EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://qroo.gob.mx	Checks	9 pruebas
Dominio	qroo.gob.mx	Hallazgos	12 totales
Fecha	17 de septiembre de 2026 a las 16:00	Problemas	0 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de ciberseguridad realizado al sitio web ha resultado en una puntuación de 100/100, otorgando una nota final de A. Durante la evaluación, se llevaron a cabo 9 checks pasivos, de los cuales 1 finalizó con éxito y el resto presentó errores de conexión que impidieron la detección de fallos o advertencias. No se registraron vulnerabilidades abiertas durante las pruebas que lograron completarse satisfactoriamente. Con base en los datos obtenidos, el sitio se considera seguro en su configuración de red externa. No obstante, se requiere una validación manual de las cabeceras para confirmar este estado de integridad total.

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 reales en los checks pasivos que finalizaron su ejecución.
Debido a que el PentestAgent no fue ejecutado, no se identificaron CWEs, endpoints de API, ni subdominios expuestos.
Los módulos de Cabeceras de Seguridad, Redirección HTTPS y Seguridad de Cookies devolvieron un error de tiempo de espera, por lo que no se pueden reportar hallazgos específicos en estas áreas.