

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://castlexpert.com  
Dominio castlexpert.com  
Fecha 8 de mayo de 2026 a las 16:43

Checks 9 pruebas  
Hallazgos 46 totales  
Problemas 13 detectados

# C

## 72/100

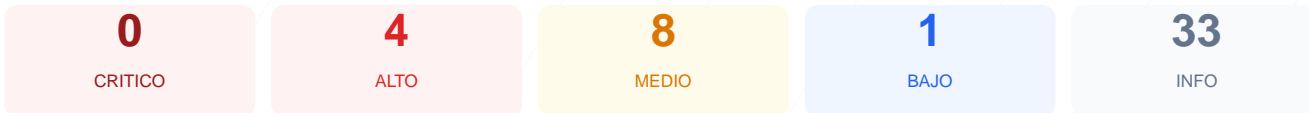
puntos de seguridad



### RESUMEN EJECUTIVO

El sitio castlexpert.com ha obtenido una puntuación de seguridad de 72/100, lo que equivale a una nota C según los estándares de auditoría. Se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue calificado como fallo crítico debido a la ausencia de cabeceras de protección. Aunque el cifrado de datos es correcto, la infraestructura presenta debilidades en la configuración del servidor y exposición de rutas técnicas. Se concluye que el sitio es vulnerable ante ataques de inyección de scripts y secuestro de clics. La implementación de medidas correctivas es necesaria para alcanzar un nivel de seguridad robusto.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

### SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 79 dias

- INFO **Certificado valido**  
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**  
79 dias restantes (expira: 2026-07-26T18:41:02.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-04-27T18:41:03.000Z
- 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: cloudflare — 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://castlexpert.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

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
- **INFO** **Archivo /README.txt**  
No accesible (correcto)
- **MEDIO** **Ruta /wp-login.php**  
Panel de login accesible publicamente
- **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 — 100/100

---

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**  
Presente (170 bytes)
- INFO **Reglas robots.txt**  
0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**  
https://castlexpert.com/sitemap.xml
- **BAJO** **security.txt**  
No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 60/100

---

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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 autentificacion 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

- [HIGH] Content-Security-Policy: Falta esta cabecera, lo que permite la ejecución de scripts no autorizados y ataques XSS.
- [HIGH] X-Frame-Options: Su ausencia hace al sitio susceptible a ataques de clickjacking al permitir que se cargue en iframes externos.
- [HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no obliga a usar conexiones cifradas permanentemente.
- [MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, facilitando la ejecución de archivos maliciosos disfrazados.
- [MEDIUM] Referrer-Policy: No hay control sobre la información de origen que se envía a otros sitios web al navegar desde castleexpert.com.
- [MEDIUM] Permissions-Policy: No se restringen funciones del navegador como el acceso a la cámara o geolocalización a través de APIs.
- [MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede contener información técnica sobre la infraestructura.
- [MEDIUM] Rutas administrativas expuestas: Se detectó acceso público a paneles de gestión en /wp-login.php, /administrator/ y /user/login.
- [MEDIUM] Puerto 8080 (HTTP-Alt): Se encontró este puerto abierto, lo cual representa un vector de ataque adicional por ser un servicio web alternativo.
- [LOW] Server header expuesto: El servidor revela el uso de Cloudflare, proporcionando pistas a posibles atacantes sobre la tecnología de red.