EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://vault.networkbits.es	Checks	9 pruebas
Dominio	vault.networkbits.es	Hallazgos	41 totales
Fecha	3 de julio de 2026 a las 09:51	Problemas	5 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio vault.networkbits.es ha resultado en una puntuación de 88/100 con una calificación de nota B. Se realizaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios y 3 generaron advertencias de seguridad debido a configuraciones incompletas. El sitio demuestra un manejo excelente del cifrado de transporte, pero presenta deficiencias en las políticas de seguridad de cabeceras y exposición de puertos. En su estado actual, el sitio se considera mayoritariamente seguro, pero vulnerable a ataques de interceptación de datos y reconocimiento de infraestructura.

Resumen de Riesgos

0	1	2	2	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 34 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 34 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  34 dias restantes (expira: 2026-08-06T11:39:49.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-08T11:39:50.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor
- INFO **Content-Security-Policy**
  Presente: default-src 'none'; font-src 'self'; manifest-src 'self'; base-uri 'self'; form-...

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- INFO **Permissions-Policy**
  Presente: accelerometer=(), ambient-light-sensor=(), autoplay=(), battery=(), camera=(), d...

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1836 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Strict-Transport-Security: Falta la cabecera HSTS, lo que impide obligar al navegador a usar conexiones HTTPS y permite posibles ataques de degradación de protocolo.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto alternativo abierto que amplía la superficie de ataque y sugiere la presencia de servicios de gestión o proxies expuestos.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea la indexación de todo el sitio mediante la directiva Disallow: /, lo que oculta la estructura pero no protege los recursos de accesos directos.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando información valiosa a atacantes sobre la infraestructura de red utilizada.
[LOW] sitemap.xml: No se encontró el mapa del sitio, lo que dificulta la auditoría de activos y la organización del contenido del servidor.