EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.manalitica.com	Checks	9 pruebas
Dominio	www.manalitica.com	Hallazgos	23 totales
Fecha	9 de septiembre de 2026 a las 17:59	Problemas	7 detectados

D

56/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre manalitica.com ha resultado en una puntuación de 56/100, lo que equivale a una calificación de nota D. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 2 resultaron satisfactorios y 1 se identificó como un fallo crítico de configuración general. La ausencia de múltiples capas de protección en las cabeceras del servidor incrementa significativamente la superficie de exposición. Concluimos que el sitio es actualmente vulnerable ante ataques web convencionales debido a la falta de políticas de seguridad preventivas. Es necesaria una intervención técnica para corregir las deficiencias detectadas y mejorar la postura defensiva de la plataforma.

Resumen de Riesgos

0	3	3	1	16
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 52 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

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: 2026-11-01T01:17:32.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-03T01:17:33.000Z
- 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: Apache — 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.)

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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking, donde un atacante puede camuflar la interfaz dentro de un marco invisible para engañar al usuario.
[HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones seguras mediante HSTS, lo que permite ataques de degradación de protocolo y el posible robo de cookies de sesión.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecución de archivos maliciosos disfrazados de elementos inocuos.
[MEDIUM] Referrer-Policy: No se controla la información enviada en la cabecera referer, lo que podría filtrar datos de navegación o parámetros sensibles a dominios de terceros.
[MEDIUM] Permissions-Policy: La falta de restricción sobre las APIs del navegador permite que funciones como la cámara, el micrófono o la geolocalización no tengan un control de seguridad explícito desde el servidor.
[LOW] Server header expuesto: La cabecera revela el uso de Apache, información que permite a los atacantes buscar vulnerabilidades específicas para esa versión y tecnología de servidor.