EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://neon.templaris.net/	Checks	9 pruebas
Dominio	neon.templaris.net	Hallazgos	12 totales
Fecha	18 de mayo de 2026 a las 17:20	Problemas	0 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación de 100/100, obteniendo una nota final de A. Durante la evaluación se ejecutaron un total de 9 checks pasivos, de los cuales 1 resultó satisfactorio y no se detectaron advertencias ni fallos en el resto de los parámetros. Al no identificarse vulnerabilidades explotables ni configuraciones erróneas en los puntos validados, el entorno se clasifica actualmente como seguro. La integridad de la plataforma cumple con los estándares de seguridad evaluados en esta fase inicial del proceso. La ausencia de hallazgos negativos refuerza la postura defensiva del servidor frente a intentos de escaneo externos.

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 escaneo pasivo ni se identificaron fallos de seguridad en los parámetros analizados. Debido a que el pentest activo no fue ejecutado, no existen hallazgos relacionados con CWEs, cabeceras faltantes confirmadas, endpoints de API descubiertos o subdominios expuestos.