EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.clinicamirave.es/	Checks	9 pruebas
Dominio	www.clinicamirave.es	Hallazgos	46 totales
Fecha	28 de septiembre de 2026 a las 15:45	Problemas	15 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha resultado en una puntuación de 60/100, obteniendo una calificación de grado C. El análisis se basó en 9 checks pasivos, de los cuales 5 fueron satisfactorios, 1 generó una advertencia y 3 fallaron debido a configuraciones críticas. Se han detectado deficiencias graves en la exposición de servicios de infraestructura y una ausencia total de cabeceras de seguridad fundamentales. Por tanto, se concluye que el sitio es vulnerable y presenta riesgos significativos que requieren atención inmediata.

Resumen de Riesgos

2	6	5	2	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 53 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, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.1.1 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 53 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  53 dias restantes (expira: 2026-11-21T02:25:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-23T02:25:30.000Z
- 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://www.clinicamirave.es/
- 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, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 7.1.1
- INFO **Tecnologias detectadas**
  Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.1.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.1.1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (210 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://www.clinicamirave.es/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — 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 3306 (MySQL) abierto: La base de datos principal se encuentra expuesta a internet, permitiendo ataques directos de fuerza bruta o explotación de credenciales.
[CRITICAL] Puerto 5432 (PostgreSQL) abierto: Exposición de un segundo motor de base de datos, incrementando la superficie de ataque y el riesgo de exfiltración de datos.
[HIGH] Puerto 21 (FTP) abierto: El uso de este protocolo implica la transferencia de archivos y credenciales sin cifrado, facilitando la interceptación de datos.
[HIGH] Content-Security-Policy faltante: La ausencia de esta política permite la ejecución de ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options faltante: El sitio es vulnerable a ataques de clickjacking al no restringir cómo se puede embeber la página en marcos externos.
[HIGH] Strict-Transport-Security (HSTS) no configurado: El servidor no obliga al navegador a usar conexiones seguras, permitiendo ataques de degradación de protocolo (SSL Stripping).
[HIGH] Exposición de versión de WordPress (7.1.1): Revelar públicamente la versión del CMS facilita a los atacantes el uso de exploits específicos para vulnerabilidades conocidas.
[MEDIUM] X-Content-Type-Options faltante: La falta de esta cabecera permite ataques de sniffing de tipos MIME, donde el navegador interpreta archivos de forma maliciosa.
[MEDIUM] Panel de login (/wp-login.php) accesible: El acceso público a la ruta administrativa permite intentos de acceso no autorizado y ataques de diccionario.
[MEDIUM] Archivo /readme.html expuesto: Este archivo revela información técnica sobre la instalación del CMS que ayuda en las fases de reconocimiento de un ataque.
[MEDIUM] Referrer-Policy y Permissions-Policy faltantes: Se carece de control sobre la información de navegación enviada y sobre las APIs del navegador permitidas.
[LOW] Cabecera Server expuesta: El servidor nginx revela su nombre, proporcionando pistas tecnológicas útiles para un atacante.
[LOW] Meta generator expuesto: La etiqueta meta confirma el uso de versiones específicas de software en el código fuente.