EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.carohotel.com/	Checks	9 pruebas
Dominio	www.carohotel.com	Hallazgos	44 totales
Fecha	1 de agosto de 2026 a las 04:36	Problemas	14 detectados

D

58/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre la plataforma arroja una puntuación de 58/100, lo que resulta en una calificación de grado D. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 4 resultaron correctos, 2 generaron advertencias y 3 fueron identificados como fallos críticos. Aunque la infraestructura cuenta con un cifrado SSL válido, se detectaron deficiencias graves en la configuración de cabeceras de seguridad y exposición de servicios internos. El nivel de riesgo actual es elevado debido a la visibilidad de puertos críticos y la falta de protecciones contra ataques web comunes. Se concluye que el sitio es vulnerable y requiere intervenciones técnicas inmediatas para asegurar su integridad y la de sus usuarios.

Resumen de Riesgos

1	6	5	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 186 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
Version CMS Expuesta	20	FALLO	WordPress 7.0.2 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	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 186 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  186 dias restantes (expira: 2027-02-03T11:40:05.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-02T11:40:06.000Z
- 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://www.carohotel.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

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 7.0.2
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0.2 expuesta

- ALTO **WordPress version**
  Version 7.0.2 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 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): Base de datos expuesta públicamente, lo que permite intentos de acceso externo y ataques de fuerza bruta.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Falta de protección contra ataques de clickjacking, permitiendo que el sitio sea cargado en marcos externos no autorizados.

[HIGH] Strict-Transport-Security: No se fuerza la conexión segura mediante HSTS, permitiendo ataques de degradación de protocolo SSL.
[HIGH] WordPress version: La versión 7.0.2 está expuesta públicamente, permitiendo que atacantes identifiquen vulnerabilidades específicas para esa versión.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos abierto que transmite credenciales y datos sin cifrado.
[HIGH] HSTS no configurado: El servidor no instruye al navegador para usar exclusivamente conexiones HTTPS, comprometiendo la redirección segura.
[MEDIUM] X-Content-Type-Options: Falta de cabecera para evitar que el navegador interprete archivos con tipos MIME incorrectos.
[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada en las peticiones, lo que puede filtrar URLs internas.
[MEDIUM] Permissions-Policy: Ausencia de restricciones sobre el uso de APIs del navegador como cámara, micrófono o geolocalización.
[MEDIUM] Ruta /wp-login.php: El panel de administración de WordPress es accesible públicamente, facilitando ataques de fuerza bruta contra cuentas de usuario.
[MEDIUM] Puerto 22 (SSH): Acceso remoto seguro abierto, lo que expande la superficie de ataque si no está correctamente limitado por IP.
[LOW] Server header expuesto: El servidor revela el uso de HTTPd, proporcionando pistas sobre la infraestructura tecnológica a potenciales atacantes.
[LOW] Meta generator: La etiqueta meta expone explícitamente el uso de WordPress 7.0.2 en el código fuente.