EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://traxionglobal.com.mx	Checks	9 pruebas
Dominio	traxionglobal.com.mx	Hallazgos	43 totales
Fecha	26 de mayo de 2026 a las 16:57	Problemas	14 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web ha arrojado una puntuación de 57/100, lo que corresponde a una calificación de nota D. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 5 verificaciones correctas, 1 advertencia y 3 fallos críticos en la configuración. A pesar de contar con un certificado SSL válido, la ausencia total de cabeceras de seguridad y la exposición de puertos administrativos representan un riesgo significativo. Por lo tanto, se concluye que el sitio es actualmente vulnerable y requiere intervenciones técnicas inmediatas para proteger la integridad de los datos y la privacidad de los usuarios.

Resumen de Riesgos

0	6	4	4	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 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	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  90 dias restantes (expira: 2026-08-24T07:33:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-26T07:34:00.000Z
- 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: LiteSpeed — 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 301 — 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
- BAJO **Meta generator**
  Expone: HubSpot

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 — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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 ausencia de esta cabecera permite ataques de inyección de código como XSS y la carga de contenido malicioso desde dominios externos.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de Clickjacking, permitiendo que atacantes oculten la web en marcos invisibles para engañar a los usuarios.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, facilitando ataques de degradación de SSL (Man-in-the-Middle).
[HIGH] HTTP a HTTPS redireccion: El servidor no redirige automáticamente el tráfico inseguro al protocolo cifrado, dejando expuesta la comunicación inicial.
[HIGH] Puerto 21 (FTP): Este puerto está abierto y utiliza un protocolo que transmite credenciales y archivos en texto plano, siendo un objetivo primario para interceptación.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede llevar a la ejecución de scripts camuflados como otros tipos de archivos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios, lo que podría filtrar URLs internas sensibles.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la cámara o el micrófono, aumentando la superficie de ataque en el lado del cliente.
[MEDIUM] Puerto 22 (SSH): El puerto de acceso remoto está expuesto, lo que facilita intentos de intrusión mediante ataques de fuerza bruta si no está debidamente protegido.
[LOW] Server header expuesto: La cabecera revela el uso de LiteSpeed, proporcionando información valiosa a un atacante sobre la tecnología del servidor.
[LOW] Meta generator: Se expone el uso de HubSpot en el código fuente, ayudando a perfilar la infraestructura del sitio.
[LOW] robots.txt: El archivo no fue encontrado, lo que dificulta el control de la indexación por parte de motores de búsqueda.
[LOW] sitemap.xml: La ausencia de este archivo puede afectar la visibilidad y el rastreo estructurado del sitio.