

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://wallapop.es
Dominio wallapop.es
Fecha 10 de mayo de 2026 a las 20:28

Checks 9 pruebas
Hallazgos 44 totales
Problemas 4 detectados

A

93/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada al dominio wallapop.es arroja una puntuación de 93/100, lo que equivale a una calificación de grado A. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 7 resultados satisfactorios, 1 advertencia técnica y 1 fallo crítico en la configuración de archivos de rastreo. La infraestructura presenta una implementación robusta de protocolos de cifrado y redirecciones seguras, aunque carece de ciertas cabeceras de control de hardware en el navegador. En conclusión, el sitio se considera seguro para la navegación del usuario, aunque requiere ajustes menores en políticas de seguridad y disponibilidad de archivos de configuración.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 181 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 181 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
181 dias restantes (expira: 2026-11-07T23:59:59.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-24T00:00:00.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

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

- INFO **Content-Security-Policy**
Presente: form-action 'self' wallapop.com *.wallapop.com; frame-ancestors 'self' wallapop....
- INFO **X-Frame-Options**
Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
Presente: nosniiff
- INFO **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- MEDIO **Permissions-Policy**
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://wallapop.es/
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
HSTS cubre subdominios
- INFO **HSTS max-age**
max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
HTTPS responde con status 403

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

- INFO **Archivo /readme.html**
No accesible (correcto)
- INFO **Archivo /README.txt**
No accesible (correcto)
- 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

- BAJO **robots.txt**
No encontrado (HTTP 403)
- BAJO **sitemap.xml**
No encontrado (HTTP 403)
- BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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

[MEDIUM] Permissions-Policy: Ausencia de esta cabecera, lo que impide restringir el uso de APIs del navegador como la cámara, micrófono o geolocalización por parte de terceros.

[LOW] Server header expuesto: El encabezado Server revela el uso de CloudFront, facilitando a un atacante potencial información sobre la tecnología de distribución de contenido.

[LOW] robots.txt no encontrado: El servidor devuelve un código de estado 403 (prohibido) al intentar acceder a las directivas de rastreo para buscadores.

[LOW] sitemap.xml no encontrado: Falta el índice de contenido del sitio o su acceso está bloqueado, lo que afecta la visibilidad y auditoría de secciones del portal.