

EscanearVulnerabilidades

Informe de Seguridad Web

URL http://tomtunguz.com/
Dominio tomtunguz.com
Fecha 31 de julio de 2026 a las 03:11

Checks 9 pruebas
Hallazgos 46 totales
Problemas 11 detectados

C

70/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web arroja una puntuación de 70/100, lo que equivale a una calificación de grado C. Se completaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue clasificado como fallo crítico. Aunque la gestión de certificados es correcta, el sistema presenta deficiencias notables en la configuración de cabeceras de protección y exposición de puertos. En su estado actual, el sitio se considera vulnerable a ataques de intermediario (MitM) y técnicas de inyección debido a la ausencia de políticas de seguridad modernas.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 41 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 41 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
41 dias restantes (expira: 2026-09-09T18:46:00.000Z)
- INFO Fecha de emision
Emitido desde: 2026-06-11T17:46:05.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO Server header expuesto
Server: cloudflare — 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)
- INFO

X-Content-Type-Options
Presente: nosniiff
- MEDIO

Referrer-Policy
Falta — Controla la informacion de referer enviada
- MEDIO

Permissions-Policy
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://tomtunguz.com/
- 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
- BAJO

Meta generator
Expone: Hugo 0.154.5
- INFO

Tecnologias detectadas
React, 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 — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO

Protocolo
El sitio no usa HTTPS

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt
Presente (612 bytes)
- INFO

Reglas robots.txt
2 Disallow, 12 Allow
- MEDIO

Bloqueo total
robots.txt bloquea todo el sitio con Disallow: /
- INFO

Sitemap en robots.txt
https://www.tomtunguz.com/sitemap.xml
- BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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)
Abierto (esperado) — 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
- MEDIO

Puerto 8080 (HTTP-Alt)
ABIERTO — Servidor web alternativo / proxy
- INFO

Puerto 27017 (MongoDB)
Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de datos.

[HIGH] X-Frame-Options: Falta de protección contra ataques de clickjacking que podrían engañar a los usuarios.

[HIGH] Strict-Transport-Security: La falta de HSTS permite que las conexiones puedan ser degradadas de HTTPS a HTTP.

[HIGH] Protocolo HTTPS: El sitio presenta inconsistencias en el uso de HTTPS por defecto según el análisis de contenido mixto.

[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó el puerto abierto, lo cual puede exponer servicios administrativos o proxies no protegidos.

[MEDIUM] Referrer-Policy: No se define el control de información de referencia enviada a terceros.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como cámara o micrófono.

[MEDIUM] Bloqueo en robots.txt: El archivo bloquea la indexación de todo el sitio, lo que sugiere una configuración de visibilidad errónea.

[LOW] Server header expuesto: Se revela el uso de Cloudflare, facilitando el reconocimiento para posibles atacantes.

[LOW] Meta generator expuesto: Se detectó el uso de Hugo 0.154.5, lo que permite identificar vulnerabilidades específicas de esa versión.