EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cpdbugarra.com	Checks	9 pruebas
Dominio	cpdbugarra.com	Hallazgos	56 totales
Fecha	13 de mayo de 2026 a las 07:01	Problemas	22 detectados

D

48/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 48/100, lo que equivale a una calificación de grado D. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales únicamente 3 resultaron exitosos, mientras que se registraron 2 advertencias y 4 fallos críticos. Se han detectado deficiencias severas en la configuración de cabeceras de seguridad, exposición de puertos de base de datos y versiones obsoletas del CMS. Debido a la acumulación de vulnerabilidades de alto impacto, el sitio se considera actualmente vulnerable y con un riesgo elevado de compromiso. Es imperativo aplicar medidas correctivas de forma inmediata para proteger la infraestructura.

Resumen de Riesgos

1	6	12	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 49 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 6.9.4 expuesta, WordPress 2 expuesta
Seguridad de Cookies	67	AVISO	ep_session_id: falta SameSite; ep_session_id: fa...
Contenido Mixto	20	FALLO	4 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 49 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  49 dias restantes (expira: 2026-07-01T08:13:23.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-02T08:13:24.000Z
- 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: HTTPd — 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://cpdbugarra.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, 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 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 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 — 67/100

Estado: AVISO

ep_session_id: falta SameSite; ep_session_id: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: ep_session_id — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ep_session_id — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ep_session_id — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: ep_session_id — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ep_session_id — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ep_session_id — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

4 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://cpdbugarra.com/wp-content/uploads/elementor/google-fo...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://cpdbugarra.com/wp-content/uploads/elementor/google-fo...
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (115 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 en robots.txt**
  https://cpdbugarra.com/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 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
- 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): La base de datos MySQL se encuentra expuesta públicamente, lo que permite ataques directos de fuerza bruta o acceso no autorizado a la información.
[HIGH] WordPress version: La versión 6.9.4 de WordPress está expuesta, permitiendo que atacantes identifiquen y exploten vulnerabilidades conocidas (CVEs) para este software desactualizado.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Falta de protección contra ataques de clickjacking, permitiendo que el sitio sea cargado en marcos externos maliciosos.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce conexiones seguras y deja la comunicación vulnerable a ataques de degradación.
[HIGH] Puerto 21 (FTP): Este puerto está abierto para transferencia de archivos sin cifrar, lo que expone las credenciales de administración en la red.
[MEDIUM] Cookie ep_session_id: Las cookies de sesión carecen del atributo SameSite, lo que hace al sitio vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se detectaron recursos cargados mediante HTTP en una página HTTPS, comprometiendo la integridad del cifrado y la privacidad.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que los navegadores realicen "MIME-type sniffing", pudiendo ejecutar archivos con contenido malicioso disfrazado.
[MEDIUM] Puerto 22 (SSH): El acceso remoto seguro está abierto, lo que representa un vector de ataque si no existen políticas de bloqueo de IP o autenticación robusta.
[MEDIUM] Archivo /readme.html y /wp-login.php: Estos archivos y rutas son accesibles públicamente, revelando detalles técnicos y facilitando ataques al panel de administración.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios, lo que puede filtrar datos de navegación.
[MEDIUM] Permissions-Policy: No se restringe el uso de APIs del navegador como la cámara o el micrófono, aumentando la superficie de riesgo para el usuario.
[LOW] Server header expuesto: El servidor revela el uso de "HTTPd", facilitando la fase de reconocimiento de un atacante.
[LOW] Meta generator: La etiqueta meta expone explícitamente la versión del CMS WordPress utilizada.
[LOW] Ruta sensible en robots.txt: El archivo de rastreo referencia rutas como "admin", guiando a los atacantes hacia áreas administrativas.