

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://passline.cl	Checks	9 pruebas
Dominio	passline.cl	Hallazgos	45 totales
Fecha	25 de agosto de 2026 a las 14:57	Problemas	6 detectados

B

84/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 84/100, obteniendo una calificación final de grado B. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron correctos, 3 presentaron advertencias y 1 fue identificado como fallo. Los resultados destacan una implementación sólida del cifrado SSL, aunque se detectaron debilidades importantes en las cabeceras de transporte seguro y la exposición de puertos innecesarios. En conclusión, el sitio se considera seguro para operaciones básicas, pero presenta vulnerabilidades de configuración que deben ser mitigadas para prevenir ataques de intermediario. La ausencia de un pentest activo impide confirmar la existencia de vulnerabilidades más profundas en la lógica de la aplicación.

Resumen de Riesgos

0	2	1	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
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	1 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
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: 2026-11-12T18:34:38.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-14T17:37:11.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

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

- INFO

Content-Security-Policy
Presente: default-src 'none'; script-src 'nonce-QGnnOrP0cpAJ74RnFNLIFM' 'unsafe-eval' http...
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: same-origin
- INFO

Permissions-Policy
Presente: accelerometer=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),g...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://www.passline.com/chile
- ALTO

HSTS (Strict-Transport-Security)
HSTS no configurado — El navegador no fuerza HTTPS
- INFO

Respuesta HTTPS
HTTPS responde con status 403

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

- INFO

Archivo /readme.html
No accesible (correcto)
- INFO

Archivo /README.txt
No accesible (correcto)
- INFO

Version CMS
No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

1 cookies, todas con flags correctos

- INFO

Cookies detectadas
1 cookie(s) encontrada(s)
- INFO

Cookie: __cf_bm — HttpOnly
HttpOnly activo — No accesible via JavaScript
- INFO

Cookie: __cf_bm — Secure
Flag Secure activo — Solo se envia por HTTPS
- INFO

Cookie: __cf_bm — SameSite
SameSite=none

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO

robots.txt
No encontrado (HTTP 403)
- BAJO

sitemap.xml
No encontrado (HTTP 403)
- 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] Strict-Transport-Security: La cabecera HSTS no está configurada, lo que impide que el navegador fuerce conexiones seguras y permite ataques de degradación de protocolo.

[HIGH] HSTS no configurado: El servidor redirige tráfico HTTP a HTTPS, pero al no tener una política HSTS activa, los usuarios son vulnerables a la interceptación en su primera conexión.

[MEDIUM] Puerto 8080 (HTTP-Alt) ABIERTO: Se detectó un servidor web alternativo o proxy expuesto, lo que incrementa la superficie de ataque y posibles accesos no autorizados a servicios internos.

[LOW] Server header expuesto: La cabecera de respuesta revela el uso de Cloudflare, proporcionando información técnica que facilita el reconocimiento por parte de actores maliciosos.

[LOW] robots.txt: El archivo de directivas de rastreo no fue encontrado o devuelve un error 403, dificultando la gestión de la indexación y privacidad del contenido.

[LOW] sitemap.xml: La ausencia de este archivo o su bloqueo mediante error 403 impide una auditoría clara de la estructura del sitio y sus endpoints públicos.