

Escanear Vulnerabilidades

Informe de Seguridad Web

URL	https://barrio-tech-hub.base44.app/store/6aa956c260ea155fed6961a2b0c	Pruebas	9 pruebas
Dominio	barrio-tech-hub.base44.app	Hallazgos	49 totales
Fecha	2 de octubre de 2026 a las 20:59	Problemas	9 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a la plataforma arroja una puntuación de 88/100 con una calificación de grado B. Se ejecutaron un total de 9 comprobaciones pasivas, resultando en 7 verificaciones satisfactorias y 2 advertencias, sin detectarse fallos críticos de bloqueo. Aunque la base de cifrado y conectividad es sólida, la ausencia de cabeceras de seguridad avanzadas y la exposición de puertos alternativos representan un riesgo moderado. El sitio se considera actualmente seguro para operaciones básicas, pero presenta vulnerabilidades específicas que podrían ser explotadas para ataques de inyección o reconocimiento. Se recomienda mitigar los hallazgos descritos para elevar el estándar de protección a un nivel óptimo.

Resumen de Riesgos

0	1	7	1	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 70 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 70 dias

●	INFO	Certificado valido	El certificado SSL es valido y de confianza
●	INFO	Dias hasta expiracion	70 dias restantes (expira: 2026-12-11T13:16:22.000Z)
●	INFO	Fecha de emision	Emitido desde: 2026-09-12T13:16:23.000Z
●	INFO	Puerto 443	Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Permissions-Policy

●	BAJO	Server header expuesto	Server: cloudflare — Revela tecnologia del servidor
---	------	-------------------------------	---

- ALTO

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- INFO

X-Frame-Options
Presente: DENY
- INFO

Strict-Transport-Security
Presente: max-age=31536000
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- MEDIO

Permissions-Policy
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK
HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://barrio-tech-hub.base44.app/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31536000
- BAJO

HSTS includeSubDomains
HSTS no cubre subdominios
- INFO

HSTS max-age
max-age=31536000 (365 dias)
- INFO

Respuesta HTTPS
HTTPS responde con status 200

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
- INFO

Tecnologias detectadas
Next.js

Version CMS Expuesta — 100/100

Estado: OK
No se detecto version de CMS expuesta

- MEDIO

Archivo /readme.html
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Archivo /README.txt
Archivo accesible publicamente — Puede revelar version e informacion del CMS

- MEDIO

Ruta /wp-login.php
Panel de login accesible publicamente
- MEDIO

Ruta /administrator/
Panel de login accesible publicamente
- MEDIO

Ruta /user/login
Panel de login accesible publicamente
- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt
Presente (79 bytes)
- INFO

Reglas robots.txt
0 Disallow, 1 Allow
- INFO

Sitemap en robots.txt
https://barrio-tech-hub.base44.app/sitemap.xml
- 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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, facilitando ataques de XSS e inyección de contenido.
- [MEDIUM] Permissions-Policy: No se restringe el acceso a funciones sensibles del navegador como la cámara o el micrófono, lo que compromete la privacidad del usuario.
- [MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de un servidor web alternativo o proxy aumenta la superficie de ataque para accesos no autorizados.
- [MEDIUM] Archivos de información expuestos (/readme.html, /README.txt): Estos archivos pueden contener metadatos sobre la tecnología utilizada, facilitando el reconocimiento a atacantes.
- [MEDIUM] Rutas administrativas accesibles (/wp-login.php, /administrator/, /user/login): La disponibilidad pública de paneles de acceso facilita intentos de intrusión mediante fuerza bruta.
- [LOW] Exposición de cabecera Server: El servidor revela el uso de Cloudflare, lo que proporciona información técnica sobre la infraestructura de red.