EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cashbeltran.es/	Checks	9 pruebas
Dominio	cashbeltran.es	Hallazgos	46 totales
Fecha	17 de agosto de 2026 a las 06:35	Problemas	15 detectados

C

63/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 63/100, lo que equivale a una calificación de grado C. Se ejecutaron 9 checks pasivos, resultando en 5 verificaciones exitosas, 1 advertencia y 3 fallos críticos en la configuración. Aunque el cifrado de datos es correcto, la exposición de servicios internos y la falta de cabeceras de seguridad básicas comprometen la integridad del servidor. En su estado actual, el sitio se considera vulnerable a ataques dirigidos debido a la visibilidad de información técnica sensible y puertos críticos abiertos.

Resumen de Riesgos

1	6	5	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 66 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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 6.9.1 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	20	FALLO	4 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 66 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  66 dias restantes (expira: 2026-10-21T21:34:41.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-23T21:34:42.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.4.2 — Revela framework/lenguaje
- 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
- INFO **Permissions-Policy**
  Presente: private-state-token-redemption=(self "https://www.google.com" "https://www.gstat...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://cashbeltran.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: WordPress 6.9.1
- INFO **Tecnologias detectadas**
  Next.js, PHP/7.4.2

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.1 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)

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 (14 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 0 Allow
- INFO **sitemap.xml**
  Presente, ? URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

4 puertos riesgosos abiertos

- 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
- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 3306 (MySQL): Servicio de base de datos expuesto públicamente, permitiendo intentos de acceso no autorizados y ataques de fuerza bruta.
[HIGH] Content-Security-Policy: Ausencia de esta cabecera, lo que facilita ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Falta de protección contra clickjacking, permitiendo que el sitio sea embebido en marcos maliciosos.
[HIGH] Strict-Transport-Security: No se aplica la política HSTS, dejando a los usuarios vulnerables a ataques de degradación de protocolo (SSL Stripping).
[HIGH] Versión de WordPress expuesta: Se detectó la versión 6.9.1, lo que permite a atacantes identificar y explotar CVEs conocidos para esa versión específica.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos está abierto, lo cual es peligroso al transmitir credenciales y datos sin cifrado.
[MEDIUM] X-Content-Type-Options: Falta de esta cabecera, permitiendo que el navegador realice MIME-type sniffing y ejecute contenido malicioso disfrazado.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a sitios externos al navegar.
[MEDIUM] Archivo /readme.html accesible: Este archivo revela detalles técnicos del CMS que facilitan la fase de reconocimiento de un atacante.
[MEDIUM] Puerto 22 (SSH): Interfaz de administración remota expuesta, incrementando el riesgo de intrusión mediante ataques automatizados de credenciales.
[MEDIUM] Puerto 8080 (HTTP-Alt): Servidor web alternativo activo que amplía la superficie de ataque disponible.
[LOW] Server header expuesto: El servidor revela que utiliza Apache, proporcionando pistas sobre la infraestructura subyacente.
[LOW] X-Powered-By expuesto: Se muestra la versión exacta de PHP/7.4.2, permitiendo la búsqueda de debilidades específicas del lenguaje.
[LOW] Meta generator: La etiqueta meta expone públicamente el uso de WordPress 6.9.1 en el código fuente.