EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://consultoriadata.com/	Checks	9 pruebas
Dominio	consultoriadata.com	Hallazgos	48 totales
Fecha	31 de julio de 2026 a las 01:54	Problemas	14 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre consultoriadata.com arroja una puntuación de 64/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 checks pasivos, resultando en 5 verificaciones correctas, 2 advertencias y 2 fallos críticos. Aunque el sitio cuenta con un cifrado SSL válido, la ausencia total de cabeceras de seguridad y la exposición pública de la versión del gestor de contenidos representan un riesgo significativo. Debido a la falta de políticas de protección contra ataques comunes y la visibilidad de rutas administrativas, se concluye que el sitio es actualmente vulnerable. Es imperativo realizar correcciones técnicas para mitigar posibles explotaciones de seguridad.

Resumen de Riesgos

0	5	6	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 83 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 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	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 83 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  83 dias restantes (expira: 2026-10-22T01:27:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-24T01:28:00.000Z
- 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: 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://consultoriadata.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 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (2031 bytes)
- INFO **Reglas robots.txt**
  11 Disallow, 2 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://consultoriadata.com/sitemaps.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 autenticacion 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] WordPress version: Version 7.0.2 expuesta publicamente lo que permite a atacantes buscar CVEs conocidos para comprometer el servidor.
[HIGH] Content-Security-Policy: Falta esta cabecera esencial para prevenir ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: No configurada, lo que deja el sitio expuesto a ataques de clickjacking mediante el uso de marcos externos.
[HIGH] Strict-Transport-Security: Ausencia de HSTS, impidiendo que el navegador fuerce conexiones seguras HTTPS de forma permanente.
[HIGH] HSTS (Strict-Transport-Security): El mecanismo de seguridad no esta configurado, permitiendo posibles ataques de degradacion de protocolo.
[MEDIUM] X-Content-Type-Options: Falta la directiva que evita el sniffing de tipos MIME por parte del navegador.
[MEDIUM] Referrer-Policy: No se ha definido una politica de referencia, lo que puede filtrar informacion de navegacion a sitios externos.
[MEDIUM] Permissions-Policy: No se restringe el acceso a las APIs del navegador como la camara o el microfono desde el sitio.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detecto un servidor web alternativo o proxy abierto, aumentando la superficie de ataque disponible.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es publicamente accesible, facilitando intentos de fuerza bruta.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea la indexacion de todo el sitio y referencia rutas sensibles como admin.
[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, proporcionando informacion tecnica sobre la infraestructura.
[LOW] Meta generator: El codigo fuente expone directamente el uso de WordPress 7.0.2 y su tecnologia asociada.