

Escanear Vulnerabilidades

Informe de Seguridad Web

URL	https://bienmun.veracruzmunipio.gob.mx/Beca-Joven-Heroe-Veracruzano-Ivan-Gonzalez/	Checks	9 ejecutados
Dominio	bienmun.veracruzmunipio.gob.mx	Hallazgos	45 totales
Fecha	29 de septiembre de 2026 a las 23:45	Problemas	13 detectados

C

62/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 62/100, lo que equivale a una nota de C. De los 9 checks pasivos ejecutados, se obtuvieron 5 resultados satisfactorios, 1 advertencia y 3 fallos críticos relacionados con la configuración de red y cabeceras. La ausencia total de políticas de seguridad en las cabeceras HTTP y la gestión deficiente de las cookies de sesión representan riesgos de seguridad considerables. En su estado actual, el sitio se considera vulnerable a ataques de secuestro de sesión y redirecciones maliciosas, por lo que requiere intervención técnica inmediata.

Resumen de Riesgos

0 CRITICO	6 ALTO	4 MEDIO	3 BAJO	32 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 42 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
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 42 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
42 dias restantes (expira: 2026-11-11T02:12:51.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-13T02:12:52.000Z
- 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 — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://bienmun.veracruzmunipicio.gob.mx/
- 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 — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO

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

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

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

Cookie: PHPSESSID — 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 — 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] Content-Security-Policy: Falta de política de seguridad que ayuda a prevenir ataques de inyección de código y XSS.

[HIGH] X-Frame-Options: La cabecera está ausente, permitiendo que el sitio sea insertado en marcos externos, lo cual facilita ataques de clickjacking.

[HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones seguras, permitiendo posibles ataques de degradación de protocolo mediante intermediarios.

[HIGH] Cookie PHPSESSID - HttpOnly: La cookie de sesión no tiene el flag de seguridad activado, permitiendo que sea leída por scripts maliciosos del navegador.

[HIGH] Cookie PHPSESSID - Secure: La cookie se transmite sin cifrar en conexiones HTTP, lo que expone la sesión del usuario a ser interceptada en redes locales.

[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que los navegadores intenten adivinar el tipo de contenido, facilitando ataques de ejecución de archivos.

[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a otros dominios cuando el usuario hace clic en enlaces externos.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones del hardware del usuario, como la cámara o el micrófono, mediante políticas del navegador.

[MEDIUM] Cookie PHPSESSID - SameSite: Falta de control en el envío de cookies entre diferentes sitios, lo que aumenta la exposición a ataques de falsificación de solicitudes (CSRF).

[LOW] Server header expuesto: El servidor revela el uso de software Apache, información que facilita a los atacantes la búsqueda de vulnerabilidades específicas para esa tecnología.

[LOW] robots.txt y sitemap.xml: La ausencia de estos archivos dificulta el control sobre el rastreo de motores de búsqueda y la organización de la estructura del sitio.