EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ntfor.com/	Checks	9 pruebas
Dominio	ntfor.com	Hallazgos	56 totales
Fecha	26 de mayo de 2026 a las 01:43	Problemas	18 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio ntfor.com ha dado como resultado una puntuación de 64/100, lo que otorga una nota de C. Durante la evaluación se ejecutaron 9 comprobaciones pasivas que resultaron en 4 validaciones correctas, 2 advertencias y 3 fallos críticos en la infraestructura. Se han detectado deficiencias graves en la exposición de servicios de red y en la gestión de la privacidad de las sesiones. Debido a la apertura de puertos críticos y la falta de cabeceras de seguridad esenciales, se concluye que el sitio es vulnerable ante ataques dirigidos.

Resumen de Riesgos

1	6	8	3	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 59 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.0 expuesta, WordPress 2 expuesta
Seguridad de Cookies	17	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 59 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  59 dias restantes (expira: 2026-07-24T05:30:44.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-25T05:30:45.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

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

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: "max-age=31536000" env=HTTPS
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- 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 302 redirige a https://ntfor.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: "max-age=31536000" env=HTTPS
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 7.0
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0 expuesta publicamente — Permite a atacantes buscar CVEs conocidos

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

Seguridad de Cookies — 17/100

Estado: FALLO

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

- INFO **Cookies detectadas**
  2 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
- ALTO **Cookie: ntfor_ut — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: ntfor_ut — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ntfor_ut — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://bampimor.net/boot/fichero/Subvenciones_Cantabria.pdf

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (191 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://ntfor.com/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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] Puerto 3306 (MySQL): El servicio de base de datos se encuentra abierto a internet, permitiendo ataques de fuerza bruta y potencial exfiltración de información sensible.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos sin cifrado detectado, lo que facilita la interceptación de credenciales en la red.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de ataques Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] WordPress versión 7.0 expuesta: La visibilidad pública de la versión del CMS permite a atacantes identificar y explotar vulnerabilidades conocidas (CVEs) de forma precisa.
[HIGH] Cookie PHPSESSID (HttpOnly/Secure): La falta de estas banderas permite que la cookie de sesión sea robada mediante scripts o interceptada en conexiones que no fuercen el cifrado.
[HIGH] Cookie ntfor_ut (HttpOnly): La carencia del atributo HttpOnly expone esta cookie a ser accedida maliciosamente a través del navegador.
[MEDIUM] Puerto 22 (SSH): El acceso remoto seguro está abierto, lo que representa un vector de ataque si no existen políticas de bloqueo de IP o autenticación multifactor.
[MEDIUM] Permissions-Policy: Falta esta cabecera para restringir el acceso de la web a funciones sensibles del hardware del usuario como cámara o micrófonos.
[MEDIUM] Cookie PHPSESSID (SameSite): La ausencia de este atributo hace que la sesión sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se detectaron recursos cargados mediante HTTP (gmpg.org y bampimor.net) dentro de la página cifrada, comprometiendo la integridad del sitio.
[MEDIUM] Archivo /readme.html y /wp-login.php: Rutas accesibles que revelan información técnica del CMS y exponen el panel de administración a intentos de acceso no autorizados.
[LOW] Cabecera Server expuesta: El servidor revela el software HTTPd, proporcionando información técnica útil para la fase de reconocimiento de un ataque.
[LOW] Meta generator: La etiqueta expone directamente el uso de WordPress 7.0 en el código fuente.
[LOW] Ruta sensible en robots.txt: Se referencia el directorio admin, lo que facilita a rastreadores maliciosos la identificación de áreas restringidas.