EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://jubilados-en-el-caribe.com.es/	Checks	9 pruebas
Dominio	jubilados-en-el-caribe.com.es	Hallazgos	41 totales
Fecha	24 de septiembre de 2026 a las 22:04	Problemas	12 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio jubilados-en-el-caribe.com.es ha arrojado una puntuación de 60/100, lo que resulta en una calificación de nota C. Se ejecutaron 9 checks pasivos, obteniendo 4 resultados satisfactorios, 2 advertencias por configuraciones incompletas y 3 fallos críticos en la infraestructura. A pesar de contar con un cifrado SSL válido, la ausencia total de cabeceras de protección y la exposición de servicios obsoletos elevan el perfil de riesgo. En su estado actual, el sitio se considera vulnerable debido a deficiencias técnicas estructurales que comprometen la integridad de la plataforma.

Resumen de Riesgos

0	5	4	3	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 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	20	FALLO	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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 89 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  89 dias restantes (expira: 2026-12-22T11:35:39.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-23T11:35:40.000Z
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://jubilados-en-el-caribe.com.es/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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 — 20/100

Estado: FALLO

WordPress 2 expuesta

- 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 — 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 — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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

[HIGH] Puerto 21 (FTP) abierto: permite el intercambio de archivos mediante un protocolo no cifrado, facilitando la captura de credenciales por terceros.
[HIGH] Falta de Content-Security-Policy: la ausencia de esta directiva permite la ejecución de ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] Falta de X-Frame-Options: el sitio es susceptible a ataques de clickjacking, permitiendo que atacantes carguen la web en marcos invisibles.
[HIGH] Falta de Strict-Transport-Security: no se fuerza el uso de HTTPS mediante HSTS, dejando la conexión expuesta a ataques de degradación de protocolo.
[MEDIUM] Versión de WordPress 2 expuesta: la accesibilidad del archivo readme.html revela el uso de una versión del CMS extremadamente antigua y con múltiples fallos conocidos.
[MEDIUM] Falta de X-Content-Type-Options: el servidor no previene el sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos maliciosos.
[MEDIUM] Falta de Referrer-Policy: no se controla la información de navegación que el sitio envía a dominios externos al hacer clic en enlaces.
[MEDIUM] Falta de Permissions-Policy: no se restringe el acceso de las APIs del navegador a funciones sensibles como la cámara o el micrófono del usuario.

[LOW] Server header expuesto: la cabecera revela el uso de Apache, proporcionando información valiosa a atacantes para buscar exploits específicos.
[LOW] Ausencia de robots.txt y sitemap.xml: la falta de estos archivos, junto con errores 403 de acceso, dificulta la gestión de indexación y seguridad básica.