EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.sitioslistosya.com/	Checks	9 pruebas
Dominio	www.sitioslistosya.com	Hallazgos	44 totales
Fecha	6 de mayo de 2026 a las 16:05	Problemas	6 detectados

B

82/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado en la plataforma arroja una puntuacion de 82/100, lo que equivale a una nota B. Durante la evaluacion se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios, uno presento advertencias y uno fallo criticamente por la ausencia de configuraciones esenciales. La infraestructura muestra una base solida en terminos de cifrado de datos y transporte, pero presenta deficiencias notables en la implementacion de politicas de seguridad en el lado del cliente. Aunque el sitio no se considera critico, es vulnerable ante ataques especificos de inyeccion y suplantacion debido a la falta de cabeceras de proteccion. El estado general de seguridad es aceptable, pero requiere intervencion tecnica para alcanzar un nivel optimo.

Resumen de Riesgos

0	2	3	1	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 44 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
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	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 44 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  44 dias restantes (expira: 2026-06-19T05:43:57.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-21T05:43:58.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: Vercel — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 308 redirige a https://www.sitioslistosya.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 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**
  React, 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 — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
  Presente, 25 URLs
- 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 Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: Falta esta cabecera, lo que aumenta el riesgo de ataques XSS e inyeccion de contenido malicioso al no restringir las fuentes de recursos.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado dentro de marcos externos, facilitando ataques de clickjacking para engañar a los usuarios.

[MEDIUM] X-Content-Type-Options: Sin esta cabecera, los navegadores podrian intentar interpretar archivos de forma incorrecta mediante MIME-sniffing, permitiendo la ejecucion de scripts ocultos.
[MEDIUM] Referrer-Policy: No se controla la informacion de navegacion enviada a sitios de terceros, lo que podria exponer involuntariamente rutas internas o datos de navegacion.
[MEDIUM] Permissions-Policy: Falta una restriccion explicita sobre el uso de APIs sensibles del navegador como la camara, el microfono o la geolocalizacion por parte de scripts externos.
[LOW] Server header expuesto: El servidor revela el valor Vercel, proporcionando informacion tecnica que un atacante podria utilizar para buscar exploits especificos de esa plataforma.
[LOW] Robots.txt faltante: No se encontro el archivo de directivas para buscadores, lo que impide gestionar correctamente que partes del sitio deben o no ser indexadas.