EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://medicitasnic.com	Checks	9 pruebas
Dominio	medicitasnic.com	Hallazgos	44 totales
Fecha	20 de septiembre de 2026 a las 05:15	Problemas	11 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado a medicitasnic.com ha arrojado una puntuación de 76/100, otorgando una nota final de B. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 6 verificaciones satisfactorias, 1 advertencia y 2 fallos críticos relacionados con la configuración del servidor. Aunque el sitio implementa correctamente el cifrado de datos mediante SSL, la exposición de servicios internos compromete la infraestructura. Se concluye que el sitio es actualmente vulnerable debido a la apertura de puertos sensibles que podrían permitir accesos no autorizados.

Resumen de Riesgos

2	2	4	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 88 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 3389 (RD...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 88 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  88 dias restantes (expira: 2026-12-16T19:19:17.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-17T19:19:18.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Microsoft-IIS/10.0 — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=2592000
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://medicitasnic.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=2592000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- MEDIO **HSTS max-age**
  max-age=2592000 (30 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

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 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 3389 (RDP), 5432 (PostgreSQL)

- 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
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3389 (RDP) abierto: Permite el acceso por escritorio remoto de Windows, facilitando ataques de fuerza bruta o intrusiones directas al servidor.
[CRITICAL] Puerto 5432 (PostgreSQL) abierto: La base de datos está expuesta públicamente, lo que aumenta el riesgo de robo de información sensible o ataques de inyección.

[HIGH] Content-Security-Policy (CSP) faltante: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).
[HIGH] X-Frame-Options faltante: El sitio no protege contra ataques de clickjacking, permitiendo que la web sea cargada dentro de marcos externos maliciosos.
[MEDIUM] X-Content-Type-Options faltante: Facilita ataques de sniffing de tipos MIME, permitiendo que el navegador interprete archivos de forma insegura.
[MEDIUM] HSTS max-age insuficiente: El tiempo de protección de 30 días es inferior a los 180 días recomendados para garantizar una navegación segura prolongada.
[MEDIUM] Referrer-Policy faltante: No se controla la información que el navegador envía a otros sitios al seguir enlaces, comprometiendo la privacidad de la navegación.
[MEDIUM] Permissions-Policy faltante: El servidor no restringe el acceso a funciones del dispositivo como la cámara o el micrófono a través del navegador.
[LOW] Server header expuesto: El encabezado revela el uso de Microsoft-IIS/10.0, proporcionando información valiosa a atacantes para buscar exploits específicos.
[LOW] Archivos de indexación faltantes: No se encontraron los archivos robots.txt ni sitemap.xml, lo que afecta el control de rastreo y la visibilidad en buscadores.