EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://toyota.cl	Checks	9 pruebas
Dominio	toyota.cl	Hallazgos	58 totales
Fecha	8 de mayo de 2026 a las 20:00	Problemas	11 detectados

B

82/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad del sitio web arroja una puntuación exacta de 82/100, lo que corresponde a una calificación de nota B. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias, una presentó advertencias y una registró fallos críticos en la configuración. Aunque la infraestructura base muestra solidez, existen debilidades significativas en la implementación de cabeceras de respuesta y en la gestión de cookies de sesión. Actualmente, el sitio se considera mayoritariamente seguro, pero presenta vectores de riesgo que podrían ser aprovechados para ataques de inyección o interceptación de datos en tránsito. Es fundamental corregir las deficiencias detectadas para alcanzar un nivel de seguridad óptimo y proteger la integridad de los visitantes.

Resumen de Riesgos

0	8	3	0	47
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 78 dias
Cabeceras de Seguridad	40	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	67	AVISO	__uzma: falta Secure; __uzmb: falta Secure; __uz...
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	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 78 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  78 dias restantes (expira: 2026-07-25T15:32:34.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-26T15:32:35.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Permissions-Policy

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- INFO **X-Frame-Options**
  Presente: DENY
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

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)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 67/100

Estado: AVISO

__uzma: falta Secure; __uzmb: falta Secure; __uzme: falta Secure; __uzmc: falta Secure; __uzmd: falta Secure; csrftoken: falta HttpOnly

- INFO **Cookies detectadas**
  6 cookie(s) encontrada(s)
- INFO **Cookie: __uzma — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: __uzma — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: __uzma — SameSite**
  SameSite=lax
- INFO **Cookie: __uzmb — HttpOnly**
  HttpOnly activo — No accesible via JavaScript

- ALTO **Cookie: __uzmb — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: __uzmb — SameSite**
  SameSite=lax
- INFO **Cookie: __uzme — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: __uzme — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: __uzme — SameSite**
  SameSite=lax
- INFO **Cookie: __uzmc — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: __uzmc — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: __uzmc — SameSite**
  SameSite=lax
- INFO **Cookie: __uzmd — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: __uzmd — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: __uzmd — SameSite**
  SameSite=lax
- ALTO **Cookie: csrftoken — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: csrftoken — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: csrftoken — SameSite**
  SameSite=lax

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 (55 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://toyota.cl/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

1 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)**
  Cerrado — 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

[ALTA] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso por parte de terceros.
[ALTA] Strict-Transport-Security: La falta de HSTS no obliga al navegador a usar conexiones cifradas, permitiendo posibles ataques de degradación de protocolo.
[ALTA] Cookie csrftoken sin atributo HttpOnly: Esta omisión permite que la cookie sea accesible mediante scripts del lado del cliente, elevando el riesgo de robo de sesión en ataques XSS.
[ALTA] Cookies sin atributo Secure: Las cookies __uzma, __uzmb, __uzme, __uzmc y __uzmd carecen del flag Secure, lo que implica que pueden ser enviadas a través de conexiones HTTP no cifradas.
[MEDIA] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador, dejando expuestas funciones como la cámara, el micrófono o la geolocalización.
[MEDIA] Archivo /README.txt accesible: La exposición pública de este archivo puede revelar información técnica interna o detalles sobre la estructura del sistema.
[MEDIA] Panel de administración /administrator/ expuesto: La visibilidad de esta ruta facilita intentos de acceso no autorizado mediante ataques de fuerza bruta o diccionario.
[BAJA] Redirección HTTPS: No se ha podido verificar automáticamente si el tráfico entrante por el puerto 80 se redirige de forma forzada hacia el protocolo seguro.