EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://caribemexicano.travel/	Checks	9 pruebas
Dominio	caribemexicano.travel	Hallazgos	46 totales
Fecha	17 de septiembre de 2026 a las 16:37	Problemas	13 detectados

C

66/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio caribemexicano.travel ha arrojado una puntuación de 66/100, lo que corresponde a una nota C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 terminaron en fallo. A pesar de contar con un cifrado SSL adecuado, la ausencia casi total de cabeceras de seguridad y la exposición de información técnica crítica representan riesgos significativos. Se concluye que el sitio es vulnerable y requiere intervenciones correctivas para mitigar posibles vectores de ataque.

Resumen de Riesgos

0	5	6	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 105 dias
Cabeceras de Seguridad	10	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
Version CMS Expuesta	20	FALLO	WordPress 6.8.3 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 105 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  105 dias restantes (expira: 2026-12-31T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-02T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 10/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: Apache/2.4.62 (Amazon Linux) — 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
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://caribemexicano.travel:443/
- 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

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.8.3
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.8.3 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.8.3 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- 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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (179 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://caribemexicano.travel/sitemap_index.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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 cabecera no está configurada, lo que deja al sitio expuesto a ataques de inyección de contenido y XSS.
[HIGH] X-Frame-Options: La falta de esta cabecera permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: HSTS no está configurado, permitiendo ataques de degradación de protocolo de HTTPS a HTTP.
[HIGH] WordPress version: La versión 6.8.3 está expuesta públicamente, permitiendo a atacantes identificar vulnerabilidades específicas para esa versión.
[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite el sniffing de tipos MIME por parte del navegador, aumentando el riesgo de ejecución de scripts maliciosos.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, como la cámara o el micrófono, a través de cabeceras.
[MEDIUM] Archivo /readme.html y /README.txt: Estos archivos son accesibles y revelan detalles técnicos del gestor de contenidos.
[MEDIUM] Ruta /wp-login.php: El panel de administración es accesible para cualquier usuario en internet, facilitando ataques de fuerza bruta.
[MEDIUM] Contenido Mixto: Existe un recurso (http://gmpg.org/xfn/11) que se carga mediante HTTP en una página protegida por HTTPS.
[LOW] Server header expuesto: El servidor revela el uso de Apache/2.4.62 en Amazon Linux, proporcionando información útil para la fase de reconocimiento de un atacante.
[LOW] Meta generator: La etiqueta meta expone la versión exacta de WordPress en el código fuente.