EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.mitenisclub.cl	Checks	9 pruebas
Dominio	www.mitenisclub.cl	Hallazgos	45 totales
Fecha	14 de julio de 2026 a las 13:15	Problemas	9 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

Se ha realizado una auditoría de seguridad pasiva sobre el dominio mitenisclub.cl obteniendo una puntuación final de 85/100 con una calificación de nota B. De los 9 controles pasivos ejecutados, 7 resultaron satisfactorios y 2 presentaron fallos relacionados con la configuración de cabeceras y la ausencia de archivos de indexación. El cifrado de datos y la gestión de puertos muestran una postura sólida, aunque la carencia de políticas de seguridad en el servidor representa un riesgo latente. En conclusión, el sitio web presenta un nivel de seguridad aceptable, pero se considera vulnerable ante ataques de inyección y suplantación de identidad debido a omisiones técnicas en la configuración del servidor.

Resumen de Riesgos

0	2	7	0	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 176 dias
Cabeceras de Seguridad	45	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
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	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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 176 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  176 dias restantes (expira: 2027-01-06T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-06T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Permissions-Policy

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=10886400; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.mitenisclub.cl/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=10886400; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- MEDIO **HSTS max-age**
  max-age=10886400 (126 dias) — Recomendado minimo 180 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
- INFO **Tecnologias detectadas**
  React, Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.

[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible para engañar al usuario.
[MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] HSTS max-age: El valor actual de 126 días es inferior al estándar recomendado de al menos 180 días para garantizar una conexión cifrada prolongada.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede revelar información técnica sobre la infraestructura o versiones del software.
[MEDIUM] Archivo /README.txt: La exposición de este archivo facilita la obtención de datos sensibles sobre el sistema por parte de terceros.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo está expuesto, facilitando ataques de fuerza bruta.
[MEDIUM] Ruta /administrator/: Se detectó un panel de gestión accesible que incrementa la superficie de ataque para accesos no autorizados.
[MEDIUM] Ruta /user/login: Punto de entrada de usuarios visible que requiere medidas de protección adicionales.
[FAIL] Robots.txt y Sitemap: La falta de estos archivos dificulta la gestión de lo que los motores de búsqueda deben indexar y puede exponer rutas privadas por descuido.