EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://mi-boleto.com	Checks	9 pruebas
Dominio	mi-boleto.com	Hallazgos	56 totales
Fecha	19 de julio de 2026 a las 14:46	Problemas	10 detectados

B

87/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre mi-boleto.com arroja una puntuación de 87/100 con una calificación de grado B. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 generaron advertencias de seguridad, sin registrarse fallos críticos totales. El sitio presenta una base sólida gracias a su infraestructura en la nube, aunque manifiesta debilidades técnicas en la configuración de cookies y políticas de cabeceras. En conclusión, el sitio es mayoritariamente seguro, pero se considera vulnerable a ataques de secuestro de sesión y exposición limitada de información técnica.

Resumen de Riesgos

0	4	4	2	46
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 63 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Shopify
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	56	AVISO	localization: falta HttpOnly; localization: falt...
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): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 63 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  63 dias restantes (expira: 2026-09-20T05:09:03.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-22T05:09:04.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: block-all-mixed-content; frame-ancestors 'none'; upgrade-insecure-requests;
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=7889238
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://mi-boleto.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=7889238
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- MEDIO **HSTS max-age**
  max-age=7889238 (91 dias) — Recomendado minimo 180 dias
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Shopify

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  Detectado via HTML body
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  Next.js

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 — 56/100

Estado: AVISO

localization: falta HttpOnly; localization: falta Secure; cart_currency: falta HttpOnly; cart_currency: falta Secure

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: localization — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: localization — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: localization — SameSite**
  SameSite=lax
- ALTO **Cookie: cart_currency — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: cart_currency — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: cart_currency — SameSite**
  SameSite=lax
- INFO **Cookie: _shopify_essential — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _shopify_essential — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _shopify_essential — SameSite**
  SameSite=lax

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 (3618 bytes)
- INFO **Reglas robots.txt**
  50 Disallow, 35 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://mi-boleto.com/sitemap.xml
- 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

[HIGH] Cookie localization sin flag HttpOnly: Al carecer de esta protección, la cookie es accesible mediante scripts del lado del cliente, lo que facilita ataques de Cross-Site Scripting (XSS).
[HIGH] Cookie localization sin flag Secure: La ausencia de este flag permite que la información se transmita por canales no cifrados, aumentando el riesgo de interceptación.
[HIGH] Cookie cart_currency sin flag HttpOnly: Esta omisión permite que atacantes puedan extraer datos de navegación o de sesión a través de vulnerabilidades en el navegador.
[HIGH] Cookie cart_currency sin flag Secure: Al no forzar la transmisión solo vía HTTPS, los datos de navegación pueden ser capturados en redes inseguras.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de un puerto alternativo de servidor web incrementa la superficie de ataque y sugiere servicios secundarios no protegidos.
[MEDIUM] Referrer-Policy ausente: El sitio no controla qué información de referencia se envía a otros dominios al navegar, lo que puede filtrar URLs privadas.
[MEDIUM] Permissions-Policy ausente: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono, dejando la seguridad del lado del usuario desprotegida.
[MEDIUM] HSTS max-age insuficiente: El tiempo de persistencia de la conexión segura es de solo 91 días, cuando el estándar de la industria recomienda un mínimo de 180 días.
[LOW] Cabecera Server expuesta: Se revela el uso de Cloudflare como tecnología de servidor, facilitando a un atacante potencial la búsqueda de vulnerabilidades específicas de ese proveedor.
[LOW] Ruta sensible en robots.txt: La referencia directa al directorio de administración permite a los atacantes identificar rápidamente el punto de entrada al panel de gestión.