EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cn-777.com/	Checks	9 pruebas
Dominio	cn-777.com	Hallazgos	43 totales
Fecha	18 de abril de 2026 a las 18:45	Problemas	10 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad del dominio cn-777.com ha resultado en una puntuacion de 64/100, lo que equivale a una calificacion de grado C. Durante la evaluacion se ejecutaron 9 checks pasivos, de los cuales 5 fueron satisfactorios, 2 generaron advertencias y 2 resultaron en fallos criticos. El sitio web muestra una gestion adecuada del cifrado SSL, pero presenta deficiencias severas en la configuracion de cabeceras de seguridad y exposicion de informacion del sistema. Debido a la falta de protecciones basicas contra ataques de inyeccion y suplantacion, se concluye que el sitio es actualmente vulnerable. No se realizo un pentest activo, por lo que existen riesgos adicionales no explorados.

Resumen de Riesgos

0	5	4	1	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 85 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	20	FALLO	WordPress 6.4.3 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

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: 2026-07-12T15:35:15.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-13T14:37:49.000Z
- 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: cloudflare — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://cn-777.com/
- 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 — 20/100

Estado: FALLO

WordPress 6.4.3 expuesta

- ALTO **WordPress version**
  Version 6.4.3 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

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 (64 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://cn-777.com/sitemap.xml
- 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] WordPress version: Version 6.4.3 expuesta publicamente, lo cual permite a posibles atacantes identificar y explotar vulnerabilidades especificas de esta version.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: Falta de proteccion que permite ataques de clickjacking, donde un atacante puede inducir al usuario a realizar acciones no deseadas.
[HIGH] Strict-Transport-Security: El mecanismo HSTS no esta configurado, permitiendo que las conexiones puedan ser degradadas de HTTPS a HTTP.

[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto, lo que indica la presencia de un servidor web alternativo o proxy que amplia la superficie de ataque.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite a los navegadores realizar MIME-sniffing, aumentando el riesgo de ejecucion de scripts maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la informacion de procedencia enviada a otros sitios, comprometiendo la privacidad de la navegacion.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la camara, el microfono o la geolocalizacion.
[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, proporcionando informacion tecnica que facilita las fases de reconocimiento de un ataque.