EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://mrttool.com/	Checks	9 pruebas
Dominio	mrttool.com	Hallazgos	44 totales
Fecha	28 de mayo de 2026 a las 19:30	Problemas	10 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada a mrttool.com ha arrojado una puntuación exacta de 61/100, lo que corresponde a una nota C. El análisis se basó en 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 generó una advertencia y 3 mostraron fallos críticos en la configuración. Aunque el cifrado de datos es correcto, se han detectado debilidades importantes en la protección contra ataques de inyección y en la gestión del tráfico seguro. Debido a la falta de redirección automática a HTTPS y la ausencia de cabeceras de seguridad fundamentales, el sitio se considera vulnerable ante ataques web comunes.

Resumen de Riesgos

0	3	4	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 51 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 51 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  51 dias restantes (expira: 2026-07-18T17:55:42.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-19T17:55:43.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: nginx — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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

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 — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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] HTTP a HTTPS redirección: El sitio no redirige automáticamente el tráfico no cifrado a una conexión segura, permitiendo el acceso mediante HTTP (puerto 80).
[HIGH] Content-Security-Policy (CSP) ausente: La falta de esta cabecera facilita la ejecución de ataques XSS y la inyección de contenido malicioso en el navegador del usuario.

[HIGH] X-Frame-Options ausente: El sitio no implementa protección contra clickjacking, lo que permitiría a un atacante embeber la web en un marco invisible para engañar a los visitantes.
[MEDIUM] Puerto 22 (SSH) abierto: El acceso remoto por SSH está expuesto públicamente, lo que aumenta la superficie de ataque y el riesgo de intentos de acceso no autorizados.
[MEDIUM] X-Content-Type-Options ausente: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría llevar a la ejecución de archivos con contenido malicioso.
[MEDIUM] Referrer-Policy ausente: No se controla qué información de origen se envía cuando un usuario navega desde el sitio hacia enlaces externos.
[MEDIUM] Permissions-Policy ausente: El sitio no restringe el uso de APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: La cabecera revela el uso de nginx, proporcionando información técnica que ayuda a potenciales atacantes a identificar vulnerabilidades específicas del software.
[LOW] Ausencia de robots.txt y sitemap.xml: No se encontraron estos archivos de configuración, lo que dificulta la indexación correcta y el control del rastreo por motores de búsqueda.