EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sudeaseg.gob.ve	Checks	9 pruebas
Dominio	sudeaseg.gob.ve	Hallazgos	13 totales
Fecha	23 de marzo de 2026 a las 17:48	Problemas	1 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio evaluado arroja una puntuación perfecta de 100/100 con una calificación de Nota A. Durante el proceso, se ejecutaron un total de 9 checks pasivos, de los cuales 1 resultó en estado OK, 0 presentaron advertencias y 0 se registraron como fallos de seguridad detectados. Los resultados indican que el servidor no expone servicios innecesarios a través de puertos abiertos, minimizando la superficie de ataque inmediata. Aunque la puntuación es máxima, se detectaron problemas de conectividad que impidieron validar ciertos parámetros de cifrado. En conclusión, el sitio se considera seguro en su configuración de red externa, pero requiere atención técnica en sus protocolos de transferencia.

Resumen de Riesgos

1	0	0	0	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
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

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

[CRITICO] Conexion SSL: No se pudo establecer una conexion SSL/TLS valida, lo que impide asegurar la confidencialidad de la informacion transmitida.
[BAJO] Cabeceras de Seguridad: No se pudieron verificar las directivas de seguridad en las cabeceras HTTP, lo que podria exponer a los usuarios a ataques de inyeccion o cross-site scripting.
[BAJO] Redireccion HTTPS: Existe una imposibilidad de confirmar si el trafico inseguro se redirige automaticamente a una conexion cifrada.
[BAJO] Tiempo de Respuesta (Timeout): Se identificaron multiples errores de tiempo de espera de 15 segundos que sugieren una baja disponibilidad o bloqueos en la respuesta del servidor.
[OK] Puertos Abiertos: No se detectaron puertos abiertos ni servicios vulnerables expuestos directamente a internet.