EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://frigosorno.cl	Checks	9 pruebas
Dominio	frigosorno.cl	Hallazgos	15 totales
Fecha	24 de marzo de 2026 a las 15:26	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio frigosorno.cl ha otorgado una puntuación de 73/100, resultando en una nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales se obtuvo 1 resultado satisfactorio y 1 fallo crítico, además de múltiples errores técnicos de verificación. La imposibilidad de validar el cifrado SSL y las cabeceras de seguridad básicas sugiere una configuración de servidor altamente restrictiva o mal implementada. Debido a la falta de visibilidad sobre los protocolos de protección de datos, el sitio se clasifica actualmente como vulnerable. Se requiere una intervención técnica inmediata para garantizar la integridad de las comunicaciones en la plataforma.

Resumen de Riesgos

1	0	0	2	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
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
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder
- BAJO **sitemap.xml**
  Error al acceder

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

[CRÍTICO] Conexión SSL/TLS: No se pudo establecer una conexión segura, lo que impide el cifrado de datos entre el usuario y el servidor.
[CRÍTICO] Cabeceras de Seguridad: Ausencia total de políticas de seguridad en las cabeceras HTTP, facilitando ataques de intermediario o inyección.
[ALTO] Redirección HTTPS: No se pudo verificar la transición automática de tráfico no cifrado a cifrado, exponiendo datos en texto plano.
[BAJO] Robots.txt y Sitemap: El servidor deniega el acceso o carece de archivos de indexación, lo que afecta la visibilidad y el control de rastreo.
[INFO] Detección de CMS: La infraestructura oculta el sistema de gestión de contenidos, lo que dificulta la identificación de parches de seguridad específicos.