EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ezquerrocatalamuebles.com	Checks	9 pruebas
Dominio	ezquerrocatalamuebles.com	Hallazgos	43 totales
Fecha	23 de septiembre de 2026 a las 16:28	Problemas	7 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ezquerrocatalamuebles.com ha dado como resultado una puntuación de 85/100, lo que otorga una calificación de nota B. Durante la auditoría se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, uno presentó una advertencia y uno fue clasificado como fallo. Aunque el cifrado de datos es correcto, la ausencia de cabeceras de seguridad críticas y políticas de transporte estricto representan una debilidad en la infraestructura. Se concluye que el sitio es generalmente seguro para el usuario final, pero se encuentra en un estado vulnerable ante ataques de intermediarios o de divulgación de información técnica.

Resumen de Riesgos

0	2	2	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 78 dias
Cabeceras de Seguridad	55	FALLO	Solo 3/6 presentes. Faltan: Strict-Transport-Sec...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 78 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  78 dias restantes (expira: 2026-12-10T09:15:41.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-10T21:42:03.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Sucuri/Cloudproxy — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests;
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://ezquerrocatalamuebles.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: All in One SEO (AIOSEO) 5.0.1.1
- INFO **Tecnologias detectadas**
  Next.js

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 (183 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://ezquerrocatalamuebles.com/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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] Strict-Transport-Security: Falta la cabecera HSTS que obliga al navegador a comunicarse exclusivamente a través de HTTPS, evitando ataques de degradación de protocolo.
[HIGH] HSTS no configurado: El sistema realiza la redirección a HTTPS pero no instruye al navegador para forzar esta conexión de forma persistente.
[MEDIUM] Referrer-Policy: Ausencia de esta cabecera, lo que impide controlar qué información de procedencia se envía a terceros al navegar desde el sitio.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador, como el acceso a la cámara o geolocalización, ampliando la superficie de riesgo.
[LOW] Server header expuesto: La cabecera revela el uso de Sucuri/Cloudproxy, proporcionando pistas valiosas a un atacante sobre la tecnología de protección utilizada.
[LOW] Meta generator expuesto: Se detectó la etiqueta de All in One SEO 5.0.1.1, lo que facilita el reconocimiento de versiones específicas de software y sus posibles fallos conocidos.
[LOW] Ruta sensible en robots.txt: El archivo menciona una ruta de administración que podría ser utilizada por agentes maliciosos para intentar accesos no autorizados.