EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://copeval.cl/	Checks	9 pruebas
Dominio	copeval.cl	Hallazgos	68 totales
Fecha	3 de mayo de 2026 a las 21:42	Problemas	11 detectados

B

86/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio copeval.cl arroja una puntuación de 86/100 con una calificación de grado B. El análisis se basó en 9 verificaciones pasivas, de las cuales 6 resultaron satisfactorias, se emitieron 2 advertencias y se detectó 1 fallo crítico en la configuración de cabeceras. Aunque la capa de transporte y el cifrado son robustos, se identificaron debilidades importantes en la protección contra ataques de inyección y en la gestión de cookies de sesión. En su estado actual, el sitio se considera moderadamente seguro, pero presenta vulnerabilidades explotables que deben ser corregidas para garantizar la integridad de los datos de los usuarios.

Resumen de Riesgos

0	4	4	3	57
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 198 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
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	76	AVISO	SF-CSRF-TOKEN: falta HttpOnly; fornax_anonymousI...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 198 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  198 dias restantes (expira: 2026-11-17T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-12T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, 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
- INFO **X-Frame-Options**
  Presente: deny
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://copeval.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

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
- INFO **Tecnologias detectadas**
  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 — 76/100

Estado: AVISO

SF-CSRF-TOKEN: falta HttpOnly; fornax_anonymousId: falta HttpOnly; Shopper-Pref: falta SameSite; XSRF-TOKEN: falta HttpOnly; __cf_bm: falta SameSite

- INFO **Cookies detectadas**
  7 cookie(s) encontrada(s)
- ALTO **Cookie: SF-CSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: SF-CSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: SF-CSRF-TOKEN — SameSite**
  SameSite=strict
- ALTO **Cookie: fornax_anonymousId — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: fornax_anonymousId — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: fornax_anonymousId — SameSite**
  SameSite=none
- INFO **Cookie: athena_short_visit_id — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: athena_short_visit_id — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: athena_short_visit_id — SameSite**
  SameSite=none
- INFO **Cookie: Shopper-Pref — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: Shopper-Pref — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: Shopper-Pref — SameSite**
  Falta SameSite — Vulnerable a CSRF
- 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
- INFO **Cookie: SHOP_SESSION_TOKEN — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: SHOP_SESSION_TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: SHOP_SESSION_TOKEN — SameSite**
  SameSite=none
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __cf_bm — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1649 bytes)
- INFO **Reglas robots.txt**
  24 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS).
[HIGH] Cookies sin atributo HttpOnly (SF-CSRF-TOKEN, fornax_anonymousId, XSRF-TOKEN): Estas cookies son accesibles mediante scripts del navegador, lo que permite el robo de sesiones en caso de una vulnerabilidad XSS.
[MEDIUM] Falta de Referrer-Policy: No se controla la cantidad de información que el navegador envía al hacer clic en enlaces externos, lo que puede filtrar datos de navegación.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del navegador como la geolocalización o la cámara, aumentando la superficie de ataque.
[MEDIUM] Cookies sin atributo SameSite (Shopper-Pref, __cf_bm): La falta de esta directiva hace que el sitio sea más susceptible a ataques de falsificación de solicitudes entre sitios (CSRF).
[LOW] Ruta sensible expuesta en robots.txt: Se hace referencia directa a la ruta "admin", lo que facilita a atacantes la identificación de paneles de administración.
[LOW] Exposición de cabecera Server: La respuesta del servidor revela el uso de Cloudflare, proporcionando información técnica que ayuda en la fase de reconocimiento de un ataque.
[LOW] Ausencia de sitemap.xml: El archivo de mapa del sitio no fue encontrado, lo que dificulta la auditoría de rutas y la indexación controlada.