EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.trencalos-team.org/contacte/	Checks	9 pruebas
Dominio	www.trencalos-team.org	Hallazgos	52 totales
Fecha	10 de agosto de 2026 a las 16:09	Problemas	14 detectados

D

54/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha resultado en una puntuación de 54/100, lo que otorga una calificación de grado D. Se han ejecutado un total de 9 verificaciones pasivas, de las cuales 4 resultaron exitosas, 2 generaron advertencias y 3 fueron fallos críticos. La evaluación técnica revela que, aunque el cifrado SSL es correcto, existen deficiencias graves en la protección contra ataques comunes y el mantenimiento del software base. Debido a la exposición de versiones obsoletas y la falta de cabeceras de seguridad esenciales, se concluye que el sitio es actualmente vulnerable. Es necesaria una intervención técnica inmediata para elevar los estándares de protección y mitigar riesgos de intrusión.

Resumen de Riesgos

0	5	6	3	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 52 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	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 4.13.8 expuesta, WordPress 2 expuesta
Seguridad de Cookies	67	AVISO	pll_language: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
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 52 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  52 dias restantes (expira: 2026-10-01T19:59:38.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-03T19:01:10.000Z
- 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: 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- 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; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS 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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- 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: Elementor 4.2.2; settings: css_print_method-external, google_font-enabled, font_display-swap
- INFO **Tecnologias detectadas**
  Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 4.13.8 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 4.13.8 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 — 67/100

Estado: AVISO

pll_language: falta HttpOnly

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: pll_language — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: pll_language — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: pll_language — 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 (123 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 en robots.txt**
  https://www.trencalos-team.org/wp-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] WordPress versión expuesta: Se detectó la versión 4.13.8 y referencias a la versión 2, lo cual es peligroso porque permite a los atacantes identificar y explotar vulnerabilidades conocidas (CVEs) para tomar el control del sitio.
[HIGH] Falta de redirección HTTPS: El servidor no redirige automáticamente el tráfico HTTP a HTTPS, permitiendo conexiones no cifradas donde los datos de los usuarios pueden ser interceptados.
[HIGH] Content-Security-Policy (CSP) faltante: La ausencia de esta cabecera facilita la ejecución de ataques de inyección de contenido y Cross-Site Scripting (XSS) al no restringir las fuentes de scripts permitidas.
[HIGH] X-Frame-Options faltante: El sitio es vulnerable a ataques de clickjacking, ya que no impide que la página sea cargada dentro de marcos (iframes) en sitios de terceros malintencionados.
[HIGH] Cookie pll_language sin atributo HttpOnly: Al carecer de esta protección, la cookie es accesible mediante scripts del navegador, lo que aumenta significativamente el riesgo de robo de sesión en caso de un ataque XSS.
[MEDIUM] X-Content-Type-Options faltante: Sin esta cabecera, los navegadores pueden intentar adivinar el tipo de contenido, permitiendo que archivos maliciosos sean ejecutados como scripts legítimos (MIME-sniffing).
[MEDIUM] Referrer-Policy faltante: No existe un control sobre la información de navegación que se envía a otros sitios cuando el usuario hace clic en un enlace externo.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el acceso a funciones sensibles del hardware del usuario, como la cámara o el micrófono, a través de APIs del navegador.
[MEDIUM] Archivo /readme.html y /wp-login.php expuestos: Estos archivos y rutas públicas facilitan el reconocimiento técnico del sistema y exponen el panel de administración a ataques de fuerza bruta.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de este puerto abierto sugiere la existencia de un servidor alternativo o proxy que podría no estar debidamente protegido.
[LOW] Cabecera de servidor expuesta: El valor Server: cloudflare revela detalles de la infraestructura tecnológica, ayudando a los atacantes a perfilar mejor sus objetivos.
[LOW] Meta generator expuesto: El sitio revela el uso de Elementor 4.2.2 y sus configuraciones internas, proporcionando información técnica innecesaria a terceros.
[LOW] Ruta sensible en robots.txt: El archivo de indexación contiene referencias a directorios administrativos, lo que ayuda a los atacantes a mapear áreas privadas del servidor.