EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.almagmao.es/l	Checks	9 pruebas
Dominio	www.almagmao.es	Hallazgos	48 totales
Fecha	10 de junio de 2026 a las 11:50	Problemas	12 detectados

C

66/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría técnica, el sitio web presenta una puntuación de seguridad de 66/100, lo que corresponde a una calificación de grado C. El análisis se basó en 9 checks pasivos, de los cuales 5 resultaron satisfactorios, se emitió 1 advertencia y se identificaron 3 fallos de seguridad críticos. No se ejecutó un pentest activo, por lo que los resultados se limitan a la configuración superficial y pública del servidor. Debido a la exposición de versiones específicas del CMS y la falta de protecciones esenciales en las cookies y cabeceras de transporte, el sitio se clasifica actualmente como vulnerable. Se requiere una intervención técnica inmediata para mitigar riesgos de interceptación de datos y ataques dirigidos.

Resumen de Riesgos

0	5	5	2	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 dias
Cabeceras de Seguridad	40	FALLO	Solo 2/6 presentes. Faltan: Strict-Transport-Sec...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.0 expuesta, WordPress 2 expuesta
Seguridad de Cookies	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
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 61 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  61 dias restantes (expira: 2026-08-10T13:29:02.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-12T13:29:03.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: frame-ancestors 'self';
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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://almagmao.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, 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 7.0
- INFO **Tecnologias detectadas**
  React, Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0 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)

Seguridad de Cookies — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — 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 (173 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.almagmao.es/sitemap_index.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, lo que impide que el navegador fuerce el uso exclusivo de conexiones seguras HTTPS.
[HIGH] WordPress version: La versión 7.0 está expuesta públicamente, permitiendo a posibles atacantes identificar y explotar vulnerabilidades conocidas (CVEs).
[HIGH] Cookie PHPSESSID - HttpOnly: La falta de este flag permite que la cookie de sesión sea accesible mediante scripts, aumentando el riesgo de robo de sesión por XSS.
[HIGH] Cookie PHPSESSID - Secure: La ausencia del flag Secure permite que la cookie de sesión sea enviada a través de conexiones no cifradas.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera deja al sitio vulnerable a ataques de MIME-type sniffing.
[MEDIUM] Referrer-Policy: No hay una política definida para controlar cuánta información de referencia se envía a otros dominios.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la ubicación.
[MEDIUM] Cookie PHPSESSID - SameSite: La ausencia de este atributo hace que las sesiones de los usuarios sean vulnerables a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y suele revelar información técnica sobre la instalación del CMS.
[LOW] Server header expuesto: El servidor revela el uso de la tecnología nginx, proporcionando pistas útiles para un atacante sobre el entorno de ejecución.
[LOW] Meta generator: El código fuente expone directamente el uso de WordPress 7.0, facilitando el reconocimiento de la infraestructura.