EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://palmaspascualdomingoderamos.es/	Checks	9 pruebas
Dominio	palmaspascualdomingoderamos.es	Hallazgos	51 totales
Fecha	5 de mayo de 2026 a las 07:03	Problemas	16 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha arrojado una puntuación de 61/100, lo que equivale a una calificación de grado C. El análisis se basó en la ejecución de 9 checks pasivos, resultando en 5 verificaciones correctas, 1 advertencia y 3 fallos críticos en la configuración. Se han detectado carencias importantes en la implementación de cabeceras de seguridad y en la protección de los datos de sesión de los usuarios. Aunque el sitio posee cifrado básico, la exposición de versiones de software y la falta de políticas de seguridad activas permiten concluir que el sitio es actualmente vulnerable a ataques dirigidos.

Resumen de Riesgos

0	7	5	4	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 62 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 6.8.5 expuesta, WordPress 2 expuesta
Seguridad de Cookies	0	FALLO	request_a_quote_user_coockie: falta HttpOnly; re...
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	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 62 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  62 dias restantes (expira: 2026-07-06T11:56:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-07T11:56:53.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy

- BAJO **Server header expuesto**
  Server: LiteSpeed — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.1.27 — 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
- INFO **Permissions-Policy**
  Presente: private-state-token-redemption=(self "https://www.google.com" "https://www.gstat...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://palmaspascualdomingoderamos.es/
- 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

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.8.5
- INFO **Tecnologias detectadas**
  React, Next.js, PHP/8.1.27

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.8.5 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.8.5 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 — 0/100

Estado: FALLO

request_a_quote_user_coockie: falta HttpOnly; request_a_quote_user_coockie: falta Secure; request_a_quote_user_coockie: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: request_a_quote_user_coockie — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: request_a_quote_user_coockie — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: request_a_quote_user_coockie — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (333 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://palmaspascualdomingoderamos.es/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] Content-Security-Policy: Ausencia de cabecera para prevenir ataques de inyección de código y XSS.
[HIGH] X-Frame-Options: La falta de esta cabecera permite que el sitio sea cargado en frames, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo posibles degradaciones de conexión.
[HIGH] WordPress version: La versión 6.8.5 se encuentra expuesta públicamente, lo que facilita la búsqueda de exploits específicos.
[HIGH] Cookie HttpOnly: La cookie request_a_quote_user_coockie no tiene el flag HttpOnly, permitiendo su robo mediante scripts maliciosos.
[HIGH] Cookie Secure: La cookie de sesión se envía a través de canales no cifrados al carecer del flag Secure.
[MEDIUM] X-Content-Type-Options: El sitio es vulnerable a ataques de MIME-type sniffing por falta de configuración en el servidor.
[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada a sitios terceros al navegar.
[MEDIUM] Archivo /readme.html: Este archivo es accesible y revela detalles técnicos innecesarios sobre el sistema.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario, aumentando el riesgo de ataques de fuerza bruta.
[MEDIUM] Cookie SameSite: La ausencia de este atributo en las cookies facilita ataques de falsificación de peticiones en sitios cruzados (CSRF).
[LOW] Server header expuesto: El encabezado revela el uso de LiteSpeed, ayudando a los atacantes en la fase de reconocimiento.
[LOW] X-Powered-By expuesto: Se muestra la versión exacta de PHP/8.1.27 utilizada en el servidor.
[LOW] Meta generator: El código fuente del sitio confirma la utilización de WordPress 6.8.5.
[LOW] Ruta sensible en robots.txt: Se exponen rutas relacionadas con la administración que deberían permanecer privadas.