EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://web.sanmiguel.cl/	Checks	9 pruebas
Dominio	web.sanmiguel.cl	Hallazgos	47 totales
Fecha	22 de mayo de 2026 a las 08:42	Problemas	16 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web.sanmiguel.cl ha resultado en una puntuación de 62/100, obteniendo una calificación de grado C. El análisis consistió en 9 checks pasivos, de los cuales 4 fueron superados con éxito, 3 generaron advertencias y 2 resultaron en fallos críticos de seguridad. Se han detectado debilidades significativas debido al uso de software desactualizado y la ausencia total de cabeceras de protección en el servidor. Debido a la exposición de versiones específicas del CMS y la falta de políticas de seguridad modernas, el sitio se considera vulnerable ante ataques dirigidos y automatizados.

Resumen de Riesgos

0	5	7	4	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 55 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	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 4.9.26 expuesta, WordPress 2.7 expuest...
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 55 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  55 dias restantes (expira: 2026-07-16T06:06:57.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-17T06:06:58.000Z
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://web.sanmiguel.cl/
- 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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 4.9.26

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 4.9.26 expuesta, WordPress 2.7 expuesta

- ALTO **WordPress version**
  Version 4.9.26 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://magenda.ingelan.cl/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://magenda.ingelan.cl/

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (286 bytes)
- INFO **Reglas robots.txt**
  13 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — 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 facilita la ejecución de ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Falta de protección contra ataques de clickjacking, permitiendo que el sitio sea embebido en marcos maliciosos.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce conexiones seguras y deja la sesión expuesta a ataques de degradación.
[HIGH] WordPress version: Se expone públicamente la versión 4.9.26, permitiendo que actores malintencionados busquen exploits específicos para las vulnerabilidades conocidas en dicha versión.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede llevar a la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No se controla la información que el navegador envía en la cabecera Referer al navegar hacia otros sitios.
[MEDIUM] Permissions-Policy: No se definen restricciones sobre el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y revela información técnica sensible sobre la instalación del CMS.
[MEDIUM] Ruta /wp-login.php: El punto de acceso administrativo es visible para cualquier usuario, aumentando el riesgo de ataques de fuerza bruta.
[MEDIUM] Recurso HTTP: Se detectaron dos recursos (hojas de estilo) cargados desde magenda.ingelan.cl a través de conexiones no cifradas, comprometiendo la integridad del sitio.
[LOW] Server header expuesto: El servidor revela el uso de LiteSpeed, proporcionando información útil para el reconocimiento de la infraestructura por parte de atacantes.
[LOW] Meta generator: El código fuente muestra explícitamente el uso de WordPress 4.9.26, facilitando la identificación del CMS.
[LOW] Ruta sensible en robots.txt: Se mencionan directorios relacionados con la administración, guiando a posibles atacantes hacia áreas críticas.
[LOW] sitemap.xml: La ausencia de este archivo dificulta la correcta gestión e indexación de la estructura del portal.