EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://aspirantes.senafront.gob.pa/	Checks	9 pruebas
Dominio	aspirantes.senafront.gob.pa	Hallazgos	13 totales
Fecha	29 de abril de 2026 a las 15:16	Problemas	1 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de ciberseguridad realizado al portal ha resultado en una puntuación de 100/100 y una calificación de nota A. Durante el proceso se ejecutaron un total de 9 checks pasivos, obteniendo 1 resultado satisfactorio, 0 advertencias y 0 fallos de seguridad detectados. A pesar de las limitaciones en la conectividad que impidieron la recolección de ciertos metadatos, no se hallaron vectores de ataque expuestos. Con base en estos parámetros específicos, el sitio se concluye como seguro. No obstante, se recomienda una validación manual para confirmar las configuraciones que presentaron tiempo de espera agotado.

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
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

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

[BAJA] Puertos Abiertos: No se detectaron puertos abiertos innecesarios, lo que reduce la superficie de ataque externa.
Nota: No se identificaron vulnerabilidades adicionales, CWEs, endpoints de API o subdominios expuestos debido a la ausencia de hallazgos en los checks pasivos y la no ejecución de pruebas activas. Los errores de conexión durante el escaneo impidieron identificar cabeceras faltantes o configuraciones de cookies.