

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://kovapell.com	Checks	9 pruebas
Dominio	kovapell.com	Hallazgos	62 totales
Fecha	29 de septiembre de 2026 a las 20:27	Problemas	10 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al dominio ha arrojado una puntuación de 88/100, obteniendo una nota B. Se ejecutaron un total de 9 comprobaciones pasivas, resultando en 6 verificaciones exitosas y 3 advertencias técnicas sin registrarse fallos críticos totales. El análisis revela una base de cifrado sólida y una correcta configuración del CMS, aunque existen deficiencias en la gestión de cookies y exposición de puertos. Actualmente, el sitio se considera mayoritariamente seguro, pero presenta vulnerabilidades moderadas que podrían comprometer la privacidad de los usuarios si no se corrigen.

Resumen de Riesgos

0 CRITICO	4 ALTO	4 MEDIO	2 BAJO	52 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 78 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Shopify
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	73	AVISO	localization: falta HttpOnly; localization: falt...
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 78 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
78 dias restantes (expira: 2026-12-17T02:29:32.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-18T02:29:33.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: Referrer-Policy, Permissions-Policy

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

- INFO

Content-Security-Policy
Presente: block-all-mixed-content; frame-ancestors 'none'; upgrade-insecure-requests;
- INFO

X-Frame-Options
Presente: DENY
- INFO

Strict-Transport-Security
Presente: max-age=7889238
- INFO

X-Content-Type-Options
Presente: nosniff
- 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 301 redirige a https://kovapell.com/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=7889238
- BAJO

HSTS includeSubDomains
HSTS no cubre subdominios
- MEDIO

HSTS max-age
max-age=7889238 (91 dias) — Recomendado minimo 180 dias
- INFO

Respuesta HTTPS
HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Shopify

- INFO

WordPress
No detectado
- INFO

Joomla
No detectado
- INFO

Drupal
No detectado
- INFO

Magento
No detectado
- INFO

Shopify
Detectado via HTML body
- INFO

PrestaShop
No detectado
- INFO

Wix
No detectado
- INFO

Squarespace
No detectado
- INFO

Tecnologias detectadas
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 — 73/100

Estado: **AVISO**

localization: falta HttpOnly; localization: falta Secure; cart_currency: falta HttpOnly; cart_currency: falta Secure

- INFO **Cookies detectadas**
5 cookie(s) encontrada(s)
- ALTO **Cookie: localization — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: localization — Secure**
Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: localization — SameSite**
SameSite=lax
- ALTO **Cookie: cart_currency — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: cart_currency — Secure**
Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: cart_currency — SameSite**
SameSite=lax
- INFO **Cookie: _shopify_essential — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _shopify_essential — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _shopify_essential — SameSite**
SameSite=lax
- INFO **Cookie: _shopify_analytics — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _shopify_analytics — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _shopify_analytics — SameSite**
SameSite=lax
- INFO **Cookie: _shopify_marketing — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _shopify_marketing — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _shopify_marketing — SameSite**
SameSite=lax

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 (3630 bytes)
- INFO **Reglas robots.txt**
50 Disallow, 35 Allow
- BAJO **Ruta sensible en robots.txt**
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
https://www.kovapell.com/sitemap.xml

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 — Envío 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] Cookie localization: Carece de los flags HttpOnly y Secure, lo que permite que sea accesible mediante scripts maliciosos y se envíe por canales no cifrados.
- [HIGH] Cookie cart_currency: La ausencia de protecciones HttpOnly y Secure facilita posibles ataques de secuestro de sesión o interceptación de datos.
- [MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La disponibilidad de este puerto alternativo aumenta la superficie de ataque y puede exponer servicios internos no previstos.
- [MEDIUM] Referrer-Policy ausente: La falta de esta cabecera impide controlar la información de procedencia que se comparte con dominios externos durante la navegación.
- [MEDIUM] Permissions-Policy ausente: El servidor no define restricciones sobre el uso de APIs del navegador, como la cámara o el micrófono, por parte de terceros.
- [MEDIUM] HSTS max-age insuficiente: El tiempo de persistencia de seguridad de 91 días es inferior a los 180 días recomendados por los estándares internacionales.
- [LOW] Cabecera Server expuesta: Se revela el uso de tecnología Cloudflare, proporcionando información útil para la fase de reconocimiento de un atacante.
- [LOW] Ruta sensible en robots.txt: La referencia directa al directorio admin en el archivo de indexación ayuda a identificar puntos de entrada administrativos.