información.

Resumen de Riesgos

2	6	5	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 66 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	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 66 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  66 dias restantes (expira: 2026-07-09T18:26:58.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-10T18:26:59.000Z
- 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: nginx — 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://casa-mundo-es.com/
- 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 — 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 (320 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://casa-mundo-es.com/wp-sitemap.xml
- 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
- 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
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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): Base de datos MySQL expuesta directamente a internet, permitiendo intentos de acceso no autorizado.
[CRITICAL] Puerto 5432 (PostgreSQL): Base de datos PostgreSQL abierta públicamente, lo que facilita ataques de fuerza bruta o exfiltración.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos está abierto y utiliza un protocolo no cifrado que expone credenciales.
[HIGH] WordPress versión 6.9.4: El uso de una versión desactualizada permite a atacantes explotar vulnerabilidades conocidas y documentadas (CVEs).
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La falta de esta directiva permite que el sitio sea cargado en marcos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security (HSTS): No se fuerza el uso de HTTPS, permitiendo posibles ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría llevar a la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a terceros, comprometiendo la privacidad de la navegación.
[MEDIUM] Permissions-Policy: Ausencia de restricciones sobre APIs del navegador como cámara, micrófono o geolocalización.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y revela información técnica detallada sobre la instalación del CMS.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario, aumentando el riesgo de ataques automatizados.
[LOW] Cabecera Server expuesta: Se revela el uso de nginx, proporcionando información útil para que un atacante perfile el servidor.
[LOW] Meta generator: La etiqueta meta expone la versión exacta de WordPress en el código fuente.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a directorios de administración, guiando a posibles atacantes hacia áreas restringidas.