EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.nuatechnology.com/	Checks	9 pruebas
Dominio	www.nuatechnology.com	Hallazgos	53 totales
Fecha	28 de abril de 2026 a las 01:37	Problemas	7 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado arroja una puntuación de 85/100, otorgando una calificación de nota B. Se ejecutaron 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias, 2 generaron advertencias y 1 fue calificada como fallo. La infraestructura presenta una base sólida en cuanto a cifrado y redirecciones seguras, aunque muestra carencias significativas en la configuración de cabeceras de respuesta del servidor. El escaneo revela vulnerabilidades moderadas relacionadas con la exposición de puertos y la gestión de cookies de sesión. En conclusión, el sitio se considera mayoritariamente seguro, pero es vulnerable a ataques específicos de manipulación de interfaz y suplantación de peticiones.

Resumen de Riesgos

0	1	4	2	46
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 88 dias
Cabeceras de Seguridad	55	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, X-C...
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	83	AVISO	__cf_bm: falta SameSite
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 88 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  88 dias restantes (expira: 2026-07-25T01:56:11.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-26T00:56:19.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: FALLO

Solo 3/6 presentes. Faltan: X-Frame-Options, X-Content-Type-Options, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- 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 301 redirige a https://www.nuatechnology.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- 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

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
- BAJO **Meta generator**
  Expone: HubSpot
- INFO **Tecnologias detectadas**
  Next.js

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 — 83/100

Estado: AVISO

__cf_bm: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __cf_bm — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: _cfuvid — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _cfuvid — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _cfuvid — SameSite**
  SameSite=none

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 (165 bytes)
- INFO **Reglas robots.txt**
  5 Disallow, 0 Allow
- INFO **sitemap.xml**
  Presente, 21 URLs
- 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] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[MEDIUM] X-Content-Type-Options: Al no estar presente, los navegadores podrían intentar interpretar el contenido de forma incorrecta, aumentando el riesgo de ataques basados en MIME-type sniffing.
[MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el uso de APIs del navegador como la cámara o el micrófono por parte de terceros.
[MEDIUM] Cookie __cf_bm (SameSite): Esta cookie carece del atributo SameSite, lo que la hace susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto y expuesto, lo que podría indicar la presencia de un servidor web alternativo o proxy no securizado.
[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, proporcionando información técnica que podría ser utilizada por atacantes para perfilar la infraestructura.
[LOW] Meta generator: Se detectó la etiqueta de metadatos de HubSpot, lo que expone el uso de esta plataforma específica para la gestión de contenidos.