EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://kmalo.com	Checks	9 pruebas
Dominio	kmalo.com	Hallazgos	49 totales
Fecha	12 de julio de 2026 a las 08:54	Problemas	10 detectados

B

78/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web arroja una puntuacion de 78/100, lo que representa una calificacion de grado B. Se ejecutaron un total de 9 checks pasivos, resultando en 6 verificaciones satisfactorias, 2 advertencias y 1 fallo en la configuracion de cabeceras. Si bien el cifrado de datos es excelente, la exposicion de servicios de base de datos y la falta de directivas de seguridad en el navegador elevan el riesgo innecesariamente. En su estado actual, el sitio se considera vulnerable debido a la visibilidad publica de infraestructuras criticas de red.

Resumen de Riesgos

1	3	3	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 32 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 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	1 cookies, todas con flags correctos
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	2 puerto(s) potencialmente riesgoso(s): 22 (SSH)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 32 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  32 dias restantes (expira: 2026-08-13T15:18:03.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-15T15:18:04.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.18.0 (Ubuntu) — 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
- INFO **X-Frame-Options**
  Presente: DENY
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.kmalo.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, 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

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: pma_web — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: pma_web — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: pma_web — 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 (135 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.kmalo.com/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 22 (SSH), 3306 (MySQL)

- 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL) abierto: Permite intentos de conexion directa a la base de datos desde internet, lo que facilita ataques de fuerza bruta y posible exfiltracion de informacion sensible.
[HIGH] Content-Security-Policy (CSP) ausente: La falta de esta cabecera permite la ejecucion de scripts no autorizados, aumentando el riesgo de ataques XSS e inyeccion de contenido.
[HIGH] Strict-Transport-Security (HSTS) no configurado: El servidor no obliga al navegador a utilizar conexiones seguras, permitiendo potenciales ataques de interceptacion de datos en transito.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de administracion remota se encuentra expuesto, ofreciendo un vector de ataque adicional para el control total del servidor.
[MEDIUM] Referrer-Policy ausente: No se controla la informacion de referencia enviada a otros sitios, lo que podria filtrar rutas internas o datos de navegacion.
[MEDIUM] Permissions-Policy ausente: El sitio no restringe el acceso a funciones sensibles del navegador como la camara o geolocalizacion a traves de directivas de seguridad.
[LOW] Server header expuesto: El servidor revela la version exacta nginx/1.18.0 (Ubuntu), lo que permite a atacantes identificar vulnerabilidades especificas de esa version.
[LOW] X-Powered-By expuesto: Se revela el uso del framework Next.js, proporcionando informacion tecnica valiosa para el perfilamiento de ataques dirigidos.
[LOW] Ruta sensible en robots.txt: La referencia al directorio "admin" en un archivo publico expone la posible ubicacion de un panel de gestion a usuarios malintencionados.