

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://mwlcrm.vercel.app	Checks	9 pruebas
Dominio	mwlcrm.vercel.app	Hallazgos	45 totales
Fecha	4 de abril de 2026 a las 21:33	Problemas	8 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio mwlcrm.vercel.app ha resultado en una puntuación de 80/100, lo que otorga una calificación de nota B. Se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración de seguridad y visibilidad. Aunque la infraestructura base presenta un cifrado robusto, la carencia de cabeceras de seguridad esenciales expone el sitio a riesgos conocidos. Se concluye que el sitio es moderadamente seguro, pero se considera vulnerable a ataques de inyección y clickjacking debido a omisiones en la configuración del servidor. No se realizó un pentest activo durante este proceso.

Resumen de Riesgos

0	2	3	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 52 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 52 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
52 dias restantes (expira: 2026-05-27T06:28:02.000Z)
- INFO Fecha de emision
Emitido desde: 2026-02-26T06:28:03.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

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

- BAJO Server header expuesto
Server: Vercel — 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
- 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 308 redirige a https://mwlcrm.vercel.app/
- 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 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
- INFO

Tecnologias detectadas
React, 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 — 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 — 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 ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) y la inyección de contenido no autorizado.

[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar al usuario.

[MEDIUM] X-Content-Type-Options: La falta de esta instrucción permite que el navegador realice MIME-type sniffing, lo que puede derivar en la ejecución de archivos maliciosos.

[MEDIUM] Referrer-Policy: No existe control sobre la información de procedencia enviada en las peticiones, lo que podría filtrar datos de navegación sensibles.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como cámara o micrófono, dejando la puerta abierta a usos no autorizados de hardware.

[LOW] Server header expuesto: El servidor revela el uso de la tecnología Vercel, proporcionando información técnica útil para que un atacante planifique un exploit específico.

[LOW] robots.txt: El archivo no se encuentra en el servidor, lo que impide gestionar correctamente el acceso de rastreadores y motores de búsqueda.

[LOW] sitemap.xml: La falta de este archivo dificulta la indexación estructurada del sitio y el análisis de su jerarquía de contenidos.