

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://guppy.es
Dominio guppy.es
Fecha 17 de abril de 2026 a las 09:35

Checks 9 pruebas
Hallazgos 47 totales
Problemas 15 detectados

C

64/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada a guppy.es ha resultado en una puntuación de 64/100 con una calificación de C. El análisis constó de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 presentaron fallos críticos. Aunque el sitio web cuenta con un certificado SSL válido, la ausencia total de cabeceras de seguridad y la exposición de versiones de software desactualizadas comprometen la integridad de la plataforma. No se ejecutó un pentest activo en este ciclo de evaluación. Debido a los hallazgos en la infraestructura y la configuración del CMS, el sitio se considera actualmente vulnerable ante ataques de inyección y explotación de CVE conocidos.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 68 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	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	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 68 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
68 dias restantes (expira: 2026-06-24T08:04:26.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-26T08:04:27.000Z
- 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/2.4.29 — 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 302 redirige a https://guppy.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)

- 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 (115 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.guppy.es/wp-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), 22 (SSH)

- ALTO** Puerto 21 (FTP)
ABIERTO — Transferencia de archivos sin cifrar
- MEDIO** Puerto 22 (SSH)
ABIERTO — 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
- 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: La ausencia de esta cabecera permite la ejecución de ataques XSS y la inyección de contenido malicioso de terceros.

[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking mediante el uso de frames.

[HIGH] Strict-Transport-Security: La falta de HSTS permite que un atacante intente degradar la conexión de los usuarios a HTTP no cifrado.

[HIGH] WordPress version: La exposición pública de la versión 6.9.4 facilita a los atacantes el uso de exploits para vulnerabilidades ya documentadas.

[HIGH] Puerto 21 (FTP): Este puerto está abierto y transmite datos sin cifrar, lo que pone en riesgo las credenciales de administración.

[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que el navegador intente adivinar el tipo de contenido, facilitando ataques de MIME-sniffing.

[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a otros dominios, lo que podría filtrar rutas internas.

[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la ubicación.

[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y confirma detalles técnicos sobre la instalación del CMS.

[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario, permitiendo intentos de fuerza bruta.

[MEDIUM] Puerto 22 (SSH): Se detectó un puerto de acceso remoto abierto que constituye un vector de ataque si no está debidamente protegido.

[LOW] Server header expuesto: El servidor revela el uso de Apache/2.4.29, facilitando el perfilado tecnológico por parte de atacantes.

[LOW] Meta generator: La etiqueta en el código fuente expone directamente que se utiliza WordPress 6.9.4.

[LOW] Ruta sensible en robots.txt: Se referencia el directorio "admin", lo que ayuda a un atacante a mapear la estructura interna del sitio.