EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ctrento.net/	Checks	9 pruebas
Dominio	ctrento.net	Hallazgos	44 totales
Fecha	16 de junio de 2026 a las 15:39	Problemas	12 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación técnica de 61/100, lo que equivale a una calificación de grado C. Se ejecutaron un total de 9 verificaciones pasivas, de las cuales 6 resultaron satisfactorias y 3 presentaron fallos críticos de configuración. Aunque el cifrado de datos es robusto, la ausencia total de cabeceras de protección y la falta de redirección segura debilitan la postura defensiva. En su estado actual, el sitio se considera vulnerable ante ataques de manipulación de tráfico y suplantación de identidad. Es imperativo aplicar las correcciones recomendadas para alcanzar un nivel de seguridad aceptable.

Resumen de Riesgos

0	5	3	4	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 109 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 109 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  109 dias restantes (expira: 2026-10-03T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-03T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- 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
- 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
- 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
- INFO **Tecnologias detectadas**
  ASP.NET

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 — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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] Falta de redirección HTTP a HTTPS: El servidor responde a peticiones no cifradas sin redirigirlas, permitiendo el acceso por canales inseguros.
[HIGH] Ausencia de Strict-Transport-Security: Sin la cabecera HSTS, el navegador no está obligado a mantener una conexión segura, facilitando ataques de interceptación.

[HIGH] Ausencia de Content-Security-Policy: No existe control sobre los recursos que el navegador puede cargar, lo que permite ataques de Cross-Site Scripting (XSS).
[HIGH] Ausencia de X-Frame-Options: El sitio es susceptible de ser embebido en marcos externos, facilitando ataques de Clickjacking para engañar al usuario.
[MEDIUM] Ausencia de X-Content-Type-Options: El navegador podría intentar interpretar archivos con tipos MIME incorrectos, derivando en la ejecución de scripts maliciosos.
[MEDIUM] Ausencia de Referrer-Policy: No se controla la información de navegación que se envía a terceros al seguir enlaces externos.
[MEDIUM] Ausencia de Permissions-Policy: No se restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[LOW] Exposición de cabecera Server: El servidor revela el uso de Microsoft-IIS/10.0, lo cual facilita la búsqueda de exploits específicos para esa versión.
[LOW] Exposición de cabecera X-Powered-By: Se expone el uso del framework ASP.NET, proporcionando información técnica valiosa para un atacante.
[LOW] Ausencia de archivos de control: No se encontraron los archivos robots.txt ni sitemap.xml, lo que afecta la visibilidad y el control del rastreo web.