EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://erp.estrategiaeinnovacion.com.mx/	Checks	9 pruebas
Dominio	erp.estrategiaeinnovacion.com.mx	Hallazgos	51 totales
Fecha	24 de abril de 2026 a las 19:56	Problemas	6 detectados

B

89/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 89/100, lo que otorga una nota de grado B. Se ejecutaron un total de 9 verificaciones pasivas, resultando en 6 verificaciones exitosas y 3 advertencias técnicas, sin registrar fallos críticos totales. El sistema demuestra una implementación robusta de cifrado y cabeceras de seguridad, aunque presenta debilidades en la configuración de cookies y exposición de servicios. En su estado actual, el sitio se considera mayormente seguro, pero es vulnerable a ataques de interceptación de sesión y reconocimiento de infraestructura si no se aplican las correcciones recomendadas.

Resumen de Riesgos

0	3	1	2	45
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	50	AVISO	XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Se...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 79 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  79 dias restantes (expira: 2026-07-12T09:53:25.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-13T09:53:26.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO **Server header expuesto**
  Server: nginx — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src '...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: camera=(), microphone=(), geolocation=(), payment=(), usb=(), fullscreen=(self)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://erp.estrategiaeinnovacion.com.mx/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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 — 50/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Secure; laravel-session: falta Secure

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: XSRF-TOKEN — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: laravel-session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: laravel-session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: laravel-session — SameSite**
  SameSite=lax

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — 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] Cookie XSRF-TOKEN: Falta el atributo HttpOnly, lo que permite que la cookie sea accesible mediante scripts del lado del cliente, aumentando el riesgo de ataques Cross-Site Scripting (XSS).
[HIGH] Cookie XSRF-TOKEN: Falta el flag Secure, permitiendo que el token se transmita a través de conexiones HTTP no cifradas, lo que facilita el robo de información en redes inseguras.
[HIGH] Cookie laravel-session: Ausencia del flag Secure, lo que implica que la sesión del usuario podría ser interceptada si la comunicación no se mantiene exclusivamente bajo HTTPS.
[MEDIUM] Puerto 22 (SSH) abierto: La detección de un puerto de administración remota expuesto facilita intentos de acceso no autorizado mediante ataques de fuerza bruta.
[LOW] Cabecera Server expuesta: El servidor revela el uso de nginx, proporcionando información técnica que ayuda a un atacante a buscar vulnerabilidades específicas del software.
[LOW] Archivo sitemap.xml no encontrado: La falta de este archivo dificulta la auditoría de rutas legítimas y la correcta indexación de la estructura del sitio.