EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.vozdelaverdad.es	Checks	9 pruebas
Dominio	www.vozdelaverdad.es	Hallazgos	53 totales
Fecha	18 de mayo de 2026 a las 10:14	Problemas	6 detectados

A

94/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web www.vozdelaverdad.es ha dado como resultado una puntuación de 94/100, lo que equivale a una nota de grado A. Se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 generaron advertencias, sin detectarse fallos críticos de bloqueo. La infraestructura presenta una configuración robusta en cuanto a cifrado y cabeceras de protección, aunque se identificaron puntos de mejora en la gestión de sesiones y exposición de archivos técnicos. Los resultados indican que, en su estado actual, el sitio es seguro para el usuario final, manteniendo estándares de protección elevados. Se recomienda atender las advertencias señaladas para mitigar riesgos potenciales de seguridad.

Resumen de Riesgos

0	1	3	2	47
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 69 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
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 69 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  69 dias restantes (expira: 2026-07-26T17:28:14.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-27T17:28:15.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
  Presente: frame-ancestors 'self';
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: camera=(), microphone=(), geolocation=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.vozdelaverdad.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- 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: Voz de la Verdad
- INFO **Tecnologias detectadas**
  React, Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: voz-de-la-verdad-session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: voz-de-la-verdad-session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: voz-de-la-verdad-session — SameSite**
  SameSite=lax

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 (306 bytes)
- INFO **Reglas robots.txt**
  8 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.vozdelaverdad.es/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] Falta de atributo HttpOnly en cookie XSRF-TOKEN: La cookie es accesible mediante scripts del lado del cliente, lo que aumenta significativamente el riesgo de robo de tokens de sesión en ataques de Cross-Site Scripting (XSS).
[MEDIUM] Archivo /readme.html accesible públicamente: Este documento puede revelar información técnica y estructural del sistema, facilitando la fase de reconocimiento para un posible atacante.
[MEDIUM] Archivo /README.txt accesible públicamente: Al igual que el archivo HTML, este documento técnico expone detalles sobre la plataforma que no deberían ser visibles para usuarios externos.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de acceso remoto está expuesto a Internet, lo que permite intentos de intrusión mediante fuerza bruta si no está correctamente filtrado.
[LOW] Cabecera de servidor expuesta: El servidor revela el uso de nginx, información que permite a un atacante identificar posibles vulnerabilidades específicas para dicha tecnología.
[LOW] Etiqueta meta generator expuesta: Se revela el nombre Voz de la Verdad en el código fuente, proporcionando datos innecesarios sobre las herramientas de creación del sitio.