EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://nexutsc.infinityfreeapp.com/	Checks	9 pruebas
Dominio	nexutsc.infinityfreeapp.com	Hallazgos	46 totales
Fecha	29 de abril de 2026 a las 00:40	Problemas	14 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web nexutsc.infinityfreeapp.com ha arrojado una puntuación de 65/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 comprobaciones pasivas, de las cuales 7 resultaron satisfactorias y 2 presentaron fallos críticos relacionados con la configuración del servidor y el cifrado. No se detectó un CMS específico, pero la exposición de rutas administrativas y la falta total de cabeceras de seguridad representan un riesgo significativo. En su estado actual, el sitio se considera vulnerable debido a que no fuerza conexiones seguras ni implementa protecciones contra ataques web comunes.

Resumen de Riesgos

0	5	8	1	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 58 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 58 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  58 dias restantes (expira: 2026-06-25T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-27T00:00:00.000Z
- 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: openresty — 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: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (156 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 2 Allow
- INFO **Sitemap en robots.txt**
  https://nexutsc.infinityfreeapp.com/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] Redirección HTTP a HTTPS: El sitio no redirige automáticamente el tráfico no cifrado, permitiendo conexiones inseguras por el puerto 80.
[HIGH] Strict-Transport-Security (HSTS): Falta la configuración que obliga al navegador a usar exclusivamente conexiones HTTPS, facilitando ataques de degradación de seguridad.
[HIGH] Content-Security-Policy (CSP): La ausencia de esta cabecera permite la ejecución de scripts no autorizados y ataques de inyección de contenido o XSS.
[HIGH] X-Frame-Options: No existe protección contra el secuestro de clics (clickjacking), lo que permite que el sitio sea cargado dentro de marcos externos maliciosos.
[MEDIUM] Rutas de administración expuestas: Se detectó que paneles de acceso como /wp-login.php, /administrator/ y /user/login están accesibles al público.
[MEDIUM] Archivos de información técnica: Los archivos /readme.html y /README.txt son consultables, lo que podría revelar versiones de software o detalles internos del sitio.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que los navegadores realicen sniffing de tipos MIME, aumentando el riesgo de ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se ha definido una política para controlar cuánta información de referencia se envía a otros sitios web.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando activos permisos para cámara, micrófono o geolocalización de forma innecesaria.
[LOW] Server header expuesto: La cabecera Server revela el uso de openresty, proporcionando información útil a atacantes para buscar exploits específicos.