

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://colegiodelvalle.cl	Checks	9 pruebas
Dominio	colegiodelvalle.cl	Hallazgos	57 totales
Fecha	8 de octubre de 2026 a las 01:32	Problemas	11 detectados

B

83/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado presenta una puntuacion de 83/100, lo que le otorga una nota B segun los estandares de auditoria pasiva. Se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios, uno presento advertencias y uno fallo criticamente en la configuracion de cabeceras. La infraestructura base es solida gracias al uso de Wix y Cloudflare, cumpliendo correctamente con el cifrado SSL y las redirecciones HTTPS. No obstante, la ausencia de politicas de seguridad avanzadas y deficiencias en la gestion de cookies exponen el sitio a riesgos conocidos. Se concluye que el sitio es generalmente seguro para la navegacion, pero vulnerable a ataques especificos de inyeccion de contenido y secuestro de sesion.

Resumen de Riesgos

0	5	4	2	46
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 46 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Wix
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	56	AVISO	XSRF-TOKEN: falta HttpOnly; ssr-caching: falta H...
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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 46 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
46 dias restantes (expira: 2026-11-22T15:54:51.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-24T15:54:52.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-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
- INFO

Strict-Transport-Security
Presente: max-age=31556952
- INFO

X-Content-Type-Options
Presente: nosniiff
- 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://colegiodelvalle.cl/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31556952
- BAJO

HSTS includeSubDomains
HSTS no cubre subdominios
- INFO

HSTS max-age
max-age=31556952 (365 dias)
- INFO

Respuesta HTTPS
HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Wix

- 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
Detectado via HTML body
- INFO

Squarespace
No detectado
- BAJO

Meta generator
Expone: Wix.com Website Builder
- INFO

Tecnologias detectadas
React, Next.js

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 — 56/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly; ssr-caching: falta HttpOnly; ssr-caching: falta Secure; ssr-caching: falta SameSite

- INFO

Cookies detectadas
3 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 envia por HTTPS
- INFO

Cookie: XSRF-TOKEN — SameSite
SameSite=none
- ALTO

Cookie: ssr-caching — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO

Cookie: ssr-caching — Secure
Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO

Cookie: ssr-caching — SameSite
Falta SameSite — Vulnerable a CSRF
- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt
Presente (496 bytes)
- INFO

Reglas robots.txt
4 Disallow, 1 Allow
- MEDIO

Bloqueo total
robots.txt bloquea todo el sitio con Disallow: /
- INFO

Sitemap en robots.txt
https://www.colegiodelvalle.cl/sitemap.xml
- BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
●	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] Content-Security-Policy: Falta esta cabecera, lo que aumenta el riesgo de ataques XSS y de inyeccion de contenido malicioso al no restringir las fuentes de scripts.

[HIGH] X-Frame-Options: La ausencia de esta cabecera deja el sitio expuesto a ataques de clickjacking, permitiendo que la web sea cargada en frames externos maliciosos.

[HIGH] Cookie XSRF-TOKEN: Carece del flag HttpOnly, permitiendo que la cookie sea accesible mediante scripts del lado del cliente, facilitando el robo de sesiones.

[HIGH] Cookie ssl-caching: No posee los atributos HttpOnly ni Secure, lo que permite el acceso via scripts y el envio de informacion sobre conexiones no cifradas.

[MEDIUM] Referrer-Policy: No se ha definido una politica de referente, lo que podria filtrar informacion sensible de la URL a sitios de terceros durante la navegacion.

[MEDIUM] Permissions-Policy: Falta de restricciones en el uso de APIs del navegador, dejando activos permisos potenciales para camara, microfono o geolocalizacion sin control.

[MEDIUM] Cookie ssl-caching (SameSite): La ausencia de este atributo hace que la cookie sea susceptible a ataques de falsificacion de peticion en sitios cruzados (CSRF).

[MEDIUM] Robots.txt: El archivo configurado bloquea el rastreo total del sitio con la directiva Disallow: /, lo cual impacta negativamente en la visibilidad y el SEO.

[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando informacion tecnica sobre la infraestructura que podria ser aprovechada por un atacante.

[LOW] Meta generator: El codigo fuente expone explicitamente el uso de Wix.com Website Builder como herramienta de creacion.