EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://portal.elektravales.com.mx	Checks	9 pruebas
Dominio	portal.elektravales.com.mx	Hallazgos	39 totales
Fecha	21 de julio de 2026 a las 00:36	Problemas	9 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio portal.elektravales.com.mx arroja una puntuación de 72/100, lo que equivale a una nota C. Se ejecutaron 9 checks pasivos, resultando en 6 verificaciones exitosas y 2 fallos críticos relacionados con la configuración del servidor. El portal cuenta con un cifrado de conexión robusto, pero carece por completo de cabeceras de seguridad esenciales para proteger a los usuarios. Por lo tanto, se concluye que el sitio es vulnerable ante ataques de inyección y manipulación de interfaz.

Resumen de Riesgos

0	3	3	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 99 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 99 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  99 dias restantes (expira: 2026-10-27T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-13T00:00:00.000Z
- 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: awselb/2.0 — 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.)

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 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 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)**
  Cerrado — 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 esta cabecera, lo que permite la ejecución de ataques Cross-Site Scripting (XSS) y la inyección de contenido no autorizado.
[HIGH] X-Frame-Options: La ausencia de esta política deja al portal expuesto a ataques de clickjacking, donde un tercero puede cargar el sitio en marcos invisibles.
[HIGH] Strict-Transport-Security: No se detectó HSTS, lo que impide forzar de manera estricta las conexiones cifradas y facilita ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: Al faltar esta configuración, el navegador puede intentar interpretar archivos con tipos MIME incorrectos, aumentando el riesgo de ejecución de scripts.
[MEDIUM] Referrer-Policy: No se controla la información de origen enviada a otros dominios, lo que podría comprometer la privacidad técnica de la navegación.
[MEDIUM] Permissions-Policy: El servidor no restringe el acceso a APIs sensibles del navegador, como la cámara o el micrófono, mediante políticas explícitas.
[LOW] Server header expuesto: Se detectó el valor awselb/2.0, revelando información sobre la infraestructura que ayuda a potenciales atacantes en la fase de reconocimiento.
[LOW] Archivos de configuración faltantes: No se localizaron los archivos robots.txt ni sitemap.xml debido a errores de acceso 403, dificultando la auditoría de rastreo.