

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://Infonautas.es
Dominio infonautas.es
Fecha 7 de abril de 2026 a las 19:50

Checks 9 pruebas
Hallazgos 48 totales
Problemas 12 detectados

C

71/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio arroja una puntuación de 71/100, lo que equivale a una nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 4 generaron advertencias y 1 fue calificado como fallo crítico. Aunque el cifrado de datos es correcto, se han detectado deficiencias importantes en las cabeceras de seguridad y una exposición de versiones de software desactualizadas. En su estado actual, el sitio se considera vulnerable debido a la falta de políticas de protección contra inyecciones y la visibilidad de información técnica sensible.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 dias
Cabeceras de Seguridad	55	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
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 6.9.4 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	3 recurso(s) HTTP en pagina HTTPS
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 90 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
90 dias restantes (expira: 2026-07-06T15:16:29.000Z)
- INFO Fecha de emision
Emitido desde: 2026-04-07T15:16:30.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security

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

- ALTO

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO

X-Content-Type-Options
Presente: nosniiff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- 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://infonautas.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: WordPress 6.9.4
- INFO

Tecnologias detectadas
Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO

WordPress version
Version 6.9.4 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

3 recurso(s) HTTP en pagina HTTPS

- MEDIO

Recurso HTTP (src (script/img/iframe))
http://192.168.50.80/wp-content/uploads/2026/04/177386234477...
- MEDIO

Recurso HTTP (src (script/img/iframe))
http://192.168.50.80/wp-content/uploads/2026/04/177488814675...
- MEDIO

Recurso HTTP (href (link/stylesheet))
http://192.168.50.80

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt
Presente (1997 bytes)
- INFO

Reglas robots.txt
10 Disallow, 1 Allow
- MEDIO

Bloqueo total
robots.txt bloquea todo el sitio con Disallow: /
- INFO

Sitemap en robots.txt
https://infonautas.es/sitemap_index.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



Analisis de Seguridad

VULNERABILIDADES DETECTADAS

- [HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques XSS y la inyección de contenido malicioso.
- [HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, permitiendo posibles degradaciones de protocolo.
- [HIGH] WordPress version: La exposición pública de la versión 6.9.4 permite a atacantes identificar y explotar vulnerabilidades conocidas (CVEs).
- [MEDIUM] Contenido Mixto: Se detectaron 3 recursos cargados mediante HTTP desde una IP privada, lo que compromete la integridad de la conexión cifrada.
- [MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede revelar detalles internos de la instalación del CMS.
- [MEDIUM] Puerto 8080 (HTTP-Alt): La apertura de este puerto aumenta la superficie de ataque al exponer un servidor web alternativo o proxy.
- [MEDIUM] Bloqueo total robots.txt: El archivo bloquea la indexación completa del sitio, lo cual es una configuración inusual que podría ocultar estructuras de directorios.
- [LOW] Server header expuesto: Se revela el uso de Cloudflare como tecnología de servidor, facilitando la fase de reconocimiento de un ataque.
- [LOW] Meta generator: La etiqueta meta en el código fuente expone explícitamente la versión de WordPress utilizada.