

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://federacionpescacv.com	Checks	9 pruebas
Dominio	federacionpescacv.com	Hallazgos	50 totales
Fecha	1 de octubre de 2026 a las 15:46	Problemas	15 detectados

C

64/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha arrojado una puntuación de 64/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 se identificaron como fallos críticos. Se han detectado deficiencias severas en la implementación de cabeceras de seguridad y una exposición innecesaria de servicios de infraestructura. Debido a la falta de protecciones contra ataques de inyección y la visibilidad de versiones de software obsoletas, el sitio se clasifica actualmente como vulnerable.

Resumen de Riesgos

0 CRITICO	6 ALTO	6 MEDIO	3 BAJO	35 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 39 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 6.9.4 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	1 cookies, todas con flags correctos
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	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 39 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
39 dias restantes (expira: 2026-11-09T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2025-10-26T00:00:00.000Z
- 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 — 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 302 redirige a https://federacionpescacv.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: WordPress 6.9.4
- INFO

Tecnologias detectadas
Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO

WordPress version
Version 6.9.4 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

1 cookies, todas con flags correctos

- **INFO** **Cookies detectadas**
1 cookie(s) encontrada(s)
- **INFO** **Cookie: PHPSESSID — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- **INFO** **Cookie: PHPSESSID — Secure**
Flag Secure activo — Solo se envia por HTTPS
- **INFO** **Cookie: PHPSESSID — SameSite**
SameSite=lax

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

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- **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
- **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] Puerto 21 (FTP): El puerto se encuentra abierto permitiendo transferencias de archivos de forma no cifrada, lo que facilita la interceptación de credenciales.
- [HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
- [HIGH] X-Frame-Options: Falta esta protección, lo que hace al sitio susceptible a ataques de Clickjacking para engañar a los usuarios.
- [HIGH] Strict-Transport-Security: No se ha configurado HSTS, permitiendo que las conexiones seguras sean degradadas a HTTP mediante ataques de interceptación.
- [HIGH] WordPress version: La versión 6.9.4 está expuesta públicamente, permitiendo a atacantes identificar y explotar vulnerabilidades conocidas para esta versión específica.
- [MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría llevar a la ejecución de scripts inesperados.
- [MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios, lo que puede filtrar datos de navegación.
- [MEDIUM] Permissions-Policy: La falta de restricciones en APIs del navegador permite que funciones como la cámara o el micrófono sean potencialmente accesibles.
- [MEDIUM] Archivo /readme.html: Este archivo es accesible y revela información técnica sensible sobre la instalación del CMS.
- [MEDIUM] Ruta /wp-login.php: El panel de administración es accesible para cualquier usuario, aumentando el riesgo de ataques de fuerza bruta.
- [MEDIUM] Puerto 22 (SSH): El acceso remoto seguro está abierto, lo que representa un vector de ataque si no posee restricciones de acceso estrictas.
- [LOW] Server header: Se expone la firma del servidor Apache, facilitando la fase de reconocimiento de un atacante.
- [LOW] Meta generator: La etiqueta meta expone explícitamente el uso de WordPress 6.9.4.
- [LOW] Ruta sensible en robots.txt: Se hace referencia directa a directorios de administración, guiando a posibles atacantes hacia zonas sensibles.