# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://kurate.com.mx | Checks | 9 pruebas |
| Dominio | kurate.com.mx | Hallazgos | 47 totales |
| Fecha | 22 de abril de 2026 a las 17:28 | Problemas | 10 detectados |

**B**

84/100

puntos de seguridad

## RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web kurate.com.mx arroja una puntuación exacta de 84/100 con una calificación de nota B. El análisis se basó en la ejecución de 9 checks pasivos, de los cuales 8 resultaron exitosos y 1 presentó fallos críticos relacionados con la configuración del servidor. Aunque la implementación del cifrado SSL y las redirecciones HTTPS son correctas, se detectó una ausencia casi total de cabeceras de protección activa. Debido a estas omisiones técnicas, el sitio se considera vulnerable ante ataques de inyección y suplantación de identidad. Es imperativo aplicar las correcciones recomendadas para elevar el nivel de seguridad y proteger a los usuarios.

## Resumen de Riesgos

| 0 | 2 | 8 | 0 | 37 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 75 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 | 100 | OK | robots.txt y sitemap.xml presentes |
| Puertos Abiertos | 100 | OK | 2 puerto(s) abierto(s), todos esperados |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 75 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  75 dias restantes (expira: 2026-07-06T21:40:24.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-07T20:42:36.000Z
- 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

- 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=31556926
- 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 301 redirige a https://kurate.com.mx/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31556926
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31556926 (365 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

## 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (175 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://kurate.com.mx/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

## 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**

[ALTA] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[ALTA] X-Frame-Options: Al no estar implementada, el sitio es susceptible a ataques de Clickjacking, permitiendo que atacantes carguen la web en marcos externos fraudulentos.
[MEDIA] X-Content-Type-Options: La falta de esta instrucción permite el MIME-type sniffing, lo que puede llevar al navegador a interpretar archivos de forma insegura.
[MEDIA] Referrer-Policy: No existe un control sobre la información de procedencia enviada a sitios externos, lo que compromete la privacidad de la navegación.
[MEDIA] Permissions-Policy: El servidor no restringe el uso de APIs sensibles del navegador, como la cámara o el micrófono, ante posibles scripts de terceros.
[MEDIA] Archivos informativos expuestos: La accesibilidad pública de /readme.html y /README.txt podría revelar detalles técnicos sobre la infraestructura interna del sitio.
[MEDIA] Paneles de gestión accesibles: Se detectaron rutas de acceso administrativo como /wp-login.php y /administrator/ expuestas a intentos de intrusión por fuerza bruta.