EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://andypsx.com	Checks	9 pruebas
Dominio	andypsx.com	Hallazgos	42 totales
Fecha	18 de abril de 2026 a las 13:51	Problemas	7 detectados

B

79/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio andypsx.com ha resultado en una puntuación exacta de 79/100 con una calificación final de nota B. Se ejecutaron un total de 9 checks pasivos, obteniendo 5 resultados satisfactorios, 3 advertencias y 1 fallo crítico en la configuración de archivos de rastreo. Aunque el sitio cuenta con un cifrado SSL robusto, la ausencia de cabeceras de seguridad esenciales y la exposición de puertos alternativos incrementan la superficie de ataque. En su estado actual, el sitio se considera vulnerable a ataques de inyección de contenido y de interceptación de tráfico por falta de políticas estrictas. Se requiere una intervención técnica para mitigar estos riesgos y mejorar la postura de seguridad global.

Resumen de Riesgos

0	3	1	3	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 64 dias
Cabeceras de Seguridad	55	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
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	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 64 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  64 dias restantes (expira: 2026-06-21T15:52:36.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-23T14:52:49.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- 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: same-origin
- INFO **Permissions-Policy**
  Presente: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://andypsx.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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 — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- 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

[ALTA] Content-Security-Policy: La ausencia de esta cabecera impide restringir qué recursos pueden cargarse, facilitando ataques de Cross-Site Scripting (XSS) e inyección de datos.
[ALTA] Strict-Transport-Security: La falta de la directiva HSTS permite ataques de degradación de protocolo, donde un atacante puede forzar la conexión a través de HTTP no cifrado.
[MEDIA] Puerto 8080 (HTTP-Alt) abierto: La presencia de este puerto activo sugiere la existencia de un servidor web alternativo o un proxy que podría exponer servicios internos no protegidos.
[BAJA] Server header expuesto: El encabezado revela el uso de tecnología Cloudflare, lo que proporciona información valiosa a un atacante para buscar exploits específicos contra dicha infraestructura.
[BAJA] Ausencia de robots.txt y sitemap.xml: El servidor devuelve un código de error 403 al intentar acceder a estos archivos, lo que impide una auditoría de indexación correcta y refleja una configuración de permisos deficiente.