EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.clinicachinita.com/	Checks	9 pruebas
Dominio	www.clinicachinita.com	Hallazgos	50 totales
Fecha	13 de abril de 2026 a las 22:16	Problemas	21 detectados

D

55/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 55/100, lo que resulta en una calificación de grado D. Se ejecutaron 9 chequeos pasivos, de los cuales 3 finalizaron correctamente, 3 generaron advertencias y 3 resultaron en fallos críticos de seguridad. Los hallazgos revelan deficiencias graves en la protección de datos y una exposición innecesaria de la infraestructura del servidor. Por lo tanto, se concluye que el sitio es actualmente vulnerable y requiere intervenciones técnicas inmediatas para mitigar riesgos de intrusión.

Resumen de Riesgos

1	6	12	2	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 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
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	33	FALLO	clinica_panamericana_session: falta Secure; clin...
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  90 dias restantes (expira: 2026-07-12T21:45:22.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-13T21:45:22.000Z
- 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: Apache — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.4.33 — Revela framework/lenguaje
- 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://www.clinicachinita.com/
- 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

- INFO **WordPress**
  Detectado via HTML body
- 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**
  Next.js, PHP/7.4.33

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 — 33/100

Estado: FALLO

clinica_panamericana_session: falta Secure; clinica_panamericana_session: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: clinica_panamericana_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: clinica_panamericana_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: clinica_panamericana_session — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://181.129.45.250:8081/calidad/modulos/pqrs/recepcion_pq...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://181.129.45.250:8081/calidad/modulos/pqrs/seguimiento....

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
  Presente, 97 URLs
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos está expuesta directamente a internet, permitiendo ataques de fuerza bruta y acceso no autorizado a información sensible.
[HIGH] Ausencia de Content-Security-Policy: No existe una política que restrinja el origen del contenido, facilitando ataques de inyección de código y XSS.
[HIGH] Ausencia de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking al permitir que sea cargado dentro de marcos en sitios externos no autorizados.
[HIGH] Falta de Strict-Transport-Security (HSTS): El servidor no obliga a los navegadores a usar conexiones cifradas, permitiendo posibles ataques de degradación de protocolo.
[HIGH] Cookie de sesión sin flag Secure: La cookie clinica_panamericana_session puede ser transmitida por canales no cifrados, arriesgando el robo de sesiones de usuario.
[HIGH] Puerto 21 (FTP) abierto: El servicio de transferencia de archivos está activo y es propenso a la interceptación de credenciales en texto plano.
[MEDIUM] Ausencia de SameSite en cookies: La falta de este atributo en las cookies de sesión hace que el sitio sea vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido mixto detectado: Existen recursos cargados mediante HTTP inseguro dentro de la página HTTPS, lo que debilita la integridad general del cifrado.
[MEDIUM] Rutas de administración expuestas: Los paneles de acceso en /wp-login.php, /administrator/ y /user/login son accesibles públicamente para cualquier atacante.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de acceso remoto está expuesto, aumentando la superficie de ataque para intentos de ingreso al sistema operativo del servidor.
[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son públicos y pueden revelar detalles técnicos internos del CMS WordPress.
[MEDIUM] Ausencia de X-Content-Type-Options: Permite que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecución de scripts maliciosos disfrazados.
[MEDIUM] Ausencia de Referrer-Policy y Permissions-Policy: No se controla la información de procedencia enviada a terceros ni se restringen las funciones sensibles del navegador.
[WARN] Falta de archivo robots.txt: No se proporcionan instrucciones de rastreo a los motores de búsqueda, dificultando la gestión de la visibilidad del sitio.
[LOW] Cabecera Server expuesta: El servidor informa que utiliza Apache, facilitando a los atacantes la búsqueda de vulnerabilidades específicas para esa tecnología.
[LOW] Cabecera X-Powered-By expuesta: Se revela el uso de PHP/7.4.33, exponiendo la versión exacta del lenguaje de programación utilizado.