EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.waldemar.es	Checks	9 pruebas
Dominio	www.waldemar.es	Hallazgos	46 totales
Fecha	26 de marzo de 2026 a las 13:52	Problemas	14 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 60/100, lo que corresponde a una calificación de grado C. Durante la evaluación, se ejecutaron 9 comprobaciones pasivas que resultaron en 4 puntos validados correctamente, 3 advertencias de configuración y 2 fallos críticos de seguridad. Los resultados indican una exposición significativa de servicios internos y el uso de software con versiones obsoletas. Por lo tanto, se concluye que el sitio es actualmente vulnerable y requiere intervenciones técnicas inmediatas para reducir el riesgo de explotación.

Resumen de Riesgos

1	6	5	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 54 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 3.5.2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
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 54 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  54 dias restantes (expira: 2026-05-19T09:49:32.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-18T09:49:33.000Z
- 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 301 redirige a https://www.waldemar.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: Site Kit by Google 1.175.0
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 3.5.2 expuesta

- ALTO **WordPress version**
  Version 3.5.2 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- 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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (62 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://waldemar.es/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), 3306 (MySQL)

- 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): ABIERTO — La base de datos está expuesta a internet, lo que permite intentos de acceso no autorizados y ataques de fuerza bruta.
[HIGH] WordPress version: Version 3.5.2 expuesta publicamente — Esta versión es extremadamente antigua y cuenta con múltiples vulnerabilidades conocidas (CVEs) que facilitan el compromiso total del sitio.
[HIGH] Content-Security-Policy: Falta — La ausencia de esta cabecera permite ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Falta — El sitio es vulnerable a ataques de clickjacking al permitir que el contenido sea embebido en marcos externos.
[HIGH] Strict-Transport-Security: Falta — No se obliga al navegador a usar conexiones seguras, permitiendo ataques de degradación de protocolo.
[HIGH] Puerto 21 (FTP): ABIERTO — El servicio de transferencia de archivos está accesible, utilizando protocolos que transmiten credenciales sin cifrar.
[MEDIUM] X-Content-Type-Options: Falta — El navegador podría interpretar archivos de forma incorrecta, facilitando la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: Falta — No se controla la información de navegación que se envía a sitios terceros a través de los enlaces.
[MEDIUM] Permissions-Policy: Falta — No se restringen funciones del navegador como la geolocalización o el acceso a hardware desde el sitio.
[MEDIUM] Recurso HTTP (href): http://gmpg.org/xfn/11 — Se detectó contenido mixto que debilita la integridad de la conexión cifrada.
[MEDIUM] Ruta /wp-login.php: Panel de login accesible — La exposición del panel administrativo facilita ataques dirigidos contra las cuentas de usuario.
[LOW] Server header expuesto: Server: Apache — Se revela el software del servidor, ayudando a los atacantes a perfilar la infraestructura.
[LOW] Meta generator: Expone: Site Kit by Google 1.175.0 — Se divulgan versiones de herramientas específicas integradas en el CMS.