EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.conservadordelosangeles.cl/	Checks	9 pruebas
Dominio	www.conservadordelosangeles.cl	Hallazgos	45 totales
Fecha	25 de septiembre de 2026 a las 19:36	Problemas	15 detectados

D

47/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado ha otorgado al sitio una puntuación de 47/100, lo que se traduce en una calificación de grado D. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 4 resultaron exitosas, 1 presenta advertencias y 4 fallaron debido a configuraciones críticas de seguridad omitidas. Los resultados evidencian una carencia absoluta de cabeceras de protección y una gestión deficiente de las cookies de sesión. Se concluye que el sitio es actualmente vulnerable, ya que no implementa estándares básicos para mitigar ataques comunes y proteger la integridad de la navegación de sus usuarios.

Resumen de Riesgos

0	7	5	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 53 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 53 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  53 dias restantes (expira: 2026-11-18T01:07:46.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-20T01:07:47.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache — 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
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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

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 — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.google-analytics.com/urchin.js

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- 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] Redirección HTTPS ausente: El servidor permite conexiones vía HTTP sin redirigir al usuario automáticamente a una versión cifrada, exponiendo los datos a interceptaciones.

[HIGH] Falta de Strict-Transport-Security: No se comunica al navegador que debe usar siempre HTTPS, permitiendo ataques de degradación de conexión.
[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] Falta de X-Frame-Options: El sitio no cuenta con protección contra clickjacking, lo que permitiría a un atacante embeber la web en un marco malicioso.
[HIGH] Cookie PHPSESSID insegura (HttpOnly): La cookie de sesión es accesible mediante scripts del lado del cliente, elevando el riesgo de robo de identidad en caso de XSS.
[HIGH] Cookie PHPSESSID insegura (Secure): El identificador de sesión puede transmitirse por canales no cifrados, facilitando su captura en redes públicas.
[MEDIUM] Falta de X-Content-Type-Options: El navegador podría intentar adivinar el tipo de contenido de un archivo, lo que permite la ejecución de scripts camuflados.
[MEDIUM] Falta de SameSite en cookies: La ausencia de este atributo en la cookie de sesión hace que el sitio sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido mixto: Se detectó la carga de un recurso externo de Google Analytics mediante el protocolo inseguro HTTP en una página que debería ser totalmente cifrada.
[MEDIUM] Falta de Referrer-Policy y Permissions-Policy: No se limita la información de origen compartida con terceros ni se restringen los permisos de hardware del navegador.
[LOW] Cabecera de servidor expuesta: El servidor revela el uso de Apache, proporcionando información técnica que un atacante puede utilizar para buscar vulnerabilidades específicas de esa versión.
[LOW] Archivos de indexación faltantes: No se encontraron los archivos robots.txt ni sitemap.xml, lo que afecta la visibilidad y el control sobre el rastreo del sitio.