EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://colegiovirtualdechile.cl	Checks	9 pruebas
Dominio	colegiovirtualdechile.cl	Hallazgos	48 totales
Fecha	22 de abril de 2026 a las 00:48	Problemas	12 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio colegiovirtualdechile.cl arroja una puntuación de 73/100, lo que equivale a una calificación de grado C. Los resultados de los checks pasivos muestran que, de las 9 comprobaciones ejecutadas, 6 fueron satisfactorias, 1 generó una advertencia y 2 resultaron en fallos críticos de configuración. Si bien el sitio posee un cifrado de conexión válido, presenta deficiencias notables en la implementación de cabeceras de seguridad y exposición de información técnica sensible. En su estado actual, el sitio se considera vulnerable a ataques de clickjacking y reconocimiento de infraestructura por parte de terceros. Se requiere una intervención técnica para elevar los estándares de protección y mitigar riesgos potenciales.

Resumen de Riesgos

0	4	4	4	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 76 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 1.1.6 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
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 76 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  76 dias restantes (expira: 2026-07-07T08:06:02.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-08T08:06:03.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

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

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.0.30 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://colegiovirtualdechile.cl/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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: Site Kit by Google 1.168.0
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.0.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1.1.6 expuesta

- ALTO **WordPress version**
  Version 1.1.6 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)

- 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 — 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 (70 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, 580 URLs
- 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] Versión de WordPress expuesta: La versión 1.1.6 es visible públicamente, permitiendo a posibles atacantes identificar vulnerabilidades conocidas (CVEs) asociadas a esta versión antigua.
[HIGH] Falta de X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en frames externos, facilitando ataques de clickjacking.
[HIGH] Falta de Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, lo que deja a los usuarios expuestos a ataques de degradación de protocolo.
[MEDIUM] Falta de X-Content-Type-Options: El sitio es vulnerable al sniffing de tipos MIME, lo que podría permitir la ejecución de scripts maliciosos camuflados.
[MEDIUM] Falta de Referrer-Policy: No se controla la información de referencia enviada en las peticiones, pudiendo filtrar datos de navegación a otros dominios.
[MEDIUM] Falta de Permissions-Policy: No se restringen las APIs del navegador, como la cámara o el micrófono, aumentando la superficie de ataque en el cliente.
[MEDIUM] Panel de login accesible: La ruta /wp-login.php está disponible públicamente, facilitando intentos de acceso no autorizado mediante fuerza bruta.
[LOW] Cabecera Server expuesta: El servidor revela el uso de hcdn, proporcionando pistas sobre la infraestructura técnica utilizada.
[LOW] Cabecera X-Powered-By expuesta: Se expone el uso de PHP/8.0.30, facilitando la identificación de vectores de ataque específicos para esa tecnología.
[LOW] Meta generator expuesto: Se revela públicamente el uso de Site Kit by Google 1.168.0 en el código fuente.
[LOW] Ruta sensible en robots.txt: El archivo referencia directamente la palabra admin, lo que puede guiar a atacantes hacia directorios de gestión interna.