EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.techihuahua.org.mx/teechnueva/estra2/estrados_Web/	Checks	9 pruebas
Dominio	www.techihuahua.org.mx	Hallazgos	54 totales
Fecha	21 de junio de 2026 a las 04:16	Problemas	17 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio web ha dado como resultado una puntuación de 70/100, lo que otorga una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, logrando 6 resultados satisfactorios, 1 advertencia y 2 fallos críticos en la configuración. Aunque el cifrado de transporte es válido, existen carencias importantes en la implementación de cabeceras de seguridad y en el manejo de las cookies de sesión. Se concluye que el sitio es vulnerable ante ataques de intermediarios (MitM) y ataques de inyección de scripts, requiriendo acciones correctivas inmediatas para alcanzar un nivel de seguridad óptimo.

Resumen de Riesgos

0	8	7	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 186 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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	11	FALLO	PHPSESSID: falta Secure; PHPSESSID: falta SameSi...
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	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 186 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  186 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 — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, 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
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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.techihuahua.org.mx/
- 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 — 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)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 11/100

Estado: FALLO

PHPSESSID: falta Secure; PHPSESSID: falta SameSite; sc_actual_lang_teechexp: falta HttpOnly; sc_actual_lang_teechexp: falta Secure;

sc_actual_lang_teechexp: falta SameSite; PHPSESSID_: falta HttpOnly; PHPSESSID_: falta Secure; PHPSESSID_: falta SameSite

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: sc_actual_lang_teechexp — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: sc_actual_lang_teechexp — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: sc_actual_lang_teechexp — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: PHPSESSID_ — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID_ — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID_ — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados y ataques de inyección de contenido.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo que las conexiones sean degradadas a canales inseguros.
[HIGH] Cookie PHPSESSID (Flag Secure): La cookie de sesión se envía sin cifrado, lo que facilita su interceptación en redes Wi-Fi públicas o comprometidas.
[HIGH] Cookie sc_actual_lang_teechexp (Flag HttpOnly/Secure): Al carecer de estos atributos, la cookie puede ser robada mediante scripts maliciosos o tráfico no cifrado.
[HIGH] Cookie PHPSESSID_ (Flag HttpOnly/Secure): La falta de protección en esta cookie de sesión expone la identidad del usuario ante ataques XSS y de red.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite al navegador adivinar el tipo de contenido, facilitando la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Cookies (Flag SameSite): Las cookies de sesión carecen del atributo para prevenir ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada a enlaces externos, lo que puede filtrar direcciones URL internas sensibles.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones del navegador como la cámara o el micrófono, aumentando la superficie de riesgo.
[MEDIUM] Acceso a panel de login: La ruta /wp-login.php es accesible públicamente, lo que invita a ataques de fuerza bruta contra las credenciales.
[LOW] Cabecera Server expuesta: Se revela que el servidor utiliza Apache, proporcionando información valiosa para que un atacante busque exploits específicos.
[LOW] Divulgación en robots.txt: El archivo menciona una ruta administrativa, orientando a posibles atacantes sobre la ubicación de áreas sensibles del sistema.