

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://pcpd.es/	Checks	9 pruebas
Dominio	pcpd.es	Hallazgos	45 totales
Fecha	8 de octubre de 2026 a las 11:18	Problemas	13 detectados

C

70/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha arrojado una puntuación de 70/100, lo que equivale a una calificación de grado C. El análisis constó de 9 checks pasivos ejecutados, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue identificado como fallo crítico. A pesar de contar con una base de cifrado correcta, la ausencia de protecciones avanzadas en el servidor web eleva el riesgo de explotación. Por lo tanto, se concluye que el sitio es actualmente vulnerable a ataques de suplantación e inyección debido a configuraciones de seguridad incompletas.

Resumen de Riesgos

0 CRITICO	4 ALTO	8 MEDIO	1 BAJO	32 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 44 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 44 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
44 dias restantes (expira: 2026-11-21T20:17:22.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-23T19:23:10.000Z
- 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://pcpd.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

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
- INFO

Tecnologias detectadas
React, Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO

Archivo /readme.html
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Archivo /README.txt
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Ruta /wp-login.php
Panel de login accesible publicamente
- 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 — 60/100

Estado: AVISO

Falta sitemap.xml

INFO

robots.txt

Presente (160 bytes)

INFO

Reglas robots.txt

0 Disallow, 5 Allow

INFO

security.txt

Presente en /.well-known/security.txt — Buena practica

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] Content-Security-Policy (CSP) faltante: La ausencia de esta política permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).

[HIGH] X-Frame-Options faltante: El sitio no previene el clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar a los usuarios.

[HIGH] Strict-Transport-Security (HSTS) no configurado: El servidor no obliga al navegador a usar conexiones HTTPS, lo que permite ataques de degradación de protocolo.

[MEDIUM] X-Content-Type-Options faltante: Facilita ataques de MIME-sniffing, permitiendo que el navegador interprete archivos de forma distinta a la declarada.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo puede indicar servicios de administración o proxies vulnerables a intrusiones.

[MEDIUM] Archivos informativos expuestos (/readme.html, /README.txt): Estos archivos son accesibles públicamente y pueden revelar detalles técnicos innecesarios sobre la plataforma.

[MEDIUM] Paneles de login expuestos (/wp-login.php, /user/login): Las rutas de acceso administrativo están abiertas, lo que facilita intentos de acceso por fuerza bruta.

[MEDIUM] Referrer-Policy faltante: No se controla la información de procedencia enviada a otros sitios, lo que puede comprometer la privacidad de la navegación.

[MEDIUM] Permissions-Policy faltante: El servidor no restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.

[LOW] Cabecera Server expuesta: Se detectó el valor cloudflare, lo que ayuda a los atacantes a identificar la tecnología de red y buscar vulnerabilidades específicas.

[LOW] Falta sitemap.xml: La ausencia de este archivo dificulta la auditoría de la estructura del sitio y afecta a la indexación correcta.