EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.fonacit.gob.ve	Checks	9 pruebas
Dominio	www.fonacit.gob.ve	Hallazgos	16 totales
Fecha	20 de mayo de 2026 a las 12:55	Problemas	4 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web fonacit.gob.ve ha resultado en una puntuacion de 73/100, lo que equivale a una nota C. Se ejecutaron un total de 9 checks pasivos, de los cuales 1 resulto en estado OK y se registro 1 fallo principal relacionado con la configuracion base. Los resultados reflejan deficiencias criticas en el cifrado de datos y la configuracion de cabeceras de proteccion. Debido a la imposibilidad de verificar la conexion SSL y la falta de redireccion segura, se concluye que el sitio es actualmente vulnerable. Es imperativo realizar ajustes tecnicos para garantizar la integridad y privacidad de la informacion de los usuarios.

Resumen de Riesgos

1	1	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

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

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

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 SSL/TLS valida, lo que impide el cifrado de la informacion transmitida.
[HIGH] Redireccion HTTPS: El sitio responde con un codigo HTTP 200 en lugar de redirigir automaticamente a una version segura, permitiendo el trafico en texto plano.
[HIGH] Cabeceras de Seguridad: Ausencia total de cabeceras de proteccion, lo que facilita ataques de inyeccion y suplantacion de identidad.
[MEDIUM] Seguridad de Cookies: No se pudo verificar la presencia de atributos de seguridad en las cookies, aumentando el riesgo de robo de sesiones.
[LOW] Robots.txt y Sitemap: No se localizaron los archivos robots.txt ni sitemap.xml, lo que dificulta la gestion del rastreo por motores de busqueda.