EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://toyota.cl	Checks	9 pruebas
Dominio	toyota.cl	Hallazgos	59 totales
Fecha	17 de junio de 2026 a las 20:28	Problemas	11 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web obtuvo una puntuación de 88/100 con una nota final de B. Se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 2 generaron advertencias de seguridad. No se realizó un pentest activo, por lo que el alcance se limitó a la inspección de cabeceras, cookies y archivos expuestos. Aunque el núcleo de la infraestructura es sólido, el sitio se considera vulnerable a ataques de interceptación de datos y manipulación de sesiones debido a configuraciones de red y cookies incompletas.

Resumen de Riesgos

0	7	4	0	48
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 38 dias
Cabeceras de Seguridad	65	AVISO	4/6 presentes. Faltan: Strict-Transport-Security...
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 38 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  38 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 — 65/100

Estado: AVISO

4/6 presentes. Faltan: Strict-Transport-Security, Permissions-Policy

- INFO **Content-Security-Policy**
  Presente: connect-src 'self' analytics.google.com www.google-analytics.com *.googletagmana...

- 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 (225 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- 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

[HIGH] Strict-Transport-Security: La ausencia de esta cabecera impide forzar conexiones HTTPS, dejando a los usuarios expuestos a ataques de degradación de protocolo.
[HIGH] Cookies __uzma, __uzmb, __uzme, __uzmc, __uzmd sin flag Secure: Estas cookies se envían en conexiones HTTP no cifradas, permitiendo el robo de información en redes inseguras.
[HIGH] Cookie csrftoken sin flag HttpOnly: El acceso a esta cookie mediante scripts de navegador aumenta significativamente el riesgo de robo de identidad ante ataques XSS.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como cámara o micrófono, ampliando la superficie de ataque para scripts maliciosos.
[MEDIUM] Archivo /README.txt accesible: Este archivo se encuentra expuesto públicamente y puede contener información sobre la estructura o versiones del software utilizado.
[MEDIUM] Ruta /administrator/ expuesta: El panel de administración es accesible desde internet, lo que facilita intentos de acceso no autorizado mediante fuerza bruta.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea el rastreo de todo el sitio, lo cual puede indicar un error de configuración o un intento rudimentario de ocultar rutas.
[LOW] Redirección HTTPS no verificada: El escáner no pudo confirmar la redirección automática del tráfico inseguro hacia la versión cifrada del portal.