EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://tiendadebicicletas.eu/	Checks	9 pruebas
Dominio	tiendadebicicletas.eu	Hallazgos	47 totales
Fecha	13 de agosto de 2026 a las 17:48	Problemas	13 detectados

C

67/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web tiendadebicicletas.eu arroja una puntuación de 67/100, lo que equivale a una nota de C. Se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fallos críticos por falta de endurecimiento del servidor. El cifrado de datos es correcto, pero la exposición de versiones del CMS y la ausencia de cabeceras de seguridad básicas elevan el nivel de riesgo. En su estado actual, el sitio se considera vulnerable ante ataques de reconocimiento y explotación de vulnerabilidades conocidas.

Resumen de Riesgos

0	5	5	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 47 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, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.0.3 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
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 47 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  47 dias restantes (expira: 2026-09-29T11:08:19.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-01T11:08:20.000Z
- 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: nginx/1.24.0 (Ubuntu) — 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
- 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://tiendadebicicletas.eu/
- 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 7.0.3
- INFO **Tecnologias detectadas**
  React, Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0.3 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0.3 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 — 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 (324 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://tiendadebicicletas.eu/wp-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] WordPress version: La versión 7.0.3 se encuentra expuesta públicamente, facilitando la búsqueda de CVEs específicos por parte de atacantes.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: El sitio carece de protección contra ataques de clickjacking, permitiendo que la web sea cargada en frames maliciosos.
[HIGH] Strict-Transport-Security: No se ha configurado la directiva HSTS, lo que impide que el navegador fuerce siempre conexiones seguras HTTPS.
[MEDIUM] Archivo /readme.html: Este archivo es accesible de forma pública y puede revelar información técnica detallada del CMS.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible, quedando expuesto a intentos de acceso por fuerza bruta.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite a los navegadores realizar MIME-type sniffing, aumentando el riesgo de ejecución de scripts maliciosos.
[MEDIUM] Puerto 22 (SSH): Se detectó este puerto abierto, lo cual representa un vector de ataque potencial para accesos remotos no autorizados.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios, lo que podría filtrar datos de navegación.
[LOW] Server header expuesto: La cabecera revela el uso de nginx/1.24.0 sobre Ubuntu, proporcionando datos valiosos para el reconocimiento del servidor.
[LOW] Meta generator: El código fuente expone directamente el uso de WordPress 7.0.3.
[LOW] Ruta sensible en robots.txt: El archivo menciona la ruta "admin", orientando a atacantes sobre la estructura interna del sitio.