EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://castillaflores.com/	Checks	9 pruebas
Dominio	castillaflores.com	Hallazgos	48 totales
Fecha	28 de julio de 2026 a las 16:24	Problemas	15 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha resultado en una puntuación de 65/100, lo que otorga una nota de grado C. Los resultados de los 9 checks pasivos ejecutados muestran un escenario de riesgo moderado, con 4 verificaciones correctas, 3 advertencias y 2 fallos críticos de configuración. Aunque el cifrado básico de datos es funcional, la exposición de servicios internos y la ausencia de cabeceras de protección comprometen la seguridad global. En su estado actual, el sitio se considera vulnerable debido a la visibilidad de su infraestructura y la falta de políticas estrictas de transporte de datos. Es imperativo implementar medidas correctivas para elevar el nivel de protección de la plataforma.

Resumen de Riesgos

1	5	5	4	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 59 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
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 1785174483 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
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 59 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  59 dias restantes (expira: 2026-09-25T18:46:42.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-27T18:46:43.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

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

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.30 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://castillaflores.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: Site Kit by Google 1.183.0
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.2.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1785174483 expuesta

- ALTO **WordPress version**
  Version 1785174483 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)

- 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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.la-weberia.com
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.la-weberia.com

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (321 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://castillaflores.com/wp-sitemap.xml
- 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): Base de datos expuesta públicamente, lo que permite intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos abierto que transmite información sin cifrado, facilitando la interceptación de credenciales.
[HIGH] WordPress versión expuesta: La visibilidad pública de la versión exacta del CMS permite a atacantes identificar vulnerabilidades específicas ya documentadas.
[HIGH] X-Frame-Options: Falta de cabecera que protege contra ataques de clickjacking, permitiendo que el sitio sea cargado en marcos maliciosos.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador obligue siempre a realizar conexiones cifradas.
[MEDIUM] Contenido Mixto: Se detectaron recursos cargados mediante HTTP en una página segura, lo que degrada la integridad de la conexión.
[MEDIUM] X-Content-Type-Options: Cabecera ausente necesaria para evitar que el navegador realice sniffing de tipos MIME.
[MEDIUM] Referrer-Policy: Falta de control sobre la información de origen que el sitio envía a otros dominios durante la navegación.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el acceso de la plataforma a APIs sensibles del navegador como cámara o micrófono.
[LOW] Server header expuesto: El servidor revela el uso de tecnología LiteSpeed, facilitando el reconocimiento para ataques dirigidos.
[LOW] X-Powered-By expuesto: Se expone la versión de PHP utilizada, lo que ayuda a perfilar el entorno de ejecución del servidor.
[LOW] Meta generator: El código fuente muestra el uso de Site Kit by Google, revelando herramientas de análisis internas.
[LOW] Ruta sensible en robots.txt: Se menciona la ruta de administración, guiando a posibles atacantes hacia áreas restringidas.