EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://concrepal.com	Checks	9 pruebas
Dominio	concrepal.com	Hallazgos	43 totales
Fecha	8 de mayo de 2026 a las 16:44	Problemas	13 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio concrepal.com ha otorgado una puntuación de 62/100, lo que resulta en una nota de calificación C. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 4 resultados satisfactorios, 3 advertencias y 2 fallos críticos relacionados con la configuración del servidor y la visibilidad de la infraestructura. La detección de puertos de bases de datos expuestos y servicios de transferencia de archivos sin cifrar representa un riesgo significativo. A pesar de contar con un cifrado SSL activo, la ausencia de cabeceras de seguridad y el uso de software desactualizado permiten concluir que el sitio es actualmente vulnerable ante ataques dirigidos y automatizados.

Resumen de Riesgos

1	6	4	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 144 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 5.8.1 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	60	AVISO	Falta robots.txt
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 144 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  144 dias restantes (expira: 2026-09-29T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-29T00:00:00.000Z
- 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://concrepal.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 5.8.1
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 5.8.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 5.8.1 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 — 60/100

Estado: AVISO

Falta robots.txt

- 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), 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): La base de datos se encuentra abierta y accesible desde internet, lo que permite ataques de fuerza bruta y posibles robos de información.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos expuesto que transmite credenciales y datos en texto plano, facilitando la interceptación de información.
[HIGH] WordPress version: Se detectó la versión 5.8.1 expuesta públicamente, la cual es obsoleta y contiene vulnerabilidades conocidas que pueden ser explotadas.
[HIGH] Content-Security-Policy: Cabecera ausente, lo que deja al sitio web vulnerable a ataques de Cross-Site Scripting (XSS) e inyecciones de código.

[HIGH] X-Frame-Options: La falta de esta cabecera permite ataques de clickjacking, donde un atacante puede engañar al usuario para que realice acciones no deseadas.
[HIGH] Strict-Transport-Security: HSTS no está configurado, impidiendo que el navegador obligue siempre el uso de conexiones seguras HTTPS.
[MEDIUM] X-Content-Type-Options: La ausencia de esta directiva permite el MIME-type sniffing, aumentando el riesgo de ejecución de archivos maliciosos ocultos.
[MEDIUM] Referrer-Policy: No se controla la información que se envía a otros sitios web al navegar desde este dominio.
[MEDIUM] Permissions-Policy: No existen restricciones sobre el acceso de las APIs del navegador a funciones como la cámara o el micrófono del usuario.
[MEDIUM] Archivo /readme.html: Este archivo de WordPress es accesible públicamente y facilita información técnica sobre la instalación a potenciales atacantes.
[LOW] Server header expuesto: El encabezado revela que el servidor utiliza Apache, lo que ayuda a los atacantes a buscar vectores de ataque específicos para ese software.
[LOW] Meta generator: La etiqueta meta expone la versión exacta de WordPress instalada en el sitio.