

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://avanzik.com	Checks	9 pruebas
Dominio	avanzik.com	Hallazgos	44 totales
Fecha	25 de septiembre de 2026 a las 15:44	Problemas	11 detectados

C

73/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 73/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 checks pasivos, obteniendo 5 resultados satisfactorios, 2 advertencias y 2 fallos críticos en la configuración. Aunque el cifrado de datos es correcto, la ausencia de cabeceras de seguridad esenciales y la exposición de puertos innecesarios comprometen la postura defensiva. En conclusión, el sitio se considera vulnerable a ataques de nivel medio que podrían ser mitigados con ajustes de configuración en el servidor.

Resumen de Riesgos

0 CRITICO	3 ALTO	4 MEDIO	4 BAJO	33 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 53 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 53 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
53 dias restantes (expira: 2026-11-17T21:20:42.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-19T21:20:43.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- BAJO

X-Powered-By expuesto
X-Powered-By: Next.js — Revela framework/lenguaje
- INFO

Content-Security-Policy
Presente: script-src 'self' 'unsafe-inline' 'unsafe-eval' https://m.avanzik.com https://*....
- ALTO

X-Frame-Options
Falta — Protege contra clickjacking
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO

X-Content-Type-Options
Falta — Evita MIME-type sniffing
- MEDIO

Referrer-Policy
Falta — Controla la informacion de referer enviada
- MEDIO

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

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://avanzik.com/
- ALTO

HSTS (Strict-Transport-Security)
HSTS no configurado — El navegador no fuerza HTTPS
- 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, Next.js

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO

robots.txt
No encontrado (HTTP 404)
- 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] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que permite que un atacante intente degradar la conexión de HTTPS a HTTP.
[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto y podría exponer servicios administrativos o proxies sin la protección adecuada.

[MEDIUM] X-Content-Type-Options: Falta esta cabecera, lo que permite al navegador interpretar archivos con tipos MIME incorrectos, aumentando el riesgo de ejecución de scripts.

[MEDIUM] Referrer-Policy: No existe una política definida, lo que puede provocar la fuga de información sensible en las URLs hacia sitios de terceros.

[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador, permitiendo potencialmente el acceso no autorizado a la cámara, micrófono o geolocalización.

[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, lo que ayuda a potenciales atacantes en la fase de reconocimiento.

[LOW] X-Powered-By expuesto: Se detecta el uso de Next.js, revelando el framework de desarrollo y acotando posibles vectores de ataque específicos.

[LOW] Archivos de indexación: No se encontraron los archivos robots.txt ni sitemap.xml, lo que dificulta la gestión del rastreo por parte de motores de búsqueda.