

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://llama-importaciones.onrender.com/
Dominio llama-importaciones.onrender.com
Fecha 17 de abril de 2026 a las 03:04

Checks 9 pruebas
Hallazgos 42 totales
Problemas 11 detectados

C

68/100

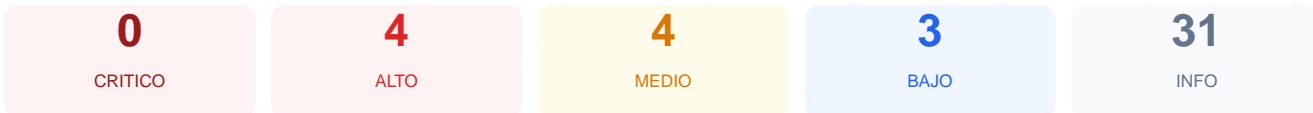
puntos de seguridad



RESUMEN EJECUTIVO

El analisis de ciberseguridad realizado al sitio web arroja una puntuacion de 68/100, lo que representa una calificacion de grado C. Se completaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron clasificados como fallos criticos. Aunque el sitio posee un cifrado de conexion valido, presenta carencias graves en la configuracion de cabeceras de seguridad y exposicion de puertos no estandar. En su estado actual, el sitio se considera vulnerable ante ataques de intermediarios y tecnicas de inyeccion de codigo.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 71 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 71 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
71 dias restantes (expira: 2026-06-26T22:00:22.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-28T21:00:26.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
Server: cloudflare — 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
- **MEDIO** **Referrer-Policy**
Falta — Controla la informacion de referer enviada
- **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://llama-importaciones.onrender.com/>
- **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

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 — 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 autentificacion 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] Content-Security-Policy: Falta esta cabecera esencial, lo que permite la ejecucion de scripts no autorizados y ataques de Cross-Site Scripting (XSS).

[HIGH] X-Frame-Options: La ausencia de esta directiva hace al sitio susceptible a ataques de clickjacking al permitir que sea embebido en frames externos.

[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide forzar conexiones seguras y deja la comunicacion expuesta a degradaciones de protocolo.

[MEDIUM] X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, aumentando el riesgo de ejecucion de archivos maliciosos disfrazados de datos.

[MEDIUM] Puerto 8080 (HTTP-Alt): Se detecto el puerto 8080 abierto, el cual suele ser utilizado para servicios administrativos o proxies que podrian estar desprotegidos.

[MEDIUM] Referrer-Policy: No existe una política definida para el manejo de información de referencia, lo que podría filtrar datos de navegación a terceros.

[MEDIUM] Permissions-Policy: Falta la restricción de acceso a funciones del navegador como cámara o geolocalización desde el sitio web.

[LOW] Server header expuesto: Se revela información técnica indicando el uso de Cloudflare, lo que facilita el reconocimiento por parte de atacantes.

[LOW] Ausencia de archivos de indexación: No se encontraron los archivos robots.txt ni sitemap.xml, lo que dificulta la gestión del rastreo y la auditoría de rutas.