EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://listindiario.com/	Checks	9 pruebas
Dominio	listindiario.com	Hallazgos	43 totales
Fecha	9 de junio de 2026 a las 19:10	Problemas	7 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha resultado en una puntuación de 76/100, lo que le otorga una calificación de grado B. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 7 resultados satisfactorios, 1 advertencia y 1 fallo crítico. El sistema muestra una gestión sólida del cifrado SSL y la visibilidad de archivos de configuración, pero presenta debilidades significativas en la implementación de políticas de seguridad del lado del servidor. Aunque el sitio no es inherentemente inseguro, se considera vulnerable a ataques de inyección y suplantación de identidad debido a la ausencia total de cabeceras de protección. Se recomienda realizar las mejoras técnicas sugeridas para elevar el nivel de defensa ante amenazas externas.

Resumen de Riesgos

0	4	3	0	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 154 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 154 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  154 dias restantes (expira: 2026-11-10T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-27T00:00:00.000Z
- 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

- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://listindiario.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**
  React, Next.js, Astro

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 (264 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://listindiario.com/sitemap-google-news.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Inteligencia Artificial

---RESUMEN EJECUTIVO---
El análisis de seguridad del sitio web ha resultado en una puntuación de 76/100, lo que le otorga una calificación de grado B. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 7 resultados satisfactorios, 1 advertencia y 1 fallo crítico. El sistema muestra una gestión sólida del cifrado SSL y la visibilidad de archivos de configuración, pero presenta debilidades significativas en la implementación de políticas de seguridad del lado del servidor. Aunque el sitio no es inherentemente inseguro, se considera vulnerable a ataques de inyección y suplantación de identidad debido a la ausencia total de cabeceras de protección. Se recomienda realizar las mejoras técnicas sugeridas para elevar el nivel de defensa ante amenazas externas.

---VULNERABILITIES---
[ALTA] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.

[ALTA] X-Frame-Options: Al no estar configurada, el sitio es vulnerable a ataques de clickjacking, permitiendo que sea cargado dentro de marcos en sitios externos no autorizados.
[ALTA] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce una conexión segura en todo momento, facilitando posibles ataques de interceptación de tráfico.
[MEDIA] X-Content-Type-Options: Sin esta directiva, los navegadores podrían intentar interpretar el tipo de contenido de forma incorrecta, permitiendo la ejecución involuntaria de scripts (MIME-sniffing).
[MEDIA] Referrer-Policy: No existe un control sobre la información de procedencia que se envía a otros dominios, lo que podría derivar en la exposición de datos de navegación.
[MEDIA] Permissions-Policy: No se están restringiendo las funciones del navegador, lo que permite que el sitio tenga acceso potencial a APIs de hardware o sensores sin una política restrictiva clara.