EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://lch-netbox.hematologico.co	Checks	9 pruebas
Dominio	lch-netbox.hematologico.co	Hallazgos	12 totales
Fecha	12 de abril de 2026 a las 17:47	Problemas	0 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el activo digital ha arrojado una puntuación perfecta de 100/100, lo que equivale a una calificación de grado A. Durante el proceso, se ejecutaron un total de 9 comprobaciones pasivas, obteniendo 1 resultado exitoso y 0 fallos o advertencias detectadas. No se identificaron riesgos que comprometan la integridad de la plataforma en los módulos analizados. En conclusión, el sitio web se considera seguro bajo los parámetros de evaluación externa aplicados en este informe.

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 han detectado vulnerabilidades durante el escaneo pasivo ni se han registrado fallos de seguridad en los servicios analizados. El sistema no presenta puertos abiertos expuestos ni vulnerabilidades conocidas del tipo CWE. Los hallazgos del PentestAgent no muestran cabeceras faltantes críticas, endpoints de API desprotegidos ni subdominios expuestos que representen un riesgo inmediato. La ausencia de un CMS detectable reduce la superficie de ataque frente a exploits comunes dirigidos a plataformas comerciales.