EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://kevins.com.co/	Checks	9 pruebas
Dominio	kevins.com.co	Hallazgos	47 totales
Fecha	28 de mayo de 2026 a las 10:05	Problemas	16 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de ciberseguridad realizado al dominio kevins.com.co arrojo una puntuacion de 72/100, lo que equivale a una calificacion de grado C. Durante la evaluacion se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 genero una advertencia y 2 fueron calificados como fallos criticos. El sitio web presenta una base solida en cuanto a cifrado de datos, pero exhibe carencias importantes en la implementacion de cabeceras de defensa activa y proteccion de rutas administrativas. En su estado actual, el sitio se considera vulnerable a ataques de inyeccion y secuestro de clics debido a la falta de politicas de seguridad modernas. Se requiere una intervencion tecnica inmediata para mitigar los riesgos identificados y mejorar la postura de seguridad global.

Resumen de Riesgos

0	4	8	4	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 70 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	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 70 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  70 dias restantes (expira: 2026-08-05T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-05T00:00:00.000Z
- 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

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Express — Revela framework/lenguaje
- 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://kevins.com.co/
- 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**
  Express

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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)
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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: La ausencia de esta cabecera permite la ejecucion de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Al no estar configurada, el sitio puede ser cargado dentro de marcos externos, lo que expone a los usuarios a ataques de clickjacking.
[HIGH] Strict-Transport-Security: La falta de HSTS permite que un atacante intente degradar la conexion de HTTPS a HTTP para interceptar datos.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecucion de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la informacion de navegacion enviada a otros sitios, lo que podria filtrar rutas internas sensibles.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la camara o el microfono, aumentando la superficie de riesgo en el cliente.
[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles y pueden revelar informacion tecnica sobre la arquitectura del sitio.
[MEDIUM] Rutas de administracion publicas: Se detecto acceso a /wp-login.php, /administrator/ y /user/login, facilitando intentos de acceso no autorizado por fuerza bruta.
[LOW] Server header expuesto: El servidor revela el uso de nginx, proporcionando informacion util para que un atacante busque vulnerabilidades especificas de esa version.
[LOW] X-Powered-By expuesto: Se expone el uso del framework Express, lo que permite a un atacante dirigir ataques especificos contra esta tecnologia.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor responde con error 404 para estos archivos, dificultando la gestion de indexacion y auditoria pasiva.