EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.cacpeco.com/	Checks	9 pruebas
Dominio	www.cacpeco.com	Hallazgos	46 totales
Fecha	15 de julio de 2026 a las 21:40	Problemas	12 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de ciberseguridad realizado al sitio cacpeco.com arroja una puntuacion de 64/100, lo que equivale a una nota C. Durante la evaluacion se ejecutaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 2 advertencias y 2 fallos criticos que comprometen la integridad del servidor. Se detecto una ausencia total de cabeceras de seguridad esenciales y la exposicion publica de versiones de software desactualizadas. Aunque el cifrado de datos es correcto, la configuracion estructural del sitio presenta debilidades importantes frente a ataques de inyeccion y secuestro de sesiones. En conclusion, el sitio se considera vulnerable debido a una superficie de ataque innecesariamente expuesta y falta de politicas de proteccion modernas.

Resumen de Riesgos

0	5	4	3	34
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, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.0 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

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: 2026-09-20T02:37:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-22T01:37:44.000Z
- 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: cloudflare — 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.cacpeco.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, 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: Powered by LayerSlider 7.14.4 - Build Heros, Sliders, and Popups. Create Animations and Beautiful, Rich Web Content as Easy as Never Before on WordPress.
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0 expuesta

- ALTO **WordPress version**
  Version 7.0 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

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 (305 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.cacpeco.com/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] WordPress version: La version 7.0 se encuentra expuesta publicamente, lo que facilita a atacantes la identificacion de vulnerabilidades conocidas para este CMS.
[HIGH] Content-Security-Policy (CSP): Esta cabecera esta ausente, dejando el sitio vulnerable a ataques de Cross-Site Scripting (XSS) e inyeccion de codigo malicioso.
[HIGH] X-Frame-Options: No se detecto esta cabecera, lo que permite que el sitio sea cargado en marcos externos y sea susceptible a ataques de clickjacking.
[HIGH] Strict-Transport-Security (HSTS): La falta de esta configuracion impide que el navegador fuerce conexiones seguras permanentemente, permitiendo ataques de degradacion de protocolo.
[MEDIUM] X-Content-Type-Options: La ausencia de esta directiva permite que el navegador realice sniffing de tipos MIME, lo que podria derivar en la ejecucion de archivos no autorizados.
[MEDIUM] Referrer-Policy: No existe una politica definida, lo que podria filtrar informacion sensible de la URL a dominios externos cuando un usuario hace clic en un enlace.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la camara o el microfono, aumentando el riesgo de uso no autorizado por scripts de terceros.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detecto el puerto abierto, lo que representa un vector de entrada adicional para servicios alternativos o proxies no documentados.
[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, proporcionando pistas sobre la infraestructura tecnologica a posibles atacantes.
[LOW] Meta generator: Se expone informacion detallada sobre el complemento LayerSlider 7.14.4, facilitando la busqueda de exploits especificos para dicho plugin.
[LOW] Ruta sensible en robots.txt: La referencia directa a la ruta admin puede ayudar a bots maliciosos a localizar areas de gestion interna del sitio web.