EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://hospitalprivado.com.ar/historiaclinicaweb/	Checks	9 pruebas
Dominio	hospitalprivado.com.ar	Hallazgos	43 totales
Fecha	12 de mayo de 2026 a las 21:43	Problemas	9 detectados

C

74/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el portal ha dado como resultado una puntuación de 74/100, lo que otorga una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, identificando 6 resultados satisfactorios, 2 advertencias y 1 fallo crítico en la configuración de seguridad. A pesar de contar con un cifrado de conexión robusto, la plataforma carece de protecciones esenciales contra ataques modernos de inyección y suplantación. Por lo tanto, se concluye que el sitio es vulnerable ante vectores de ataque que aprovechan la falta de cabeceras de seguridad en el servidor.

Resumen de Riesgos

0	4	3	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 193 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 193 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  193 dias restantes (expira: 2026-11-21T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-07T00:00:00.000Z
- 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 — 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://hospitalprivado.com.ar/
- 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)
- 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (135 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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 la ejecución de scripts maliciosos y ataques de inyección de contenido, aumentando el riesgo de XSS.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking donde un atacante puede cargar la página en un marco invisible para engañar al usuario.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras por defecto, permitiendo posibles degradaciones de protocolo a HTTP.
[MEDIUM] X-Content-Type-Options: Sin esta protección, el navegador podría intentar interpretar el contenido de forma distinta al tipo MIME declarado, facilitando ataques de sniffing.

[MEDIUM] Referrer-Policy: No existe un control sobre la información de navegación que se envía a servidores externos al seguir enlaces salientes.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono, dejando expuestas funcionalidades innecesarias.
[LOW] Server header expuesto: El servidor revela el uso de nginx, proporcionando información técnica que ayuda a un atacante a buscar vulnerabilidades específicas del software.
[LOW] sitemap.xml: El archivo no fue localizado, lo que puede afectar la indexación correcta y el análisis de la estructura del sitio.