EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.clinicauhalde.com/	Checks	9 pruebas
Dominio	www.clinicauhalde.com	Hallazgos	46 totales
Fecha	26 de abril de 2026 a las 17:16	Problemas	15 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación exacta de 60/100, lo que otorga una calificación de nota C. Se ejecutaron un total de 9 checks pasivos, resultando en 5 verificaciones correctas, 1 advertencia y 3 fallos críticos en la configuración. El sistema presenta riesgos significativos debido a la exposición de servicios internos y la ausencia total de cabeceras de protección en el servidor. Por lo tanto, el sitio se concluye como vulnerable, requiriendo atención inmediata para mitigar posibles intrusiones o fugas de datos.

Resumen de Riesgos

1	6	6	2	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 66 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	20	FALLO	WordPress 6.4.8 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 66 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  66 dias restantes (expira: 2026-07-01T08:17:06.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-02T08:17:07.000Z
- 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: HTTPd — 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.clinicauhalde.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
- BAJO **Meta generator**
  Expone: WordPress 6.4.8
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.4.8 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.4.8 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 (92 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://clinicauhalde.com/index.php/sitemap.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
- 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): Base de datos expuesta públicamente, lo que permite ataques directos de fuerza bruta o explotación de vulnerabilidades del motor.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos abierto que utiliza protocolos no cifrados, facilitando la interceptación de credenciales.
[HIGH] Content-Security-Policy: Cabecera ausente que permite ataques de inyección de contenido y ejecución de scripts maliciosos (XSS).
[HIGH] X-Frame-Options: Falta de protección contra Clickjacking, permitiendo que el sitio sea cargado en marcos externos para engañar a usuarios.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS, dejando a los usuarios vulnerables a ataques de degradación de conexión.
[HIGH] WordPress version: La versión 6.4.8 se encuentra expuesta, lo que permite a atacantes buscar exploits específicos para esta edición del CMS.
[MEDIUM] Puerto 22 (SSH): El puerto de acceso remoto está abierto, aumentando la superficie de ataque y el riesgo de acceso no autorizado al servidor.
[MEDIUM] X-Content-Type-Options: Ausencia de la cabecera que previene al navegador de interpretar archivos con tipos MIME incorrectos.
[MEDIUM] Referrer-Policy: No existe una política definida para el control de la información enviada en las peticiones de referencia.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador como la cámara o el micrófono a través de políticas de seguridad.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y confirma detalles técnicos sobre la instalación de WordPress.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo está expuesto sin restricciones de red, facilitando intentos de inicio de sesión no autorizados.
[LOW] Server header expuesto: El servidor revela el uso de HTTPd, proporcionando información valiosa a posibles atacantes sobre la infraestructura.
[LOW] Meta generator: La etiqueta meta expone explícitamente la versión de WordPress utilizada.