EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://formate.igssgt.org	Checks	9 pruebas
Dominio	formate.igssgt.org	Hallazgos	12 totales
Fecha	4 de junio de 2026 a las 21:56	Problemas	0 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio formate.igssgt.org ha finalizado con una puntuación de 100/100 y una calificación de grado A. Durante la auditoría se ejecutaron 9 checks pasivos, obteniendo 1 resultado satisfactorio y cero incidencias en las categorías de advertencias o fallos. Al no haberse detectado vulnerabilidades críticas ni configuraciones erróneas en los parámetros analizados, el sitio se clasifica como seguro bajo el alcance de esta revisión. Es fundamental considerar que estos resultados se basan en un escaneo pasivo, por lo que la integridad total del sistema se mantiene dentro de los estándares óptimos reportados.

Resumen de Riesgos

0	0	0	0	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

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
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

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

No se detectaron vulnerabilidades durante la ejecución de los checks pasivos. Debido a que no se registraron fallos ni advertencias, y dado que el pentest activo no fue ejecutado, no existen hallazgos de CWEs, endpoints de API expuestos o subdominios vulnerables en este informe. Los escaneos realizados confirman la ausencia de puertos abiertos críticos detectables de forma externa.