EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://pro-media-file-manager.vrento.site:8443/home.php?id=35df501936f2584e9b335[illegible]feeh6alkvr65l7		
Dominio	pro-media-file-manager.vrento.site	Hallazgos	41 totales
Fecha	19 de mayo de 2026 a las 20:57	Problemas	14 detectados

F

38/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha arrojado una puntuación de 38/100, lo que corresponde a una calificación de grado F. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 3 verificaciones correctas, 1 advertencia y 4 fallos críticos de seguridad. Los hallazgos principales revelan una ausencia total de protecciones básicas contra ataques comunes y una gestión de identidad digital deficiente. En su estado actual, el sitio se clasifica como vulnerable, representando un riesgo significativo para la integridad de los datos y la privacidad de los usuarios.

Resumen de Riesgos

1	5	7	1	27
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
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): 22 (SSH)

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- INFO **Dias hasta expiracion**
  67 dias restantes (expira: 2026-07-25T09:44:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-26T09:44:53.000Z
- 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/1.18.0 (Ubuntu) — 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 — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://pro-media-file-manager.vrento.site/

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

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

Seguridad de Cookies — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)

- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- 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 **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — 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

[CRITICAL] Certificado SSL no válido: El certificado SSL no es válido o no está configurado correctamente, impidiendo una conexión cifrada confiable.
[HIGH] Ausencia de Content-Security-Policy: Falta la cabecera CSP, lo que permite la ejecución de ataques de inyección de contenido y scripts maliciosos (XSS).
[HIGH] Ausencia de X-Frame-Options: La falta de esta cabecera deja al sitio desprotegido contra ataques de clickjacking.
[HIGH] Ausencia de Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo posibles degradaciones de conexión a HTTP.
[HIGH] Cookie PHPSESSID sin flag HttpOnly: El identificador de sesión es accesible mediante JavaScript, facilitando el robo de sesiones en caso de XSS.
[HIGH] Cookie PHPSESSID sin flag Secure: La cookie de sesión se envía a través de conexiones no cifradas, exponiéndola a intercepción en la red.
[MEDIUM] Ausencia de X-Content-Type-Options: El sitio no previene el sniffing de tipos MIME, lo que puede ser explotado para ejecutar código malicioso.
[MEDIUM] Ausencia de Referrer-Policy: No existe control sobre la información de referencia enviada a terceros al navegar desde el sitio.

[MEDIUM] Ausencia de Permissions-Policy: No se restringen los permisos de acceso a APIs del navegador como cámara, micrófono o geolocalización.
[MEDIUM] Archivos técnicos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, revelando información potencial sobre la estructura del sitio.
[MEDIUM] Cookie PHPSESSID sin flag SameSite: La ausencia de este atributo hace que el sitio sea vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Puerto 22 (SSH) abierto: El puerto de acceso remoto está abierto, lo que aumenta la superficie de ataque si no cuenta con restricciones de acceso estrictas.
[LOW] Cabecera Server expuesta: El servidor revela el uso de nginx/1.18.0 (Ubuntu), proporcionando información valiosa a posibles atacantes sobre la infraestructura.