EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sirei.mx	Checks	9 pruebas
Dominio	sirei.mx	Hallazgos	49 totales
Fecha	31 de marzo de 2026 a las 02:29	Problemas	10 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 80/100 con una calificación de grado B. Se ejecutaron 9 checks pasivos de los cuales 6 resultaron satisfactorios, mientras que se identificó una advertencia y dos fallos en la configuración de seguridad. Los resultados indican una implementación correcta del cifrado de datos, pero se detectaron carencias importantes en las directivas de protección del navegador y en la privacidad de las cookies. Por lo tanto, el sitio se considera vulnerable ante ataques de inyección y de interceptación de sesiones en entornos no controlados.

Resumen de Riesgos

0	2	4	4	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 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	67	AVISO	.AspNetCore.Antiforgery.2PCPcozloZM: falta Secur...
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 89 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  89 dias restantes (expira: 2026-06-28T03:52:00.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-30T03:52:01.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=2592000
- 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 307 redirige a https://sirei.mx/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=2592000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- MEDIO **HSTS max-age**
  max-age=2592000 (30 dias) — Recomendado minimo 180 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
- INFO **Tecnologias detectadas**
  ASP.NET

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)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 67/100

Estado: AVISO

.AspNetCore.Antiforgery.2PCPcozloZM: falta Secure

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: .AspNetCore.Antiforgery.2PCPcozloZM — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: .AspNetCore.Antiforgery.2PCPcozloZM — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: .AspNetCore.Antiforgery.2PCPcozloZM — SameSite**
  SameSite=strict

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)
- 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 facilita la ejecución de ataques Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Cookie sin flag Secure: La cookie .AspNetCore.Antiforgery.2PCPcozloZM puede ser transmitida por canales no cifrados, arriesgando el secuestro de la sesión.
[MEDIUM] Falta de X-Content-Type-Options: Permite que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecución de scripts inesperados.
[MEDIUM] Falta de Referrer-Policy: No se restringe la información que el navegador envía a otros dominios al seguir enlaces, comprometiendo la privacidad de la navegación.
[MEDIUM] Falta de Permissions-Policy: El sitio no limita el acceso a funciones sensibles del dispositivo del usuario como la cámara o el micrófono.
[MEDIUM] HSTS max-age insuficiente: El tiempo de persistencia de la conexión segura es de solo 30 días, cuando el estándar de seguridad recomienda al menos 180 días.
[LOW] Cabecera Server expuesta: Se revela el uso de Microsoft-IIS/10.0, lo que permite a atacantes identificar vulnerabilidades específicas para esa tecnología.
[LOW] Cabecera X-Powered-By expuesta: Indica que el sitio corre sobre ASP.NET, proporcionando información técnica valiosa para perfilar ataques dirigidos.
[LOW] Ausencia de archivos de control: No se encontraron los archivos robots.txt ni sitemap.xml, necesarios para la gestión adecuada del rastreo y auditoría.