EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://t.co/NNCmhRZaQP	Checks	9 pruebas
Dominio	t.co	Hallazgos	26 totales
Fecha	13 de julio de 2026 a las 23:10	Problemas	4 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha resultado en una puntuación de 53/100, lo que otorga una calificación de grado D. Tras ejecutar 9 checks pasivos, se han identificado resultados preocupantes que incluyen 1 acierto, 2 advertencias y 1 fallo crítico de configuración. El sistema presenta deficiencias notables en la gestión de cabeceras de seguridad y en la redirección de tráfico cifrado. Debido a estos hallazgos técnicos, se concluye que el sitio es actualmente vulnerable y no cumple con los estándares mínimos de protección web.

Resumen de Riesgos

0	1	2	1	22
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 85 dias
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 85 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  85 dias restantes (expira: 2026-10-07T09:30:26.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-09T09:30:27.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 520 — No redirige a HTTPS

- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=631138519; includeSubdomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=631138519 (7305 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (152 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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)**
  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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[ALTA] Redirección HTTPS ausente: El servidor no redirige el tráfico HTTP hacia HTTPS, devolviendo un error 520, lo que expone los datos de los usuarios a intercepciones.
[MEDIA] Bloqueo de rastreo en robots.txt: El archivo está configurado para bloquear todo el sitio mediante la directiva Disallow: /, afectando la visibilidad en motores de búsqueda.

[MEDIA] Puerto 8080 abierto: Se detectó el puerto HTTP-Alt abierto, lo que puede exponer servicios administrativos o proxies vulnerables a ataques externos.
[BAJA] Falta de sitemap.xml: La ausencia de un mapa del sitio dificulta la auditoría de contenido y la indexación estructurada de la plataforma.
[ERROR] Cabeceras de seguridad no verificadas: La imposibilidad de validar las cabeceras indica una configuración de servidor incompleta frente a ataques como XSS o Clickjacking.