EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://voypati.com	Checks	9 pruebas
Dominio	voypati.com	Hallazgos	46 totales
Fecha	21 de mayo de 2026 a las 10:18	Problemas	12 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado presenta una puntuación de seguridad de 61/100, lo que equivale a una nota C. El análisis se basó en la ejecución de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 generó una advertencia y 2 fueron calificados como fallos críticos. Se han identificado carencias graves en la configuración de las cabeceras de seguridad y en la gestión de la redirección de tráfico cifrado. Debido a la ausencia de políticas de protección básicas y la exposición de servicios en puertos no estándar, el sitio se considera actualmente vulnerable a ataques de interceptación y suplantación de identidad. Se requiere una intervención técnica inmediata para mitigar los riesgos detectados y elevar el nivel de protección de la plataforma.

Resumen de Riesgos

0	5	4	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 85 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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 85 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  85 dias restantes (expira: 2026-08-14T06:22:27.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-16T05:23:53.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, 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
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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**
  React, 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (159 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://voypati.com/product/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] Falta de Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] Falta de X-Frame-Options: El sitio no protege contra ataques de clickjacking, permitiendo que la web sea cargada dentro de marcos externos maliciosos.
[HIGH] Falta de Strict-Transport-Security: La carencia de HSTS impide que el navegador fuerce conexiones seguras, facilitando ataques de degradación de protocolo.
[HIGH] Fallo en Redirección HTTPS: El servidor responde a peticiones HTTP sin redirigir automáticamente al puerto seguro, exponiendo datos en tránsito.
[MEDIUM] Puerto 8080 (HTTP-Alt) Abierto: La presencia de un puerto alternativo abierto aumenta la superficie de ataque y puede exponer servicios internos o proxies.
[MEDIUM] Falta de X-Content-Type-Options: Permite que el navegador realice MIME-type sniffing, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Falta de Referrer-Policy: No se controla la información de referencia enviada a otros dominios, lo que podría filtrar rutas internas.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el acceso de las APIs del navegador a funciones sensibles como la cámara o la ubicación.
[LOW] Puerto 8080 expuesto: Se detectó un servidor web alternativo activo que requiere revisión de acceso.
[LOW] Cabeceras de información expuestas: El servidor revela el uso de Cloudflare y el framework Next.js, facilitando el reconocimiento para un atacante.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a una ruta de administración, lo que ayuda a identificar puntos de entrada críticos.