EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.wordreference.com/	Checks	9 pruebas
Dominio	www.wordreference.com	Hallazgos	44 totales
Fecha	22 de mayo de 2026 a las 04:44	Problemas	12 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio wordreference.com ha resultado en una puntuación de 59/100, obteniendo una calificación de nota D. Se realizaron 9 comprobaciones pasivas, de las cuales 5 fueron satisfactorias, 2 generaron advertencias y 2 resultaron en fallos críticos de configuración. La evaluación revela una carencia absoluta de cabeceras de seguridad modernas y una gestión deficiente de las conexiones cifradas. En consecuencia, el sitio se clasifica actualmente como vulnerable, ya que no implementa las protecciones básicas necesarias para mitigar ataques web comunes.

Resumen de Riesgos

0	5	5	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 60 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 60 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  60 dias restantes (expira: 2026-07-21T07:48:01.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-22T07:48:02.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.31.0 — Revela tecnologia del servidor

- 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
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 418 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 418

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

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (7361 bytes)
- INFO **Reglas robots.txt**
  306 Disallow, 5 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 418)
- 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: La ausencia de esta cabecera permite ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Al no estar configurada, la página es vulnerable a ataques de clickjacking que pueden engañar a los usuarios.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador obligue a realizar conexiones seguras, facilitando ataques de interceptación.

[HIGH] Redirección HTTPS: El servidor no redirige automáticamente el tráfico HTTP a HTTPS, devolviendo un código de estado 418.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla qué información de origen se envía a otros sitios, lo que puede comprometer la privacidad del tráfico.
[MEDIUM] Permissions-Policy: No existen restricciones sobre el uso de APIs del navegador como la cámara, el micrófono o la ubicación.
[MEDIUM] Puerto 22 (SSH) ABIERTO: La exposición de este puerto de administración remota aumenta el riesgo de intentos de acceso no autorizado.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea la indexación de todo el sitio, lo cual puede ser un error de configuración o afectar la visibilidad.
[LOW] Server header expuesto: El servidor revela el uso de nginx/1.31.0, proporcionando información valiosa a posibles atacantes sobre la infraestructura.
[LOW] sitemap.xml: No se encontró el mapa del sitio, lo que dificulta las auditorías de estructura y el rastreo organizado.