

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://Monitor.kahunasl.com  
Dominio monitor.kahunasl.com  
Fecha 21 de abril de 2026 a las 07:09

Checks 9 pruebas  
Hallazgos 42 totales  
Problemas 11 detectados

# C

## 68/100

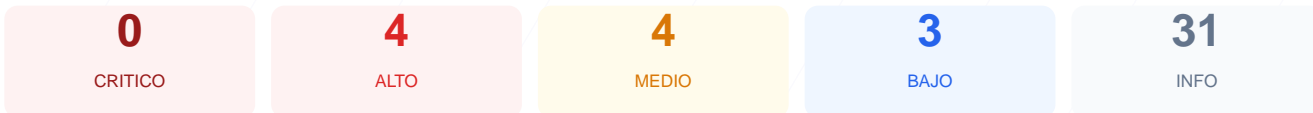
puntos de seguridad



### RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio ha arrojado una puntuación de 68/100, resultando en una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 fueron satisfactorios, 2 generaron advertencias y 2 se identificaron como fallos críticos por falta de configuraciones esenciales. El servidor web presenta una ausencia total de cabeceras de protección y expone puertos de administración que aumentan la superficie de ataque. Tras analizar estos resultados, se concluye que el sitio es actualmente vulnerable y requiere una intervención técnica inmediata para mitigar riesgos de interceptación y explotación de vulnerabilidades conocidas.

### Resumen de Riesgos



### 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	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): 22 (SSH)

### 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: 2026-07-15T16:12:26.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-04-16T16:12:27.000Z
- 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: nginx/1.24.0 (Ubuntu) — 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
- **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://monitor.kahunasl.com/>
- **ALTO** **HSTS (Strict-Transport-Security)**  
HSTS no configurado — El navegador no fuerza HTTPS
- **INFO** **Respuesta HTTPS**  
HTTPS responde con status 401

## 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

## 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): 22 (SSH)

- INFO **Puerto 21 (FTP)**  
Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**  
ABIERTO — 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 permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.  
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking donde un atacante puede camuflar la interfaz.  
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce siempre una conexión cifrada, facilitando ataques de degradación de SSL.  
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite al navegador intentar adivinar el tipo de contenido, facilitando la ejecución de archivos maliciosos ocultos.  
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a otros sitios, lo que puede filtrar datos sensibles de las URLs.  
[MEDIUM] Permissions-Policy: El servidor no restringe el acceso a funciones del navegador como cámara o micrófono, dejando la puerta abierta a abusos de privacidad.

[MEDIUM] Puerto 22 (SSH) ABIERTO: La exposición de este puerto permite intentos de acceso remoto al servidor y posibles ataques de fuerza bruta.

[LOW] Server header expuesto: El servidor revela el uso de nginx/1.24.0 (Ubuntu), proporcionando a los atacantes información valiosa sobre versiones con posibles exploits conocidos.

[LOW] Ausencia de robots.txt y sitemap.xml: No se encontraron estos archivos, lo que dificulta la gestión del rastreo por parte de buscadores y revela una configuración incompleta.