

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://prefieroacr.com	Checks	9 pruebas
Dominio	prefieroacr.com	Hallazgos	45 totales
Fecha	6 de octubre de 2026 a las 03:05	Problemas	13 detectados

C

74/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del dominio prefieroacr.com ha resultado en una puntuación de 74/100, lo que equivale a una calificación de grado C. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 presentó fallos críticos en la configuración. Aunque la infraestructura de red básica y el cifrado SSL presentan un estado sólido, la ausencia total de cabeceras de seguridad debilita significativamente la protección del entorno. Debido a la falta de medidas proactivas contra ataques de inyección y suplantación, se concluye que el sitio es actualmente vulnerable a diversas amenazas web comunes.

Resumen de Riesgos

0 CRITICO	4 ALTO	7 MEDIO	2 BAJO	32 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 81 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 robots.txt
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 81 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
81 dias restantes (expira: 2026-12-26T03:28:13.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-27T03:28:14.000Z
- 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: nginx/1.24.0 (Ubuntu) — Revela tecnologia del servidor

- BAJO

X-Powered-By expuesto
X-Powered-By: Next.js — Revela framework/lenguaje
- 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://prefieroacr.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

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, 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 robots.txt

- INFO

sitemap.xml
Presente, 3754 URLs
- INFO

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

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 esta cabecera que es vital para prevenir ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.

[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado en frames externos, facilitando ataques de clickjacking.

[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide forzar conexiones HTTPS y deja la sesión expuesta a ataques de degradación de protocolo.

[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría realizar sniffing de tipos MIME, permitiendo la ejecución de archivos con contenido inesperado.

[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada en las peticiones, lo que puede comprometer la privacidad de la navegación.

[MEDIUM] Permissions-Policy: Falta la restricción de acceso a APIs del navegador, permitiendo potencialmente el uso no autorizado de funciones como la cámara o el micrófono.

[MEDIUM] Archivos técnicos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, lo cual puede revelar detalles internos y versiones de la tecnología.

[MEDIUM] Rutas administrativas expuestas: Se detectó acceso público a los paneles de login /wp-login.php y /user/login, aumentando el riesgo de ataques de fuerza bruta.

[LOW] Cabecera Server expuesta: Se revela el uso de nginx/1.24.0 (Ubuntu), información que un atacante puede usar para buscar exploits específicos del servidor.

[LOW] Cabecera X-Powered-By expuesta: Se identifica el uso del framework Next.js, lo cual ayuda a perfilar la superficie de ataque tecnológica.

[LOW] Falta de robots.txt: La ausencia de este archivo genera una advertencia en la gestión de indexación y rastreo de directorios por motores de búsqueda.