EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://babelt1900.com/	Checks	9 pruebas
Dominio	babelt1900.com	Hallazgos	47 totales
Fecha	20 de mayo de 2026 a las 20:50	Problemas	15 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre babelt1900.com arroja una puntuación de 64/100, lo que equivale a una nota de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fallaron debido a configuraciones críticas ausentes. Se han detectado carencias importantes en las cabeceras de seguridad y una exposición peligrosa de la versión del sistema de gestión de contenidos. Debido a la presencia de puertos de administración abiertos y software desactualizado, el sitio web se considera actualmente vulnerable ante ataques externos.

Resumen de Riesgos

0	6	6	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 296 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
Version CMS Expuesta	20	FALLO	WordPress 7.0 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 296 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  296 dias restantes (expira: 2027-03-12T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-26T00:00:00.000Z
- 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://babelt1900.com/
- 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

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 7.0
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0 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 (68 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.xml**
  Presente, ? URLs
- 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: Falta — La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Falta — El sitio es vulnerable a ataques de clickjacking, permitiendo que atacantes carguen la web en frames externos.
[HIGH] Strict-Transport-Security: Falta — No se fuerza el protocolo HTTPS a nivel de navegador, permitiendo posibles degradaciones de conexión (SSL Stripping).
[HIGH] WordPress version: Versión 7.0 expuesta públicamente — El uso de versiones desactualizadas permite a atacantes explotar vulnerabilidades conocidas (CVEs) para tomar el control del sitio.
[HIGH] Puerto 21 (FTP): ABIERTO — El servicio FTP transmite datos y credenciales en texto plano, siendo altamente susceptible a interceptación.
[MEDIUM] X-Content-Type-Options: Falta — El navegador podría intentar interpretar el contenido de forma distinta al tipo MIME declarado, facilitando la ejecución de scripts.
[MEDIUM] Referrer-Policy: Falta — No se controla la información de referencia enviada a terceros, lo que puede filtrar URLs internas.
[MEDIUM] Permissions-Policy: Falta — El sitio no restringe el acceso de las APIs del navegador a funciones sensibles como la cámara o el micrófono.
[MEDIUM] Archivo /readme.html: Accesible — Este archivo confirma detalles técnicos y versiones del CMS a cualquier usuario o bot.
[MEDIUM] Ruta /wp-login.php: Expuesta — El panel de acceso administrativo está visible, facilitando ataques de fuerza bruta contra las credenciales.
[MEDIUM] Puerto 22 (SSH): ABIERTO — La exposición de este puerto de administración remota aumenta la superficie de ataque para accesos no autorizados.
[LOW] Server header: Expone Apache — Se revela la tecnología del servidor web, facilitando el perfilado para ataques específicos.
[LOW] Meta generator: Expone WordPress 7.0 — Etiqueta en el código fuente que confirma la versión del software a herramientas de escaneo automatizado.
[LOW] Ruta sensible en robots.txt: Referencia a "admin" — El archivo indica proactivamente a los rastreadores dónde se encuentran las áreas restringidas.