EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://plantillaseducacion.tamaulipas.gob.mx	Checks	9 pruebas
Dominio	plantillaseducacion.tamaulipas.gob.mx	Hallazgos	59 totales
Fecha	8 de mayo de 2026 a las 22:21	Problemas	17 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 68/100, lo que equivale a una calificación de nota C. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 5 verificaciones exitosas, 1 advertencia y 2 fallos críticos en la configuración. El informe destaca una carencia absoluta de cabeceras de seguridad y una gestión deficiente en los atributos de las cookies. Se concluye que el sitio es vulnerable debido a la falta de protecciones modernas contra ataques de inyección y suplantación.

Resumen de Riesgos

0	10	5	2	42
CRITICO	ALTO	MEDIO	BAJO	INFO

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: 2026-10-01T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-24T00:00:00.000Z
- 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

- 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 — Envio 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 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 — Previene XSS y ataques de inyección de contenido malicioso.
[HIGH] X-Frame-Options: Falta — Protege al usuario final contra ataques de clickjacking.
[HIGH] Strict-Transport-Security: Falta — No se fuerza la conexión segura mediante HSTS.
[HIGH] Cookies sin flag Secure: Las cookies __uzma, __uzmb, __uzme, __uzmc, __uzmd, __uzmf y uzmx pueden ser enviadas a través de conexiones HTTP no cifradas.
[MEDIUM] X-Content-Type-Options: Falta — Permite el MIME-type sniffing, lo que puede derivar en la ejecución de scripts inesperados.
[MEDIUM] Referrer-Policy: Falta — No hay control sobre la información de navegación que se envía a otros sitios.
[MEDIUM] Permissions-Policy: Falta — No se restringe el acceso de las APIs del navegador a componentes sensibles como cámara o micrófono.
[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente y podrían revelar detalles técnicos del servidor.
[LOW] Ausencia de archivos de rastreo: No se encontraron los archivos robots.txt ni sitemap.xml, necesarios para la correcta indexación y control de bots.