EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://europia.neopi.es	Checks	9 pruebas
Dominio	europia.neopi.es	Hallazgos	43 totales
Fecha	22 de abril de 2026 a las 06:32	Problemas	13 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web determinó una puntuación de 72/100, lo que equivale a una nota de grado C. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 finalizaron con fallos críticos. Aunque la implementación del cifrado SSL es excelente, se detectó una carencia total de cabeceras de seguridad y la exposición de rutas administrativas sensibles. Concluimos que el sitio es actualmente vulnerable a ataques de clickjacking e inyección de contenido debido a configuraciones de servidor incompletas. Se recomienda aplicar las medidas correctivas detalladas para elevar el nivel de protección de la infraestructura.

Resumen de Riesgos

0	4	8	1	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 66 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	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

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: 2026-06-26T20:48:09.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-28T20:48:10.000Z
- 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: nginx/1.24.0 (Ubuntu) — 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://europia.neopi.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

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 — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- INFO **Version CMS**
  No se detecta ninguna version expuesta

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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

[LOW] Server header expuesto: El servidor devuelve la cabecera nginx/1.24.0 (Ubuntu), lo cual revela la tecnología exacta y facilita la búsqueda de exploits específicos.
[HIGH] Content-Security-Policy: Esta cabecera no está configurada, permitiendo que el sitio sea vulnerable a ataques de Cross-Site Scripting (XSS) y otros métodos de inyección.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado en iframes ajenos, facilitando ataques de secuestro de clics o clickjacking.
[HIGH] Strict-Transport-Security: No se detectó la cabecera HSTS, lo que impide que el sitio fuerce de manera persistente las conexiones seguras a través de HTTPS.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador realice sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No existe una política definida para el control de la información de referencia enviada a otros dominios durante la navegación.
[MEDIUM] Permissions-Policy: El sitio no restringe el uso de APIs del navegador, dejando expuestas funciones como la cámara o el micrófono ante posibles abusos.
[HIGH] HSTS en redirección: Aunque el tráfico HTTP redirige a HTTPS, la falta de HSTS en la respuesta deja una ventana de vulnerabilidad ante ataques de degradación de protocolo.
[MEDIUM] Archivo /readme.html: El archivo es accesible públicamente y puede contener información técnica o versiones internas de la plataforma.
[MEDIUM] Archivo /README.txt: Este archivo de texto expone datos del desarrollo o configuración que no deberían estar disponibles para usuarios externos.
[MEDIUM] Rutas de administración expuestas: Se detectaron paneles de acceso activos en /wp-login.php, /administrator/ y /user/login, aumentando el riesgo de ataques de fuerza bruta.
[LOW] Ausencia de robots.txt y sitemap.xml: El sitio carece de archivos de indexación estándar, lo que impacta negativamente en la gestión del rastreo por parte de motores de búsqueda.