EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Walmart.com	Checks	9 pruebas
Dominio	walmart.com	Hallazgos	12 totales
Fecha	2 de julio de 2026 a las 14:46	Problemas	0 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el dominio principal arroja una puntuación perfecta de 100/100 con una calificación de nota A. Durante el proceso se ejecutaron un total de 9 checks pasivos, de los cuales 1 resultó completamente satisfactorio y el resto no reportó fallos ni advertencias críticas de seguridad. Al no detectarse vectores de ataque inmediatos en los módulos procesados, se concluye que el sitio presenta una postura de seguridad sólida en su capa externa. Sin embargo, la falta de una auditoría profunda mediante pruebas activas sugiere mantener una vigilancia continua sobre la infraestructura. Es imperativo complementar este resultado con pruebas de intrusión manuales para garantizar una protección integral.

Resumen de Riesgos

0	0	0	0	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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

No se detectaron vulnerabilidades durante los checks pasivos ejecutados. El sistema no reportó fallos relacionados con CWE, cabeceras faltantes, endpoints de API expuestos ni subdominios vulnerables en los módulos que finalizaron su ejecución.