EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://techihuahua.org.mx	Checks	9 pruebas
Dominio	techihuahua.org.mx	Hallazgos	49 totales
Fecha	23 de junio de 2026 a las 17:39	Problemas	8 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha resultado en una puntuación de 80/100, lo que otorga una calificación de nota B. Durante el proceso se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue identificado como fallo crítico. Se han detectado debilidades importantes en la configuración de cabeceras de seguridad y en la exposición de información técnica del sistema de gestión de contenidos. En conclusión, el sitio es mayormente seguro para el usuario final, pero se encuentra en un estado vulnerable frente a ataques dirigidos de reconocimiento y explotación de software desactualizado.

Resumen de Riesgos

0	3	2	3	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 183 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, Drupal, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.0 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 183 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  183 dias restantes (expira: 2026-12-23T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-24T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options

- 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: private-state-token-redemption=(self "https://www.google.com" "https://www.gstat...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://techihuahua.org.mx/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, Drupal, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  Detectado via HTML body
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 7.0
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0 expuesta

- ALTO **WordPress version**
  Version 7.0 expuesta publicamente — Permite a atacantes buscar CVEs conocidos

- INFO **Archivo /readme.html**
  No accesible (correcto)
- 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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://@TEE_Chihuahua

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (119 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://techihuahua.org.mx/wp-sitemap.xml
- 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] WordPress version: La versión 7.0 de WordPress se encuentra expuesta públicamente, lo que facilita a los atacantes la identificación y explotación de vulnerabilidades conocidas (CVEs).
[HIGH] Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: La falta de esta configuración deja el portal desprotegido ante técnicas de clickjacking que podrían engañar a los usuarios.
[MEDIUM] Recurso HTTP: Se detectó contenido mixto a través de una hoja de estilos cargada mediante protocolo inseguro, comprometiendo la integridad de la conexión HTTPS.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario de internet, permitiendo intentos de intrusión por fuerza bruta.
[LOW] Server header expuesto: La cabecera del servidor revela el uso de tecnología Apache, proporcionando información técnica valiosa para el perfilado de ataques.
[LOW] Meta generator: La etiqueta meta en el código fuente expone explícitamente que el sitio utiliza WordPress 7.0.
[LOW] Ruta sensible en robots.txt: El archivo incluye una referencia directa a la ruta de administración, guiando a actores malintencionados hacia áreas privadas del servidor.