EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://pfactura.petco.com.mx	Checks	9 pruebas
Dominio	pfactura.petco.com.mx	Hallazgos	47 totales
Fecha	13 de abril de 2026 a las 21:49	Problemas	9 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

La evaluación de seguridad realizada al sitio web pfactura.petco.com.mx ha arrojado una puntuación de 70/100, lo que equivale a una nota de C. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 4 resultaron exitosos, 3 generaron advertencias y 2 se identificaron como fallos críticos. Aunque el sitio cuenta con un certificado SSL válido, existen deficiencias importantes en la configuración de protocolos de transporte seguro y exposición de información técnica. Por tanto, se concluye que el sitio es moderadamente vulnerable y requiere ajustes inmediatos en sus políticas de cabeceras y redirecciones.

Resumen de Riesgos

0	3	2	4	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 40 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	67	AVISO	__cf_bm: falta SameSite
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 40 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  40 dias restantes (expira: 2026-05-23T16:00:19.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-22T15:00:22.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Petco Mexico — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: frame-ancestors 'self' https://petco.com.mx https://www.petco.com.mx *.petco.com...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(self), camera=(), microphone=(), accelerometer=(), autoplay=(), ...

Redireccion HTTPS — 0/100

Estado: FALLO
No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 499 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 499

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**
  Petco Mexico

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)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 67/100

Estado: AVISO

__cf_bm: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __cf_bm — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 499)
- BAJO **sitemap.xml**
  No encontrado (HTTP 499)
- 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] Strict-Transport-Security: La cabecera HSTS no está configurada, lo que impide que el navegador fuerce conexiones HTTPS y permite ataques de degradación de protocolo.
[HIGH] Redirección HTTP a HTTPS: El servidor no redirige automáticamente el tráfico inseguro al puerto seguro, respondiendo con un error 499 en lugar de gestionar la transición.
[MEDIUM] Puerto 8080 (HTTP-Alt) Abierto: Se detectó un puerto alternativo abierto que podría exponer servicios internos, proxies o interfaces de administración no protegidas.
[MEDIUM] Cookie __cf_bm sin atributo SameSite: La falta de esta configuración en la cookie de Cloudflare aumenta el riesgo de ataques de falsificación de solicitud en sitios cruzados (CSRF).
[LOW] Cabecera Server expuesta: El servidor revela el uso de Cloudflare, lo que facilita a un atacante potencial identificar la infraestructura de protección y buscar vectores específicos.
[LOW] Cabecera X-Powered-By expuesta: Se divulga que el sitio utiliza tecnología específica de Petco México, lo que ayuda en la fase de reconocimiento de un ataque.
[LOW] Ausencia de archivos robots.txt y sitemap.xml: El servidor devuelve errores 499 para estos archivos, lo que dificulta la indexación controlada por parte de motores de búsqueda.