EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://noticiasobreras.es	Checks	9 pruebas
Dominio	noticiasobreras.es	Hallazgos	49 totales
Fecha	13 de mayo de 2026 a las 11:44	Problemas	13 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio noticiasobreras.es arroja una puntuación de 68/100, lo que equivale a una nota C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron calificados como fallos críticos. Aunque la infraestructura base cuenta con un cifrado SSL robusto y una redirección HTTPS correcta, existen deficiencias significativas en la configuración de cabeceras de seguridad y la exposición de versiones de software. Por lo tanto, el sitio se considera actualmente vulnerable ante ataques de inyección de código y reconocimiento de infraestructura.

Resumen de Riesgos

0	3	7	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 75 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress
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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 75 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  75 dias restantes (expira: 2026-07-27T15:59:46.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-28T15:59:47.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

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

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.1.34, PleskLin — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=15768000; includeSubDomains
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://noticiasobreras.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15768000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15768000 (183 dias)
- 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: All in One SEO Pro (AIOSEO) 4.9.7
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.1.34, PleskLin

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 (83 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.noticiasobreras.es/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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] Content-Security-Policy: Falta esta cabecera que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en marcos, facilitando ataques de clickjacking.
[HIGH] WordPress version: La versión 6.9.4 se encuentra expuesta públicamente, permitiendo a posibles atacantes identificar y explotar CVEs conocidos.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede llevar a la ejecución de archivos no seguros.
[MEDIUM] Referrer-Policy: No se ha definido una política para controlar qué información de navegación se envía a otros sitios.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs del navegador como la cámara o el micrófono, aumentando la superficie de riesgo.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede revelar información técnica detallada sobre la instalación del CMS.
[MEDIUM] Ruta /wp-login.php: El panel de administración es visible para cualquier usuario, quedando expuesto a ataques de fuerza bruta.
[MEDIUM] Recurso HTTP: Se detectó el uso de una hoja de estilo insegura (http://gmpg.org/xfn/11) que provoca alertas de contenido mixto.
[MEDIUM] Puerto 22 (SSH): Se encuentra abierto, lo que representa un punto de entrada potencial si no está correctamente protegido por firewall.
[LOW] Server header expuesto: El encabezado revela el uso de Nginx, facilitando el reconocimiento de la tecnología del servidor.
[LOW] X-Powered-By expuesto: Revela explícitamente el uso de PHP/8.1.34 y PleskLin, acotando los vectores de ataque posibles.
[LOW] Meta generator: Expone el uso y la versión exacta de la herramienta All in One SEO Pro 4.9.7.