

EscanearVulnerabilidades

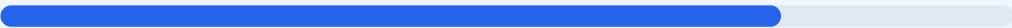
Informe de Seguridad Web

URL	https://www.municipalidaddehuehuetenango.gob.gt/	Checks	9 pruebas
Dominio	www.municipalidaddehuehuetenango.gob.gt	Hallazgos	51 totales
Fecha	12 de abril de 2026 a las 15:31	Problemas	10 detectados

B

77/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 77/100 con una nota final de B. Se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración de cabeceras y cookies. Aunque el cifrado de datos es robusto, la ausencia de políticas de seguridad modernas expone al sitio a vectores de ataque conocidos. En su estado actual, el sitio se considera moderadamente seguro, pero vulnerable a ataques de inyección y manipulación de sesiones.

Resumen de Riesgos

0	4	4	2	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 32 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	CMS detectado: Wix
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	0	FALLO	ssr-caching: falta HttpOnly; ssr-caching: falta ...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 32 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
32 dias restantes (expira: 2026-05-15T00:30:36.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-02-14T00:30:37.000Z
- 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-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
Server: Pepyaka — 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
- INFO

Strict-Transport-Security
Presente: max-age=31556952
- INFO

X-Content-Type-Options
Presente: nosniiff
- 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 301 redirige a https://www.municipalidaddehuehuetenango.gob.gt/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31556952
- BAJO

HSTS includeSubDomains
HSTS no cubre subdominios
- INFO

HSTS max-age
max-age=31556952 (365 dias)
- INFO

Respuesta HTTPS
HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Wix

- 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
Detectado via HTML body
- INFO

Squarespace
No detectado
- BAJO

Meta generator
Expone: Wix.com Website Builder
- INFO

Tecnologias detectadas
React, Next.js

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 — 0/100

Estado: FALLO

ssr-caching: falta HttpOnly; ssr-caching: falta Secure; ssr-caching: falta SameSite

- INFO

Cookies detectadas
1 cookie(s) encontrada(s)
- ALTO

Cookie: ssr-caching — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO

Cookie: ssr-caching — Secure
Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO

Cookie: ssr-caching — SameSite
Falta SameSite — Vulnerable a CSRF

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt
Presente (513 bytes)
- INFO

Reglas robots.txt
4 Disallow, 1 Allow
- MEDIO

Bloqueo total
robots.txt bloquea todo el sitio con Disallow: /
- INFO

Sitemap en robots.txt
<https://www.municipalidaddehuehuetenango.gob.gt/sitemap.xml>
- 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] Content-Security-Policy: La falta de esta cabecera permite ataques de XSS y la inyección de contenido malicioso por parte de terceros.
- [HIGH] X-Frame-Options: No se detectó esta política, lo que deja el sitio expuesto a ataques de clickjacking para engañar a los usuarios.
- [HIGH] Cookie ssl-caching sin HttpOnly: La cookie es accesible mediante scripts de cliente, lo que facilita el robo de sesiones en caso de una vulnerabilidad de scripting.
- [HIGH] Cookie ssl-caching sin Secure: El identificador se transmite en conexiones no cifradas, permitiendo su captura por atacantes en redes locales.
- [MEDIUM] Cookie ssl-caching sin SameSite: La ausencia de este atributo aumenta el riesgo de ataques de falsificación de solicitudes entre sitios (CSRF).
- [MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a otros dominios al hacer clic en enlaces externos.
- [MEDIUM] Permissions-Policy: El navegador no tiene restricciones para acceder a hardware o APIs sensibles como cámara, micrófono o geolocalización.
- [MEDIUM] Configuración de robots.txt: El archivo bloquea actualmente todo el contenido del sitio, lo que impide una indexación correcta en motores de búsqueda.
- [LOW] Server header expuesto: El servidor revela el uso de la tecnología Pepyaka, facilitando la búsqueda de exploits específicos para esa versión.
- [LOW] Meta generator expuesto: El código fuente confirma públicamente el uso de Wix.com Website Builder como gestor de contenidos.