EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://metis.clinicaimet.cl/Login	Checks	9 pruebas
Dominio	metis.clinicaimet.cl	Hallazgos	44 totales
Fecha	12 de mayo de 2026 a las 16:00	Problemas	13 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

La evaluacion de seguridad de metis.clinicaimet.cl arrojo una puntuacion de 64/100, lo que equivale a una nota C. Se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron calificados como fallos. Los hallazgos principales incluyen la ausencia total de cabeceras de seguridad y una expiracion critica del certificado SSL en el corto plazo. En su estado actual, el sitio se considera vulnerable debido a la falta de protecciones fundamentales contra ataques de inyeccion y suplantacion.

Resumen de Riesgos

0	5	5	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	50	AVISO	Certificado expira en 8 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	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	No se detectaron puertos abiertos

SSL/TLS — 50/100

Estado: AVISO

Certificado expira en 8 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- ALTO **Dias hasta expiracion**
  8 dias restantes (expira: 2026-05-20T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-05-14T00:00:00.000Z
- 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: nginx/1.24.0 — 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.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://metis.clinicaimet.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

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)
- 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

- 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 — 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] Expiracion de SSL: El certificado actual expira en solo 8 dias, lo que provocara alertas de seguridad para los usuarios.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de XSS e inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: No esta configurada, dejando el portal vulnerable a ataques de secuestro de clics o clickjacking.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce siempre conexiones cifradas, facilitando ataques man-in-the-middle.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede derivar en la ejecucion de archivos peligrosos.
[MEDIUM] Referrer-Policy: No existe control sobre la informacion de referencia enviada, lo que podria filtrar rutas internas a terceros.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el uso no autorizado de hardware como la camara.
[MEDIUM] Rutas de login expuestas: Los paneles en /administrator/ y /user/login son accesibles publicamente, facilitando ataques de fuerza bruta.
[LOW] Server header expuesto: El servidor revela el uso de nginx/1.24.0, permitiendo a atacantes buscar vulnerabilidades especificas para esa version.
[LOW] Archivos de indexacion faltantes: No se encontraron robots.txt ni sitemap.xml, lo que dificulta la gestion del rastreo por buscadores.