EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sociedadtransportesmaritimoso.sg-host.com/	Checks	9 pruebas
Dominio	sociedadtransportesmaritimoso.sg-host.com	Hallazgos	13 totales
Fecha	24 de agosto de 2026 a las 22:01	Problemas	4 detectados

F

20/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el activo digital ha resultado en una puntuación de 20/100, lo que equivale a una calificación de grado F. Durante el proceso se ejecutaron un total de 9 checks pasivos, de los cuales ninguno resultó satisfactorio y se registró un fallo crítico relacionado con la exposición de servicios de red. La evaluación revela una superficie de ataque peligrosamente amplia debido a la falta de cifrado en las comunicaciones y la visibilidad pública de bases de datos sensibles. No se detectaron mecanismos de protección básicos activos, lo que compromete la integridad de la plataforma. Se concluye que el sitio es altamente vulnerable y requiere intervención técnica inmediata para mitigar riesgos de intrusión.

Resumen de Riesgos

2	2	0	0	9
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

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

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL) abierto: El servicio de base de datos MySQL es accesible directamente desde internet, lo que permite ataques de fuerza bruta y posible exfiltración de datos.
[CRITICAL] Puerto 5432 (PostgreSQL) abierto: La exposición de este puerto de base de datos facilita que actores externos intenten comprometer la información almacenada mediante vulnerabilidades conocidas o credenciales débiles.
[HIGH] Puerto 21 (FTP) abierto: La transferencia de archivos mediante FTP estándar no cifra los datos ni las credenciales, permitiendo la interceptación de información sensible en tránsito.
[HIGH] HTTP a HTTPS redirección: El sitio web no fuerza el uso de conexiones cifradas, permitiendo que los usuarios accedan vía HTTP y queden expuestos a ataques de intermediario (Man-in-the-Middle).
[LOW] Cabeceras de Seguridad ausentes: No se pudieron verificar políticas de seguridad fundamentales, lo que indica una falta de endurecimiento del servidor frente a ataques de inyección o suplantación.