EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://fichar.vigiprot.com	Checks	9 pruebas
Dominio	fichar.vigiprot.com	Hallazgos	47 totales
Fecha	18 de julio de 2026 a las 06:22	Problemas	11 detectados

D

58/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha arrojado una puntuación de 58/100, lo que conlleva una calificación de grado D. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 4 resultaron exitosos, 2 generaron advertencias y 3 fueron clasificados como fallos. Se han detectado debilidades críticas en la configuración de las cabeceras de seguridad y en la exposición de servicios de transferencia de archivos sin cifrar. El sitio carece de una redirección forzosa hacia conexiones seguras, permitiendo el acceso mediante protocolos vulnerables. Se concluye que el sitio es actualmente vulnerable y presenta una superficie de ataque que debe ser mitigada con urgencia.

Resumen de Riesgos

0	4	4	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
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	PHPSESSID: 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): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 84 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  84 dias restantes (expira: 2026-10-10T07:28:05.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-12T07:28:06.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, 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
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000; includeSubDomains; preload
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 302 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 dias)
- 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

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

PHPSESSID: falta SameSite

- 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
- MEDIO **Cookie: PHPSESSID — 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 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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] Puerto 21 (FTP) abierto: La presencia de este puerto abierto indica el uso de un protocolo de transferencia de archivos que no utiliza cifrado, permitiendo que un atacante intercepte credenciales y datos en tránsito.
[HIGH] Content-Security-Policy (CSP) ausente: Al no existir esta política, el sitio es altamente vulnerable a ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options ausente: La falta de esta cabecera permite que el sitio sea embebido en iframes de dominios maliciosos, facilitando ataques de clickjacking.
[HIGH] Redirección HTTP a HTTPS inexistente: El servidor no fuerza el uso de conexiones cifradas, lo que permite ataques de intermediario (Man-in-the-Middle) al navegar por la versión insegura del sitio.
[MEDIUM] Cookie PHPSESSID sin atributo SameSite: Esta configuración deja la sesión del usuario desprotegida ante ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] X-Content-Type-Options ausente: El navegador puede intentar adivinar el tipo de contenido (MIME-sniffing), lo que puede ser explotado para ejecutar scripts maliciosos disfrazados de otros archivos.
[MEDIUM] Referrer-Policy ausente: No se controla la información de referencia que el navegador envía a otros sitios, lo que puede derivar en la filtración de URLs internas.
[MEDIUM] Permissions-Policy ausente: El sitio no restringe el acceso a funciones sensibles del hardware o APIs del navegador, aumentando el riesgo de privacidad.
[LOW] Cabecera Server expuesta: Se revela que el servidor utiliza Apache, proporcionando información valiosa a los atacantes para buscar exploits específicos de dicha tecnología.
[LOW] Ausencia de archivos robots.txt y sitemap.xml: El servidor responde con errores 404 para estos archivos, lo que indica una falta de configuración básica en la gestión de rastreo.