EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.trota.com	Checks	9 pruebas
Dominio	www.trota.com	Hallazgos	47 totales
Fecha	23 de julio de 2026 a las 12:22	Problemas	14 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación técnica de 62/100, lo que se traduce en una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 fueron marcados como fallos críticos. No se llevó a cabo un pentest activo, por lo que el informe se basa en la configuración externa y cabeceras detectadas. Debido a la presencia de software desactualizado y la ausencia de protecciones esenciales contra ataques comunes, el sitio se considera vulnerable.

Resumen de Riesgos

0	5	6	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 224 dias
Cabeceras de Seguridad	10	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 5.1.22 expuesta, WordPress 2.7 expuest...
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 224 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  224 dias restantes (expira: 2027-03-04T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-04T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 10/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: Apache/2.4.58 (Ubuntu) — 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)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- 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://www.trota.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: 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 5.1.22
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 5.1.22 expuesta, WordPress 2.7 expuesta

- ALTO **WordPress version**
  Version 5.1.22 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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://app.trota.com/

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (67 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, ? URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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] WordPress versión 5.1.22 expuesta: El uso de una versión obsoleta permite a atacantes explotar vulnerabilidades conocidas (CVEs) para tomar el control del sitio.
[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques XSS y la inyección de contenido malicioso.
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking, donde un tercero puede secuestrar los clics del usuario en marcos invisibles.
[HIGH] Falta de Strict-Transport-Security: No se fuerza el uso de conexiones seguras mediante HSTS, permitiendo ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que el navegador realice MIME-sniffing, aumentando el riesgo de ejecución de scripts ocultos.
[MEDIUM] Recurso HTTP (Contenido Mixto): Se carga el recurso http://app.trota.com/ bajo una conexión segura, lo que debilita la integridad de la sesión HTTPS.
[MEDIUM] Puerto 22 (SSH) abierto: La exposición pública de este puerto de administración remota incrementa el riesgo de intentos de intrusión por fuerza bruta.
[MEDIUM] Ruta /wp-login.php y archivo /readme.html accesibles: Estos elementos facilitan la identificación del panel de control y revelan detalles técnicos internos.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador como la geolocalización o la cámara.
[LOW] Server header expuesto: La cabecera revela el uso de Apache/2.4.58 (Ubuntu), orientando a posibles atacantes sobre las debilidades de la infraestructura.
[LOW] Ruta sensible en robots.txt: La mención directa a directorios de administración ayuda a mapear la estructura interna del servidor.