

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://flow.cfrd.cl	Checks	9 pruebas
Dominio	flow.cfrd.cl	Hallazgos	51 totales
Fecha	29 de mayo de 2026 a las 14:08	Problemas	3 detectados

A

93/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio flow.cfrd.cl arroja una puntuación técnica de 93/100, lo que equivale a una nota de A. Durante la auditoría se ejecutaron 9 checks pasivos, obteniendo 7 resultados satisfactorios y 2 advertencias, sin registrar fallos críticos. Aunque no se detectaron brechas de seguridad inmediatas, existen debilidades en la configuración de las cabeceras de respuesta y en la protección de cookies. En conclusión, el sitio web se considera seguro en su estado actual, pero requiere de ajustes preventivos para mitigar riesgos potenciales de inyección de código y robo de información de sesión.

Resumen de Riesgos

0 CRITICO	2 ALTO	0 MEDIO	1 BAJO	48 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 147 dias
Cabeceras de Seguridad	75	AVISO	5/6 presentes. Faltan: Content-Security-Policy
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	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
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 147 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
147 dias restantes (expira: 2026-10-23T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-04-08T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-Policy

- BAJO Server header expuesto
Server: Apache/2.4.67 (Debian) — Revela tecnologia del servidor

- ALTO

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- INFO

Strict-Transport-Security
Presente: max-age=31536000; includeSubDomains
- INFO

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

Referrer-Policy
Presente: strict-origin-when-cross-origin
- INFO

Permissions-Policy
Presente: camera=(), microphone=(), geolocation=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://flow.cfrd.cl/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31536000; includeSubDomains
- 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

- 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 — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO

Cookies detectadas
2 cookie(s) encontrada(s)
- ALTO

Cookie: XSRF-TOKEN — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO

Cookie: XSRF-TOKEN — Secure
Flag Secure activo — Solo se envía por HTTPS
- INFO

Cookie: XSRF-TOKEN — SameSite
SameSite=lax
- INFO

Cookie: flow-session — HttpOnly
HttpOnly activo — No accesible via JavaScript
- INFO

Cookie: flow-session — Secure
Flag Secure activo — Solo se envía por HTTPS
- INFO

Cookie: flow-session — SameSite
SameSite=lax

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 (67 bytes)
- INFO

Reglas robots.txt
1 Disallow, 0 Allow
- INFO

Sitemap en robots.txt
<https://flow.cfrd.cl/sitemap.xml>
- INFO

security.txt
Presente en /.well-known/security.txt — Buena practica

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 — Envío 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

[ALTA] Content-Security-Policy: La ausencia de esta cabecera de seguridad impide definir qué fuentes de contenido son confiables, lo cual facilita ataques de inyección de scripts y Cross-Site Scripting (XSS).

[ALTA] Cookie XSRF-TOKEN sin atributo HttpOnly: Esta configuración permite que la cookie de seguridad sea accesible a través de scripts del lado del cliente, incrementando el riesgo de secuestro de sesión en caso de un ataque XSS.

[BAJA] Server header expuesto: El servidor revela información técnica específica (Apache/2.4.67 Debian) en sus respuestas, lo que proporciona a un atacante datos útiles para buscar vulnerabilidades conocidas para esa versión de software.