EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://pormabeva.es/	Checks	9 pruebas
Dominio	pormabeva.es	Hallazgos	42 totales
Fecha	24 de junio de 2026 a las 05:59	Problemas	12 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha resultado en una puntuación de 72/100, lo que otorga una calificación de nota C. Durante la evaluación, se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, se identificó una advertencia y se detectaron 2 fallos críticos en la configuración. Aunque la implementación del cifrado de datos es correcta, la ausencia de políticas de seguridad en las cabeceras del servidor representa un riesgo de explotación. Por tanto, el sitio se considera actualmente vulnerable ante ataques de inyección y suplantación de identidad. Se requiere la aplicación inmediata de medidas correctivas para elevar el estándar de protección.

Resumen de Riesgos

0	4	7	1	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 67 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	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 67 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  67 dias restantes (expira: 2026-08-30T15:51:55.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-01T15:51:56.000Z
- 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: nginx — 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://pormabeva.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

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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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 Inteligencia Artificial

---RESUMEN EJECUTIVO---
El análisis de ciberseguridad realizado al sitio web ha resultado en una puntuación de 72/100, lo que otorga una calificación de nota C. Durante la evaluación, se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, se identificó una advertencia y se detectaron 2 fallos críticos en la configuración. Aunque la implementación del cifrado de datos es correcta, la ausencia de políticas de seguridad en las cabeceras del servidor representa un riesgo de explotación. Por tanto, el sitio se considera actualmente vulnerable ante ataques de inyección y suplantación de identidad. Se requiere la aplicación inmediata de medidas correctivas para elevar el estándar de protección.

---VULNERABILITIES---
[HIGH] Content-Security-Policy: Falta esta cabecera esencial para prevenir ataques XSS y la inyección de contenido malicioso en el navegador del usuario.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce siempre una conexión segura HTTPS.
[MEDIUM] X-Content-Type-Options: Falta esta cabecera para evitar que los navegadores realicen MIME-type sniffing y ejecuten archivos con formatos incorrectos.

[MEDIUM] Referrer-Policy: No existe una política definida para controlar cuánta información de referencia se envía a otros sitios web al navegar.
[MEDIUM] Permissions-Policy: No se han establecido restricciones sobre el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Archivos técnicos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, lo que puede revelar detalles internos de la plataforma.
[MEDIUM] Paneles de gestión accesibles: Las rutas /administrator/ y /user/login están abiertas al público, aumentando el riesgo de ataques de fuerza bruta.
[LOW] Exposición de cabecera de servidor: Se revela el uso de la tecnología nginx, proporcionando información útil a posibles atacantes sobre la infraestructura.
[LOW] Ausencia de archivos de indexación: No se detectaron robots.txt ni sitemap.xml, lo que dificulta la gestión del rastreo por parte de buscadores.