EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://broncesymetales.cl	Checks	9 pruebas
Dominio	broncesymetales.cl	Hallazgos	44 totales
Fecha	8 de mayo de 2026 a las 02:28	Problemas	10 detectados

C

63/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web determinó una puntuación de 63/100, lo que equivale a una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 6 resultados satisfactorios, 1 advertencia y 2 fallos críticos en la configuración del servidor. A pesar de contar con un cifrado de conexión válido, la ausencia de cabeceras de seguridad fundamentales y la falta de redirección forzada a HTTPS elevan el nivel de riesgo. En su estado actual, el sitio se considera vulnerable a ataques de intermediario y técnicas de inyección.

Resumen de Riesgos

0	5	3	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 54 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	100	OK	No se encontraron cookies
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 54 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  54 dias restantes (expira: 2026-07-01T04:28:31.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-02T04:28:32.000Z
- 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
- 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 — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (25 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- 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 no redirige el tráfico HTTP a HTTPS, permitiendo conexiones no cifradas propensas a intercepción.
[HIGH] Content-Security-Policy ausente: No existe una política que restrinja el origen de los recursos, facilitando ataques de Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options ausente: La falta de esta cabecera permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security (HSTS) ausente: El servidor no instruye al navegador para usar exclusivamente conexiones seguras en futuras visitas.

[MEDIUM] X-Content-Type-Options ausente: El navegador podría intentar interpretar archivos con tipos MIME incorrectos, permitiendo la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy ausente: No se controla la cantidad de información que el navegador envía al navegar desde este sitio hacia otros enlaces.
[MEDIUM] Permissions-Policy ausente: No se restringe el acceso a funciones sensibles del navegador como la cámara, micrófono o geolocalización.
[LOW] Server header expuesto: La cabecera revela el uso del servidor Apache, lo cual ayuda a un atacante a buscar vulnerabilidades específicas para esa tecnología.
[LOW] sitemap.xml ausente: No se encontró el archivo de mapa del sitio, lo cual es una advertencia de configuración menor pero relevante para la integridad del servicio.