EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://tenttation.com/	Checks	9 pruebas
Dominio	tenttation.com	Hallazgos	49 totales
Fecha	22 de mayo de 2026 a las 18:49	Problemas	13 detectados

C

66/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 66/100, lo que equivale a una calificación de C. Se ejecutaron un total de 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 4 generaron advertencias y 2 fallaron debido a configuraciones críticas de seguridad. El análisis revela una infraestructura con servicios obsoletos expuestos y una carencia severa de cabeceras de protección modernas. Aunque la conexión inicial está cifrada, la presencia de versiones de software antiguas y puertos inseguros permite concluir que el sitio es vulnerable a ataques dirigidos. Es imperativo corregir las deficiencias técnicas para evitar posibles brechas de datos o toma de control del servidor.

Resumen de Riesgos

0	5	5	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 68 dias
Cabeceras de Seguridad	40	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: Joomla, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 3.7.1 expuesta, WordPress 2 expuesta
Seguridad de Cookies	67	AVISO	fd2237b40027014680eda93b5d0a1977: falta SameSite
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 68 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  68 dias restantes (expira: 2026-07-30T02:35:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-01T02:36:00.000Z
- 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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.30 — Revela framework/lenguaje

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://tenttation.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

CMS detectado: Joomla, PrestaShop

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  Detectado via HTML body
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Joomla! - Open Source Content Management
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.2.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 3.7.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 3.7.1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

Seguridad de Cookies — 67/100

Estado: AVISO

fd2237b40027014680eda93b5d0a1977: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: fd2237b40027014680eda93b5d0a1977 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: fd2237b40027014680eda93b5d0a1977 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: fd2237b40027014680eda93b5d0a1977 — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (764 bytes)
- INFO **Reglas robots.txt**
  16 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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

- 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] Puerto 21 (FTP): El puerto está abierto permitiendo la transferencia de archivos sin cifrar, lo que expone credenciales y datos a interceptación.
[HIGH] Version CMS Expuesta: Se detectó la exposición de WordPress 3.7.1 y WordPress 2, lo que facilita a atacantes la búsqueda de CVEs conocidos para comprometer el sitio.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] Strict-Transport-Security: No se detectó la configuración HSTS, lo que impide que el navegador fuerce conexiones HTTPS seguras en todo momento.
[MEDIUM] Cookie SameSite: Las cookies de sesión carecen del atributo SameSite, dejando la plataforma vulnerable a ataques de falsificación de peticiones en sitios cruzados (CSRF).
[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, revelando detalles técnicos innecesarios sobre el sistema.
[MEDIUM] Ruta /administrator/ accesible: El panel de gestión de Joomla es visible para cualquier usuario, aumentando el riesgo de ataques de fuerza bruta.
[MEDIUM] Permissions-Policy: Falta esta cabecera para restringir el uso de APIs del navegador como la cámara o el micrófono, afectando la privacidad del usuario.
[LOW] X-Powered-By expuesto: La cabecera revela el uso de PHP/8.2.30, proporcionando información valiosa a los atacantes para perfilar el entorno de ejecución.
[LOW] Meta generator: La etiqueta meta expone el uso de Joomla! como gestor de contenidos, facilitando el reconocimiento de la plataforma por parte de terceros.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a la ruta "admin", lo que orienta a posibles atacantes hacia directorios sensibles del servidor.