EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.snpp.edu.py	Checks	9 pruebas
Dominio	www.snpp.edu.py	Hallazgos	12 totales
Fecha	17 de septiembre de 2026 a las 23:11	Problemas	0 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de ciberseguridad realizado ha otorgado una puntuación de 100/100 y una nota A. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 1 resultó satisfactorio y no se detectaron advertencias ni fallos en el resto de los parámetros evaluados. En base a estos resultados, el sitio se concluye como seguro bajo el alcance de esta auditoría externa preliminar. No obstante, la ausencia de riesgos detectados en esta fase no excluye la posibilidad de vulnerabilidades en capas más profundas de la aplicación. Es un resultado excelente que refleja una configuración robusta frente a escaneos pasivos.

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 el análisis de checks pasivos realizado. Debido a que no se ejecutó un pentest activo, no se han identificado hallazgos adicionales por parte del PentestAgent, tales como debilidades CWE, endpoints de API expuestos o subdominios vulnerables. El sistema no reportó fallos de seguridad en la configuración de cabeceras ni en la gestión de cookies en los datos procesados con éxito.