EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.sidcai.fonacit.gob.ve	Checks	9 pruebas
Dominio	www.sidcai.fonacit.gob.ve	Hallazgos	15 totales
Fecha	20 de mayo de 2026 a las 13:18	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio arroja una puntuación exacta de 73/100, lo que corresponde a una nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 1 resultó en estado conforme, 0 presentaron advertencias y 1 se categorizó formalmente como fallo de acceso, aunque la imposibilidad de establecer conexiones seguras afectó la visibilidad de otros parámetros. El escaneo detectó problemas críticos de conectividad que impidieron la verificación de cifrado y cabeceras de seguridad esenciales. Debido a la falta de validación SSL/TLS y la ausencia de políticas de seguridad visibles, el sitio se considera vulnerable en su estado actual.

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

[CRITICAL] Conexion SSL: No se pudo establecer una conexion segura SSL/TLS, lo que impide el cifrado de la informacion entre el usuario y el servidor.
[CRITICAL] Cabeceras de Seguridad: No fue posible verificar la presencia de cabeceras HTTP de proteccion, lo que expone al sitio a ataques de inyeccion y secuestro de clics.
[MEDIUM] Seguridad de Cookies: La imposibilidad de verificar los atributos de las cookies impide garantizar que los datos de sesion esten protegidos contra robos.
[LOW] robots.txt: Error al acceder al archivo, lo que dificulta la gestion del rastreo por parte de motores de busqueda.
[LOW] sitemap.xml: El archivo de mapa del sitio no esta accesible o no existe, afectando la indexacion y transparencia de la estructura web.