EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://intercity.cl	Checks	9 pruebas
Dominio	intercity.cl	Hallazgos	52 totales
Fecha	23 de junio de 2026 a las 16:24	Problemas	15 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio intercity.cl arroja una puntuación de 68/100, lo que resulta en una calificación de grado C. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 fueron satisfactorios y 3 presentaron fallos críticos que comprometen la integridad de la plataforma. El sitio demuestra un manejo sólido del cifrado de datos y redirecciones, pero falla significativamente en la implementación de cabeceras de seguridad y en la protección de información del sistema. Debido a la exposición de versiones del CMS y la presencia de contenido mixto, el sitio se clasifica actualmente como vulnerable a ataques de inyección y ataques de intermediario. Se requiere una intervención técnica inmediata para elevar los estándares de protección actuales.

Resumen de Riesgos

0	3	9	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 130 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.0 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	7 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 130 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  130 dias restantes (expira: 2026-10-31T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-16T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: nginx — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.intercity.cl/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no 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

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
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0 expuesta publicamente — Permite a atacantes buscar CVEs conocidos

- 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

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 — 20/100

Estado: FALLO

7 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://mail.intercity.cl:90/CGI-BIN/WCONSOLE.DLL
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://panel.intercity.net:9001/Default.aspx?pid=Login&...
- MEDIO **href (link/stylesheet)**
  ...y 4 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (738 bytes)
- INFO **Reglas robots.txt**
  16 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.intercity.cl/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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
- 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

[HIGH] WordPress version: Version 7.0 expuesta publicamente — Permite a atacantes buscar CVEs conocidos para explotar el sitio.
[HIGH] Content-Security-Policy: Falta — La ausencia de esta cabecera facilita ataques de XSS y de inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: Falta — Deja el sitio desprotegido ante ataques de clickjacking, permitiendo que sea cargado en frames externos.
[MEDIUM] Contenido Mixto: 7 recursos HTTP en pagina HTTPS — El uso de enlaces hacia mail.intercity.cl y panel.intercity.net sin cifrar debilita la seguridad de la sesion.
[MEDIUM] X-Content-Type-Options: Falta — No previene que el navegador realice MIME-type sniffing, aumentando el riesgo de ejecucion de scripts.
[MEDIUM] Referrer-Policy: Falta — No se controla la informacion de navegacion que se envia a otros sitios web.
[MEDIUM] Permissions-Policy: Falta — El sitio no restringe el acceso de las APIs del navegador a componentes sensibles como camara o microfono.
[MEDIUM] Archivo /readme.html: Archivo accesible publicamente — Este documento suele revelar detalles especificos de la instalacion y version del CMS.
[MEDIUM] Ruta /wp-login.php: Panel de login accesible publicamente — Facilita el reconocimiento para ataques dirigidos de fuerza bruta contra las credenciales.
[LOW] Server header expuesto: Server: nginx — La cabecera revela el software del servidor, facilitando la planificacion de ataques especificos.
[LOW] Meta generator: Expone: WordPress 7.0 — Divulga informacion interna sobre la tecnologia utilizada en el sitio.
[LOW] Ruta sensible en robots.txt: Referencia a "admin" — Indica a los rastreadores y atacantes potenciales la localizacion de directorios privados.