

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://estructuras-siie.tamaulipas.gob.mx
Dominio estructuras-siie.tamaulipas.gob.mx
Fecha 8 de mayo de 2026 a las 22:23

Checks 9 pruebas
Hallazgos 59 totales
Problemas 17 detectados

C

68/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado al portal arroja una puntuación de 68/100 con una calificación de C. Durante la evaluación, se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, se emitió 1 advertencia y se identificaron 2 fallos críticos en la configuración. Aunque el cifrado de datos mediante SSL es correcto, la ausencia total de cabeceras de seguridad y la configuración inadecuada de cookies representan riesgos significativos. Concluimos que el sitio es vulnerable ante ataques de interceptación y manipulación de sesiones. Se recomienda una intervención técnica inmediata para mitigar estas deficiencias.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 146 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
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	__uzma: falta Secure; __uzmb: falta Secure; __uz...
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	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 146 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
146 dias restantes (expira: 2026-10-01T23:59:00Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-24T00:00:00Z
- 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

- 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.)

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

Seguridad de Cookies — 67/100

Estado: AVISO

__uzma: falta Secure; __uzmb: falta Secure; __uzme: falta Secure; __uzmc: falta Secure; __uzmd: falta Secure; __uzmf: falta Secure; uzmx: falta Secure

- **INFO** **Cookies detectadas**
7 cookie(s) encontrada(s)
- **INFO** **Cookie: __uzma — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- **ALTO** **Cookie: __uzma — Secure**
Falta flag Secure — Cookie se envia en conexiones HTTP
- **INFO** **Cookie: __uzma — SameSite**
SameSite=lax
- **INFO** **Cookie: __uzmb — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- **ALTO** **Cookie: __uzmb — Secure**
Falta flag Secure — Cookie se envia en conexiones HTTP

- INFO **Cookie: __uzmb — SameSite**
SameSite=lax
- INFO **Cookie: __uzme — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: __uzme — Secure**
Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: __uzme — SameSite**
SameSite=lax
- INFO **Cookie: __uzmc — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: __uzmc — Secure**
Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: __uzmc — SameSite**
SameSite=lax
- INFO **Cookie: __uzmd — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: __uzmd — Secure**
Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: __uzmd — SameSite**
SameSite=lax
- INFO **Cookie: __uzmf — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: __uzmf — Secure**
Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: __uzmf — SameSite**
SameSite=lax
- INFO **Cookie: uzmx — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: uzmx — Secure**
Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: uzmx — SameSite**
SameSite=lax

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)
- INFO **security.txt**
Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

1 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 — Envío de correo
- **INFO Puerto 80 (HTTP)**
Cerrado — 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 autenticación 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: Ausencia de cabecera que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
- [HIGH] X-Frame-Options: Falta de protección contra Clickjacking, lo que permite que el sitio sea embebido en marcos externos fraudulentos.
- [HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones seguras HSTS, permitiendo posibles degradaciones de protocolo por atacantes.
- [HIGH] Flags de Cookies (Secure): Las cookies __uzma, __uzmb, __uzme, __uzmc, __uzmd, __uzmf y uzmx se envían por canales no cifrados al carecer del atributo de seguridad.
- [MEDIUM] X-Content-Type-Options: El servidor no previene el MIME-type sniffing, aumentando el riesgo de ejecución de scripts disfrazados de otros tipos de archivos.
- [MEDIUM] Archivos Informativos Expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente y pueden revelar detalles técnicos de la infraestructura.
- [MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a otros sitios, lo que puede exponer URLs internas sensibles.
- [MEDIUM] Permissions-Policy: Ausencia de restricciones sobre el acceso de las APIs del navegador a componentes de hardware y software del usuario.
- [LOW] Redirección HTTPS: No se pudo verificar la redirección automática desde HTTP, lo que podría exponer el tráfico inicial de los usuarios.
- [LOW] Robots.txt y Sitemap: La falta de estos archivos dificulta la gestión del rastreo por buscadores y la visibilidad de la estructura del sitio.