# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://nextgt.es | Checks | 9 pruebas |
| Dominio | nextgt.es | Hallazgos | 48 totales |
| Fecha | 28 de septiembre de 2026 a las 18:04 | Problemas | 14 detectados |

C

72/100

puntos de seguridad

**RESUMEN EJECUTIVO**

La auditoría de seguridad realizada al sitio web arroja una puntuación de 72/100, obteniendo una calificación de grado C. El análisis se basó en 9 checks pasivos, resultando en 5 verificaciones correctas, 2 advertencias por configuraciones incompletas y 2 fallos de seguridad críticos. Aunque el cifrado de datos es adecuado, se han detectado debilidades significativas en las cabeceras de seguridad y la exposición de servicios internos del servidor. En conclusión, el sitio se considera vulnerable debido a la visibilidad de puertos críticos y la falta de mecanismos de protección contra ataques web comunes.

## Resumen de Riesgos

| 1 | 5 | 4 | 4 | 34 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 66 dias |
| Cabeceras de Seguridad | 40 | FALLO | Solo 2/6 presentes. Faltan: X-Frame-Options, Str... |
| Redireccion HTTPS | 70 | AVISO | HTTP redirige a HTTPS pero falta HSTS |
| Deteccion CMS | 100 | OK | CMS detectado: WordPress, PrestaShop |
| Version CMS Expuesta | 20 | FALLO | WordPress 6.8.10 expuesta, WordPress 2 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 | 2 puerto(s) potencialmente riesgoso(s): 21 (FTP)... |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 66 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  66 dias restantes (expira: 2026-12-03T14:12:08.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-04T14:12:09.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 2/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.33 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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
- INFO **Permissions-Policy**
  Presente: private-state-token-redemption=(self "https://www.google.com" "https://www.gstat...

## Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://nextgt.es/
- 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

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: All in One SEO (AIOSEO) 5.0.1.1
- INFO **Tecnologias detectadas**
  Next.js, Astro, PHP/8.2.33

## Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.8.10 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.8.10 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 — 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 (151 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://nextgt.es/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- 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): ABIERTO. La base de datos está expuesta a internet, lo que permite intentos de intrusión directa.
[HIGH] Puerto 21 (FTP): ABIERTO. El servicio de transferencia de archivos no utiliza cifrado, exponiendo credenciales y datos.
[HIGH] WordPress version: Versión 6.8.10 expuesta públicamente. Permite a los atacantes identificar vulnerabilidades específicas para esta versión.
[HIGH] X-Frame-Options: Falta. El sitio es vulnerable a ataques de clickjacking que pueden engañar al usuario.
[HIGH] Strict-Transport-Security: Falta. No se obliga al navegador a usar conexiones HTTPS mediante HSTS, permitiendo ataques de degradación.
[HIGH] HSTS (Strict-Transport-Security): No configurado. El navegador no fuerza la navegación segura de forma automática.
[MEDIUM] X-Content-Type-Options: Falta. Permite que el navegador interprete archivos de forma incorrecta, facilitando ataques de ejecución de scripts.
[MEDIUM] Referrer-Policy: Falta. No se controla la información de navegación enviada a otros sitios al hacer clic en enlaces.
[MEDIUM] Archivo /readme.html: Accesible públicamente. Facilita información técnica sobre la instalación del CMS a posibles atacantes.
[MEDIUM] Ruta /wp-login.php: Panel de login accesible. Facilita ataques de fuerza bruta contra las credenciales de administración.
[LOW] Server header expuesto: Server: LiteSpeed. Revela información sobre la tecnología del servidor web.
[LOW] X-Powered-By expuesto: PHP/8.2.33. Expone la versión exacta del lenguaje de programación utilizado.
[LOW] Meta generator: Expone AIOSEO 5.0.1.1. Revela versiones de plugins que podrían tener fallos conocidos.
[LOW] Ruta sensible en robots.txt: Referencia a "admin". Indica a los rastreadores y atacantes la ubicación de directorios sensibles.