EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://tunuevocomienzo.cl/	Checks	9 pruebas
Dominio	tunuevocomienzo.cl	Hallazgos	34 totales
Fecha	23 de marzo de 2026 a las 12:02	Problemas	3 detectados

B

87/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio tunuevocomienzo.cl arrojó una puntuación de 87/100, lo que equivale a una nota B. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron exitosos y 2 generaron advertencias críticas relacionadas con la configuración de cabeceras y contenido. No se detectaron fallos críticos totales, pero la exposición de la versión del CMS y la falta de políticas de seguridad modernas representan un riesgo latente. En conclusión, el sitio se considera mayoritariamente seguro, aunque es vulnerable a ataques de inyección y pérdida de integridad por contenido mixto.

Resumen de Riesgos

0	1	1	1	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 37 dias
Cabeceras de Seguridad	75	AVISO	5/6 presentes. Faltan: Content-Security-Policy
Deteccion CMS	100	OK	CMS detectado: WordPress
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 37 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  37 dias restantes (expira: 2026-04-29T14:52:17.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-29T14:52:18.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-Policy

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload

- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- INFO **Permissions-Policy**
  Presente: geolocation=(), microphone=(), camera=(), payment=(), usb=()

Deteccion CMS — 100/100

Estado: OK
CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.9.1
- INFO **Tecnologias detectadas**
  Next.js

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 — 60/100

Estado: AVISO
1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.maulestudio.com

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] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) e inyecciones de datos maliciosos.
[MEDIUM] Contenido Mixto: Se detectó un recurso stylesheet cargado mediante HTTP (http://www.maulestudio.com) dentro de una conexión HTTPS, lo que compromete el cifrado de la sesión.
[LOW] Meta generator: El sitio expone públicamente que utiliza WordPress 6.9.1, permitiendo a atacantes identificar vulnerabilidades específicas de esa versión.