# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://participa.saltillo.gob.mx | Checks | 9 pruebas |
| Dominio | participa.saltillo.gob.mx | Hallazgos | 42 totales |
| Fecha | 26 de abril de 2026 a las 05:59 | Problemas | 11 detectados |

**C**

61/100

puntos de seguridad

## RESUMEN EJECUTIVO

El analisis de ciberseguridad realizado al dominio revela una puntuacion de 61/100, lo que equivale a una nota de C. Se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos criticos relacionados con la configuracion del servidor. No se realizo un pentest activo en esta sesion, por lo que los hallazgos se limitan a la infraestructura visible y cabeceras de respuesta. Debido a la ausencia total de politicas de seguridad en las cabeceras y la falta de redireccion forzada a protocolos seguros, el sitio se considera vulnerable. El nivel de riesgo actual compromete la integridad de las sesiones de los usuarios y la proteccion contra ataques de inyeccion.

## Resumen de Riesgos

| 0 | 5 | 3 | 3 | 31 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 74 dias |
| Cabeceras de Seguridad | 0 | FALLO | Solo 0/6 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 | 100 | OK | 2 puerto(s) abierto(s), todos esperados |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 74 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  74 dias restantes (expira: 2026-07-08T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-07-09T00:00:00.000Z
- 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

- BAJO **Server header expuesto**
  Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.4.25 — Revela tecnologia del servidor

- 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.)

## Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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)
- 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 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 100/100

Estado: OK

2 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)**
  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
- 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] Ausencia de redireccion HTTPS: El servidor no redirige automaticamente las conexiones inseguras HTTP a HTTPS, permitiendo la interceptacion de datos.
[HIGH] Falta de Strict-Transport-Security (HSTS): No existe una instruccion para que los navegadores utilicen exclusivamente conexiones cifradas, facilitando ataques de degradacion de protocolo.
[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecucion de scripts maliciosos y ataques de Cross-Site Scripting (XSS).
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking al no restringir como debe mostrarse el contenido en marcos o iframes.
[MEDIUM] Falta de X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podria permitir la ejecucion de archivos con contenido malicioso camuflado.

[MEDIUM] Falta de Referrer-Policy: No se controla la informacion de navegacion que se envia a sitios externos mediante el enlace de procedencia.
[MEDIUM] Falta de Permissions-Policy: No existen restricciones sobre el uso de APIs del navegador como la camara, el microfono o la geolocalizacion.
[LOW] Exposicion de cabecera Server: El servidor revela explicitamente el uso de Apache/2.4.51 (Win64), OpenSSL/1.1.1l y PHP/7.4.25, lo que ayuda a atacantes a buscar exploits especificos para esas versiones.
[LOW] Ausencia de archivos de indexacion: No se detectaron los archivos robots.txt ni sitemap.xml, afectando la transparencia hacia los motores de busqueda.