EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://lamarque.marcosnoborrar.workers.dev/	Checks	9 pruebas
Dominio	lamarque.marcosnoborrar.workers.dev	Hallazgos	41 totales
Fecha	11 de mayo de 2026 a las 15:00	Problemas	11 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría técnica del sitio web, se ha determinado una puntuación de 57/100, lo que otorga una nota de grado D. El análisis se ha limitado a 9 comprobaciones pasivas, de las cuales 5 resultaron satisfactorias, 1 presenta advertencias y 3 han fallado críticamente. Se han detectado deficiencias importantes en la configuración de las cabeceras de seguridad y en la gestión del tráfico cifrado. Debido a la ausencia de mecanismos de defensa básicos contra ataques de inyección y suplantación, se concluye que el sitio es actualmente vulnerable.

Resumen de Riesgos

0	5	4	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 37 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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 37 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  37 dias restantes (expira: 2026-06-17T03:26:21.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-19T02:31:56.000Z
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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 **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 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

[LOW] Server header expuesto: Se detectó la cabecera Server con el valor cloudflare, lo cual revela la infraestructura técnica y facilita el reconocimiento a atacantes.
[HIGH] Content-Security-Policy faltante: La ausencia de esta política permite la ejecución de scripts maliciosos y ataques de inyección de contenido como XSS.
[HIGH] X-Frame-Options faltante: El sitio no protege contra ataques de clickjacking, permitiendo que la web sea cargada dentro de marcos no autorizados.
[HIGH] Strict-Transport-Security faltante: No se implementa HSTS, lo que deja a los usuarios expuestos a ataques de degradación de protocolo e interceptación de datos.
[MEDIUM] X-Content-Type-Options faltante: Sin esta cabecera, los navegadores pueden intentar adivinar el tipo de contenido, permitiendo la ejecución involuntaria de scripts.
[MEDIUM] Referrer-Policy faltante: No existe un control sobre la información de navegación que se comparte con sitios externos a través de los enlaces.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el acceso de las APIs del navegador a funciones de hardware sensibles como la cámara o el micrófono.

[HIGH] Ausencia de redirección HTTPS: El servidor permite el acceso por el puerto 80 sin redirigir automáticamente al tráfico cifrado, exponiendo la comunicación.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de este puerto alternativo abierto aumenta la superficie de ataque al exponer servicios potencialmente no protegidos.
[LOW] Falta de robots.txt y sitemap.xml: La inexistencia de estos archivos dificulta la gestión de la indexación y puede ocultar errores de visibilidad en el sitio.