EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://marscrm.bolt.host/	Checks	9 pruebas
Dominio	marscrm.bolt.host	Hallazgos	50 totales
Fecha	18 de mayo de 2026 a las 17:21	Problemas	15 detectados

C

63/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 63/100, lo que corresponde a una calificación de C. Durante la evaluación se ejecutaron 9 comprobaciones pasivas, obteniendo 5 resultados satisfactorios, 2 advertencias por configuraciones mejorables y 2 fallos críticos en la infraestructura base. El sitio presenta deficiencias significativas en la implementación de cabeceras de seguridad y en la gestión del tráfico cifrado. Debido a la exposición de rutas administrativas y la falta de redirección obligatoria a HTTPS, el sitio se considera actualmente vulnerable ante ataques de interceptación de datos y manipulación de contenido.

Resumen de Riesgos

0	3	10	2	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 46 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 46 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  46 dias restantes (expira: 2026-07-03T20:40:35.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-04T19:40:52.000Z
- 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: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Bolt.new — Revela framework/lenguaje
- 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=31536000; 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 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**
  Bolt.new

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- 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
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (2525 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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

[HIGH] Redireccion HTTP a HTTPS: El servidor responde con un código 200 en el puerto 80 en lugar de redirigir al puerto 443, permitiendo conexiones no cifradas.
[HIGH] Content-Security-Policy: Falta esta cabecera crítica, lo que deja al sitio expuesto a ataques de Cross-Site Scripting (XSS) e inyección de datos.
[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en marcos (iframes), facilitando ataques de clickjacking.
[MEDIUM] X-Content-Type-Options: No está presente, lo que permite al navegador intentar interpretar el contenido de forma distinta al tipo MIME declarado.
[MEDIUM] Referrer-Policy: Falta configuración para controlar cuánta información de referencia se envía al navegar desde el sitio hacia otros enlaces.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Archivos técnicos expuestos: Los archivos /readme.html y /README.txt son accesibles, lo que podría revelar información sobre la estructura del sitio.
[MEDIUM] Paneles de login expuestos: Se detectaron rutas de administración (/wp-login.php, /administrator/, /user/login) accesibles públicamente, aumentando el riesgo de ataques de fuerza bruta.
[MEDIUM] Robots.txt restrictivo: El archivo bloquea el rastreo de todo el sitio mediante la directiva Disallow: /, lo que afecta la visibilidad y el SEO.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: Este puerto alternativo está activo, representando un vector de ataque adicional o un servicio secundario no protegido.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando pistas sobre la infraestructura tecnológica.
[LOW] X-Powered-By expuesto: Indica el uso del framework Bolt.new, lo que facilita a un atacante la búsqueda de vulnerabilidades específicas de dicha herramienta.