

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://tickets-copamex.netlify.app/	Checks	9 pruebas
Dominio	tickets-copamex.netlify.app	Hallazgos	44 totales
Fecha	21 de septiembre de 2026 a las 05:27	Problemas	8 detectados

B

80/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación de 80/100, lo que corresponde a una calificación de grado B. Durante el proceso se ejecutaron un total de 9 checks pasivos, obteniendo 7 resultados satisfactorios y 2 fallos críticos relacionados con la configuración de seguridad y metadatos del sitio. No se llevó a cabo un pentest activo, por lo que los resultados se limitan a la configuración externa y cabeceras de respuesta. En conclusión, el sitio se considera moderadamente seguro pero vulnerable a ataques de inyección y suplantación debido a la ausencia de políticas de seguridad en el servidor.

Resumen de Riesgos

0 CRITICO	2 ALTO	3 MEDIO	3 BAJO	36 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 180 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 180 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
180 dias restantes (expira: 2027-03-19T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-02-16T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO Server header expuesto
Server: Netlify — 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
- INFO

Strict-Transport-Security
Presente: max-age=31536000; includeSubDomains; preload
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://tickets-copamex.netlify.app/
- 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

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO

robots.txt
No encontrado (HTTP 404)
- BAJO

sitemap.xml
No encontrado (HTTP 404)
- BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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 Cross-Site Scripting (XSS) y la inyección de contenido malicioso en el navegador del usuario.
[HIGH] X-Frame-Options: La falta de esta directiva hace que el sitio sea vulnerable a Clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar al usuario.

[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría intentar interpretar archivos como scripts (MIME-sniffing), facilitando la ejecución de código no deseado.

[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada en las peticiones, lo que puede exponer URLs internas o datos sensibles a terceros.

[MEDIUM] Permissions-Policy: La falta de restricciones en las APIs del navegador permite que funcionalidades como la cámara o el micrófono no estén debidamente limitadas por el servidor.

[LOW] Server header expuesto: La cabecera revela el uso de la tecnología Netlify, proporcionando pistas a posibles atacantes sobre la infraestructura subyacente.

[LOW] robots.txt: El archivo de instrucciones para rastreadores no existe, dificultando la gestión de la visibilidad en motores de búsqueda.

[LOW] sitemap.xml: No se ha detectado el mapa del sitio, lo cual es una deficiencia en la estructura de información y auditoría de páginas expuestas.