EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://frankprocleaner.ca	Checks	9 pruebas
Dominio	frankprocleaner.ca	Hallazgos	47 totales
Fecha	15 de agosto de 2026 a las 02:24	Problemas	16 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 53/100, lo que corresponde a una calificación de grado D. Se ejecutaron 9 checks pasivos, resultando en 5 verificaciones correctas, 1 advertencia y 3 fallos críticos en la configuración de seguridad. A pesar de contar con un certificado SSL válido, la carencia de cabeceras de protección y la exposición de puertos críticos comprometen la integridad de la plataforma. Por lo tanto, se concluye que el sitio es actualmente vulnerable ante ataques dirigidos y automatizados.

Resumen de Riesgos

1	7	5	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 46 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	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.0.3 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
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	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 46 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  46 dias restantes (expira: 2026-09-29T22:53:37.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-01T22:53:38.000Z
- 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: LiteSpeed — 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
- 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

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: WordPress 7.0.3
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0.3 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0.3 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 — 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 (163 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://frankprocleaner.ca/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos está expuesta a internet, permitiendo intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP) abierto: Este servicio transmite datos y credenciales en texto plano, facilitando la interceptación de información sensible.
[HIGH] Ausencia de redirección HTTPS: El sitio permite conexiones inseguras a través de HTTP sin forzar el cifrado de los datos.
[HIGH] Falta de Strict-Transport-Security (HSTS): El navegador no recibe la instrucción de usar exclusivamente conexiones seguras.
[HIGH] Content-Security-Policy (CSP) ausente: El sitio no cuenta con protección contra ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options faltante: La página es susceptible a ataques de clickjacking que pueden engañar a los usuarios.
[HIGH] Exposición de versión WordPress 7.0.3: Publicar la versión exacta del CMS permite a los atacantes buscar exploits específicos.
[MEDIUM] X-Content-Type-Options ausente: No se previene el sniffing de tipos MIME por parte del navegador.
[MEDIUM] Referrer-Policy faltante: No se controla la cantidad de información enviada al navegar hacia enlaces externos.
[MEDIUM] Archivo readme.html y ruta wp-login expuestos: Revelan información técnica del sistema y exponen el punto de entrada administrativo.
[LOW] Cabecera Server expuesta: Se revela el uso del servidor LiteSpeed, facilitando la fase de reconocimiento del atacante.
[LOW] Rutas sensibles en robots.txt: Se menciona la ruta de administración, guiando a posibles atacantes hacia directorios privados.