EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://nexusprosystem.online/	Checks	9 pruebas
Dominio	nexusprosystem.online	Hallazgos	45 totales
Fecha	3 de mayo de 2026 a las 17:50	Problemas	10 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada a nexusprosystem.online arroja una puntuacion de 80/100 con una calificacion final de nota B. Se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos criticos relacionados con la configuracion de cabeceras y archivos del sistema. Aunque la infraestructura base de red y el cifrado son solidos, la ausencia de politicas de seguridad en el servidor web expone el sitio a ataques conocidos. Por tanto, el sitio se considera vulnerable en su capa de aplicacion debido a la falta de protecciones contra inyeccion y suplantacion.

Resumen de Riesgos

0	2	8	0	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 85 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 85 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  85 dias restantes (expira: 2026-07-27T12:03:55.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-28T11:04:34.000Z
- 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

- 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=31556926
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://nexusprosystem.online/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31556926
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31556926 (365 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
- INFO **Tecnologias detectadas**
  React

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 /administrator/**
  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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- 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: La ausencia de esta cabecera permite la ejecucion de scripts no autorizados, aumentando el riesgo de ataques XSS y robo de datos.

[HIGH] X-Frame-Options: Al no estar implementada, el sitio es susceptible a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible para engañar al usuario.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, lo que facilita ataques de sniffing de MIME-type.
[MEDIUM] Referrer-Policy: No se controla que informacion de referencia se envia a otros sitios, lo que podria exponer URLs privadas o datos de navegacion.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la camara o el microfono, aumentando la superficie de ataque.
[MEDIUM] Archivos README expuestos: Los archivos /readme.html y /README.txt son accesibles publicamente, lo que facilita la obtencion de informacion sobre la arquitectura interna.
[MEDIUM] Paneles de login accesibles: Las rutas /wp-login.php, /administrator/ y /user/login estan expuestas, lo que permite intentos de acceso por fuerza bruta.
[MEDIUM] Ausencia de Robots.txt y Sitemap: La falta de estos archivos dificulta la gestion del rastreo por motores de busqueda y la visibilidad de la estructura del sitio.