EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://respaldosvms.pentasec.net	Checks	9 pruebas
Dominio	respaldosvms.pentasec.net	Hallazgos	42 totales
Fecha	17 de marzo de 2026 a las 21:48	Problemas	8 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El activo evaluado presenta una puntuacion exacta de 76/100 y una nota final de B. Durante la auditoria se ejecutaron 9 checks pasivos, de los cuales 5 resultaron correctos, 2 generaron advertencias y 2 se marcaron como fallos de seguridad. Se realizo un pentest activo con IA utilizando herramientas como Nmap, WhatWeb y curl para el reconocimiento de la infraestructura. El analisis descubrio que, aunque el subdominio esta correctamente apuntado, el servidor de origen es inalcanzable debido a un error de tunel (Cloudflare 530), lo que impide el acceso a endpoints de API y otras funcionalidades. Se concluye que el sitio es actualmente vulnerable debido a fallos criticos en las cabeceras de transporte y una configuracion de red incompleta.

Resumen de Riesgos

0	3	2	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 63 dias
Cabeceras de Seguridad	40	FALLO	Solo 3/6 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	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 63 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  63 dias restantes (expira: 2026-05-19T15:56:43.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-18T14:57:10.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Permissions-Policy

- 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
- 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://respaldosvms.pentasec.net/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 530

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 530)
- BAJO **sitemap.xml**
  No encontrado (HTTP 530)
- 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

[HIGH] CWE-404: El servidor de origen es inalcanzable a traves del tunel de Cloudflare, provocando una denegacion de servicio tecnica.
[HIGH] CWE-319: Ausencia de la cabecera HSTS, lo que permite que el sitio sea vulnerable a ataques de degradacion de SSL/TLS.
[HIGH] CWE-1021: Falta de la cabecera Content-Security-Policy (CSP), lo que facilita la ejecucion de ataques XSS e inyeccion de contenido.
[MEDIUM] Permissions-Policy: La ausencia de esta cabecera permite que el navegador acceda a APIs sensibles sin restricciones explicitas.
[MEDIUM] Puerto 8080 (HTTP-Alt) Abierto: La exposicion de un puerto alternativo de servidor web aumenta la superficie de ataque innecesariamente.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando informacion tecnica util para un atacante en fase de reconocimiento.
[LOW] Faltan archivos de indexacion: La ausencia de robots.txt y sitemap.xml dificulta la gestion de rastreo y sugiere una configuracion incompleta del servidor.