

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://www.caribex.cu
Dominio www.caribex.cu
Fecha 20 de abril de 2026 a las 19:58

Checks 9 pruebas
Hallazgos 44 totales
Problemas 7 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el sitio web arroja una puntuación final de 85/100, lo que corresponde a una calificación de grado B. Durante el proceso se ejecutaron 9 checks pasivos, resultando 7 de ellos exitosos y 2 con hallazgos de error que afectan la robustez del servidor. A pesar de contar con una implementación de cifrado impecable, la ausencia de cabeceras de seguridad críticas eleva el riesgo de ataques dirigidos a los usuarios finales. Los resultados indican que el sitio web es generalmente seguro en su capa de transporte, pero se considera vulnerable ante técnicas de clickjacking y manipulación de contenido por falta de políticas de seguridad modernas.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 56 dias
Cabeceras de Seguridad	45	FALLO	Solo 2/6 presentes. Faltan: X-Frame-Options, X-C...
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	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 56 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
56 dias restantes (expira: 2026-06-15T23:26:53.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-17T23:26:54.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

Solo 2/6 presentes. Faltan: X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https;; styl...
- ALTO **X-Frame-Options**
Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
Presente: max-age=63072000;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://www.caribex.cu/
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=63072000;includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
HSTS cubre subdominios
- INFO **HSTS max-age**
max-age=63072000 (730 dias)
- INFO **Respuesta HTTPS**
HTTPS responde con status 403

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 403)
- BAJO **sitemap.xml**
No encontrado (HTTP 403)
- BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

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

[HIGH] X-Frame-Options: La falta de esta cabecera permite que el sitio sea embebido en marcos externos, facilitando ataques de secuestro de clics o clickjacking.

[MEDIUM] X-Content-Type-Options: Al no estar presente, los navegadores podrían interpretar archivos de forma distinta a la declarada, permitiendo la ejecución de scripts maliciosos mediante sniffing de contenido.

[MEDIUM] Referrer-Policy: La ausencia de esta directiva provoca que se envíe información de navegación potencialmente sensible a sitios externos cuando un usuario hace clic en un enlace.

[MEDIUM] Permissions-Policy: El servidor no restringe el acceso a funciones del navegador como la cámara, el micrófono o la geolocalización, ampliando la superficie de ataque.

[LOW] Server header expuesto: La cabecera revela el uso de openresty, proporcionando a posibles atacantes información técnica específica sobre la infraestructura del servidor.

[LOW] robots.txt: No se encontró este archivo o el acceso está denegado, lo que impide gestionar correctamente el rastreo de motores de búsqueda.

[LOW] sitemap.xml: La falta de un mapa del sitio dificulta la auditoría de rutas y la indexación organizada del contenido web.