EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://servimain.cl	Checks	9 pruebas
Dominio	servimain.cl	Hallazgos	15 totales
Fecha	25 de mayo de 2026 a las 06:26	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 73/100 con una calificación de grado C. Durante la evaluación, se ejecutaron 9 checks pasivos que resultaron en 1 elemento correcto, 0 advertencias y 1 fallo crítico en la estructura de indexación. Debido a la imposibilidad de verificar componentes esenciales como el certificado SSL y las cabeceras de seguridad, el sitio presenta una postura de seguridad incierta. Se concluye que el sitio es potencialmente vulnerable ya que no se han podido validar los mecanismos básicos de cifrado y protección de datos. Los resultados sugieren una necesidad urgente de revisión técnica para asegurar la integridad de 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: No se pudo establecer una conexión SSL/TLS válida, lo que impide el cifrado de la información transmitida entre el servidor y el usuario.
[ALTO] Cabeceras de Seguridad: Ausencia total de verificación de cabeceras HTTP, facilitando ataques de tipo Cross-Site Scripting (XSS) y Clickjacking por falta de políticas de seguridad.
[ALTO] Redirección HTTPS: No se pudo confirmar el forzado de tráfico seguro, lo que permite que los usuarios naveguen por canales no cifrados vulnerables a la interceptación.
[MEDIO] Seguridad de Cookies: La falta de acceso a la configuración de cookies impide confirmar si poseen los atributos Secure y HttpOnly necesarios para evitar el robo de sesiones.
[BAJO] Robots.txt y Sitemap: Los archivos robots.txt y sitemap.xml no son accesibles o no existen, lo que compromete la gestión del rastreo y la visibilidad controlada del sitio.