EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://voxkom.cl	Checks	9 pruebas
Dominio	voxkom.cl	Hallazgos	44 totales
Fecha	9 de septiembre de 2026 a las 17:12	Problemas	12 detectados

C

66/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 66/100, lo que equivale a una nota C. Se ejecutaron un total de 9 checks pasivos, obteniendo 5 resultados satisfactorios, 2 advertencias y 2 fallos críticos en la configuración del servidor. El certificado SSL se encuentra vigente y correctamente instalado, sin embargo, la ausencia total de cabeceras de protección web representa un riesgo significativo. Se detectaron componentes de administración expuestos que facilitan posibles vectores de ataque externos. En su estado actual, se concluye que el sitio es vulnerable debido a la falta de medidas preventivas esenciales contra ataques de inyección y suplantación.

Resumen de Riesgos

0	4	5	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 51 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	20	FALLO	WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 51 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  51 dias restantes (expira: 2026-10-30T07:43:21.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-01T07:43:22.000Z
- 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: Apache — 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://www.voxkom.cl/
- 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

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2 expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (94 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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: Falta esta cabecera indispensable para prevenir ataques XSS y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: Su ausencia permite ataques de clickjacking, permitiendo que el sitio sea cargado en marcos externos no autorizados.
[HIGH] Strict-Transport-Security: No está configurado, lo que impide que el navegador fuerce conexiones HTTPS de manera permanente.
[HIGH] HSTS no configurado: El navegador no está obligado a mantener la conexión segura, lo que permite posibles ataques de degradación de protocolo.

[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el MIME-type sniffing, pudiendo ejecutar archivos con extensiones incorrectas.
[MEDIUM] Referrer-Policy: No hay control sobre la información de navegación enviada a otros dominios al seguir enlaces.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando expuestas funciones como la cámara, micrófono o ubicación.
[MEDIUM] Archivo /readme.html accesible: Este archivo público puede revelar la versión exacta y detalles técnicos de la infraestructura del CMS.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de acceso administrativo es accesible públicamente, lo que facilita intentos de acceso no autorizado.
[LOW] Server header expuesto: La respuesta del servidor revela el uso de Apache, proporcionando información útil para ataques dirigidos.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a directorios de administración, guiando a posibles atacantes hacia rutas críticas.
[LOW] sitemap.xml ausente: No se encontró el archivo de mapa del sitio, dificultando la auditoría de la estructura web completa.