EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://nintenhype.cat	Checks	9 pruebas
Dominio	nintenhype.cat	Hallazgos	46 totales
Fecha	11 de agosto de 2026 a las 09:22	Problemas	14 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre nintenhype.cat arroja una puntuación de 53/100, lo que equivale a una nota D. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 5 resultaron correctos, 1 generó una advertencia y 3 fallaron con severidad alta. Los resultados demuestran una carencia crítica de cabeceras de seguridad y una configuración de cifrado incompleta. Debido a la exposición pública de versiones de software y la falta de redirección segura, se concluye que el sitio es vulnerable ante ataques de interceptación y explotación dirigida.

Resumen de Riesgos

0	6	6	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 67 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	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.8.7 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
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	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 67 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  67 dias restantes (expira: 2026-10-17T02:32:33.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-19T02:32:34.000Z
- 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: Apache — 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 301 — 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

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
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.8.7 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.8.7 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)

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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.elegantthemes.com
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.wordpress.org

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (168 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://www.nintenhype.cat/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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] Content-Security-Policy: Falta — Previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.

[HIGH] X-Frame-Options: Falta — Protege a los usuarios contra ataques de clickjacking que pueden suplantar la interfaz.
[HIGH] Strict-Transport-Security: Falta — No se fuerza el uso de HSTS, permitiendo que las conexiones se degraden a protocolos no seguros.
[HIGH] Redirección HTTP a HTTPS: No configurada — El servidor no redirige automáticamente el tráfico inseguro al puerto seguro.
[HIGH] WordPress versión expuesta: La versión 6.8.7 es visible — Facilita a los atacantes la búsqueda de vulnerabilidades específicas conocidas (CVE).
[MEDIUM] X-Content-Type-Options: Falta — Permite que el navegador intente adivinar el tipo de contenido, facilitando ataques de MIME-sniffing.
[MEDIUM] Referrer-Policy: Falta — No se controla la información de referencia que se envía al navegar hacia enlaces externos.
[MEDIUM] Permissions-Policy: Falta — No se restringen las capacidades del navegador como el acceso a la cámara o geolocalización.
[MEDIUM] Archivo /readme.html accesible: Expuesto públicamente — Revela información técnica detallada sobre la instalación del CMS.
[MEDIUM] Contenido Mixto: Se detectaron recursos HTTP (elegantthemes y wordpress.org) en una página HTTPS — Debilita la integridad de la conexión cifrada.
[LOW] Server header expuesto: Server: Apache — Revela la tecnología y software del servidor, acortando la fase de reconocimiento de un atacante.
[LOW] Ruta sensible en robots.txt: Referencia a "admin" — Expone directorios de gestión administrativa a rastreadores y atacantes.