EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://chpmaco.b2b.siesadigital.net/	Checks	9 pruebas
Dominio	chpmaco.b2b.siesadigital.net	Hallazgos	43 totales
Fecha	15 de mayo de 2026 a las 14:22	Problemas	11 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría de seguridad en el sitio web, se ha obtenido una puntuación exacta de 72/100 con una calificación de grado C. El análisis se basó en la ejecución de 9 checks pasivos, de los cuales 6 resultaron exitosos, 1 generó una advertencia y 2 finalizaron en fallo. A pesar de contar con un cifrado de conexión válido, la ausencia total de cabeceras de seguridad críticas debilita la protección contra ataques de inyección y suplantación. Se concluye que el sitio es actualmente vulnerable debido a configuraciones de servidor incompletas que podrían ser aprovechadas por agentes malintencionados.

Resumen de Riesgos

0	4	4	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 103 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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 103 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  103 dias restantes (expira: 2026-08-26T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-07-28T00:00:00.000Z
- 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: Apache/2.4.38 (Debian) — 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://chpmaco.b2b.siesadigital.net:443/
- 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)
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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 500)
- BAJO **sitemap.xml**
  No encontrado (HTTP 500)
- 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: Falta — Previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Falta — Protege a los usuarios contra ataques de clickjacking que buscan engañarlos para realizar acciones no deseadas.
[HIGH] Strict-Transport-Security: Falta — Obliga al navegador a usar siempre conexiones HTTPS, evitando ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: Falta — Impide que el navegador interprete archivos de forma distinta a su tipo MIME declarado, evitando la ejecución de scripts ocultos.
[MEDIUM] Referrer-Policy: Falta — Controla cuánta información sobre la procedencia del usuario se comparte con otros dominios.
[MEDIUM] Permissions-Policy: Falta — No restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] Ruta /user/login expuesta: El panel de acceso es públicamente visible, lo que aumenta la superficie de ataque para intentos de fuerza bruta.

[LOW] Server header expuesto: Se revela la versión específica Apache/2.4.38 (Debian), facilitando a un atacante la búsqueda de exploits conocidos para esa versión.
[LOW] Archivos robots.txt y sitemap.xml ausentes: El servidor devuelve un error interno (HTTP 500) al intentar acceder a estos archivos, indicando una configuración incorrecta.