EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://api.sigep.com.mx	Checks	9 pruebas
Dominio	api.sigep.com.mx	Hallazgos	42 totales
Fecha	19 de septiembre de 2026 a las 05:30	Problemas	10 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad de api.sigep.com.mx arrojo una puntuacion de 62/100 con una nota final de C. La evaluacion se baso en nueve checks pasivos, de los cuales cinco resultaron exitosos, uno genero una advertencia y tres fallaron categoricamente. Las principales deficiencias se concentran en la configuracion de las cabeceras de seguridad y la gestion de redirecciones de trafico cifrado. Debido a la falta de politicas para prevenir inyecciones y la exposicion de puertos alternativos, el sitio se clasifica actualmente como vulnerable. Se requiere una intervencion inmediata para elevar los estandares de proteccion de la infraestructura.

Resumen de Riesgos

0	4	3	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 83 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 83 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  83 dias restantes (expira: 2026-12-11T12:32:26.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-12T11:33:41.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: cloudflare — 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
- INFO **Referrer-Policy**
  Presente: same-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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

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 — 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 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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)**
  Abierto (esperado) — 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — 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 ataques de Cross-Site Scripting (XSS) y la carga de contenido malicioso desde fuentes externas.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que permite que un atacante degrade la conexion a HTTP para interceptar datos sensibles.
[HIGH] Redireccion HTTPS: El servidor no redirige automaticamente las peticiones HTTP a HTTPS, permitiendo comunicaciones no cifradas.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera expone al sitio a ataques de MIME-sniffing, donde el navegador interpreta archivos de forma insegura.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente que aplicaciones de terceros accedan a funciones como la camara o el microfono.
[MEDIUM] Puerto 8080 (HTTP-Alt) Abierto: La exposicion de este puerto alternativo aumenta la superficie de ataque y puede revelar servicios administrativos o proxies no protegidos.

[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, informacion que facilita a los atacantes el diseño de vectores especificos basados en esa tecnologia.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor responde con errores 403 para estos archivos, lo que impide una correcta gestion de la indexacion y estructura del sitio.