EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://prodato.cl/	Checks	9 pruebas
Dominio	prodato.cl	Hallazgos	48 totales
Fecha	3 de abril de 2026 a las 14:05	Problemas	8 detectados

A

94/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al dominio ha arrojado una puntuación de 94/100 con una calificación final de nota A. Se ejecutaron un total de 9 checks pasivos, obteniendo 7 resultados satisfactorios y 2 advertencias, sin detectarse fallos críticos de seguridad. Los sistemas de cifrado y las cabeceras de protección presentan una configuración óptima, lo que garantiza una comunicación segura. En conclusión, el sitio se considera seguro, aunque requiere ajustes en la exposición de archivos técnicos y puertos para mitigar riesgos de reconocimiento.

Resumen de Riesgos

0	0	7	1	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 84 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  84 dias restantes (expira: 2026-06-26T22:07:42.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-28T22:07:43.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
  Presente: default-src 'none'; script-src 'self' https://cdn.jsdelivr.net https://fonts.goo...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: camera=(), microphone=(), geolocation=(), payment=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://prodato.cl/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (2182 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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

[LOW] Cabecera de servidor expuesta: El valor Server: cloudflare revela la tecnología de infraestructura utilizada, facilitando la identificación de posibles vectores de ataque.
[MEDIUM] Archivo /readme.html accesible: Este archivo informativo se encuentra disponible públicamente y puede filtrar detalles técnicos sobre la plataforma.
[MEDIUM] Archivo /README.txt accesible: La visibilidad de este recurso permite a terceros obtener información sobre la estructura o versión del sistema.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de acceso es detectable, lo que lo hace susceptible a ataques de fuerza bruta.
[MEDIUM] Ruta /administrator/ expuesta: La interfaz de gestión administrativa es accesible desde internet sin restricciones de red.
[MEDIUM] Ruta /user/login expuesta: Se ha identificado un punto de entrada para usuarios que podría ser explotado mediante ingeniería social o ataques automatizados.
[MEDIUM] Bloqueo total en robots.txt: La directiva Disallow: / impide la indexación legítima y señala una configuración de ocultamiento que atrae la atención de atacantes.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un servidor web alternativo activo incrementa la superficie de ataque fuera de los puertos estándar.
[LOW] Ausencia de sitemap.xml: El sitio carece de un mapa de estructura, lo que dificulta la auditoría de contenidos y la navegación de motores de búsqueda.