EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://dev.savoirs.sdc.quebec/	Checks	9 pruebas
Dominio	dev.savoirs.sdc.quebec	Hallazgos	12 totales
Fecha	17 de marzo de 2026 a las 18:38	Problemas	0 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras completar la auditoria tecnica, la plataforma ha obtenido una puntuacion de 100/100 y una nota A. Se ejecutaron 9 checks pasivos, resultando en 1 validacion correcta de puertos y 8 fallos de tiempo de espera que impidieron la verificacion de cabeceras y CMS. El pentest activo con IA se ejecuto satisfactoriamente utilizando herramientas como Nmap, Nuclei, WhatWeb, FFUF, HTTP Probing y analisis SSL/TLS. Durante el proceso se descubrio una superficie de ataque reducida limitada a los puertos estandar 80 y 443, sin exposicion de directorios sensibles ni vulnerabilidades criticas. En conclusion, el sitio se considera seguro bajo las condiciones actuales de evaluacion.

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

[INFO] Puertos Abiertos: No se detectaron puertos innecesarios, manteniendo solo los servicios web estandar operativos.
[LOW] Fallo de Verificacion de Cabeceras: El sistema no pudo confirmar la presencia de cabeceras de seguridad debido a un error de tiempo de espera en el analisis.
[LOW] Referencias de Configuracion: El informe de PentestAgent identifica dos referencias de severidad baja relacionadas con la optimizacion de la superficie expuesta.
[INFO] Ausencia de CVEs: El escaneo activo con Nuclei no detecto vulnerabilidades conocidas o exploits aplicables a las tecnologias detectadas.
[INFO] Seguridad de Directorios: El fuzzing de rutas confirmo que no hay endpoints de API sensibles ni archivos de configuracion (.env, .git) expuestos.