EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.thebeartrapsreport.com	Checks	9 pruebas
Dominio	www.thebeartrapsreport.com	Hallazgos	45 totales
Fecha	12 de mayo de 2026 a las 15:19	Problemas	11 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web https://www.thebeartrapsreport.com ha dado como resultado una puntuación de 81/100, lo que equivale a una nota B. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue identificado como fallo crítico. No se detectó un CMS específico, aunque la infraestructura cuenta con medidas de protección perimetral activas. En su estado actual, el sitio se considera moderadamente seguro, pero presenta vulnerabilidades de configuración técnica que deben ser subsanadas para evitar riesgos de interceptación de datos.

Resumen de Riesgos

0	2	8	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 53 dias
Cabeceras de Seguridad	55	FALLO	Solo 3/6 presentes. Faltan: Strict-Transport-Sec...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 53 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  53 dias restantes (expira: 2026-07-04T08:50:57.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-05T08:50:57.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Sucuri/Cloudproxy — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests;
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- 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.thebeartrapsreport.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

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**
  React, Next.js, Astro

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.lawrencegmcdonald.com

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
  Presente, 77 URLs
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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

[ALTA] Strict-Transport-Security (HSTS): Falta la cabecera HSTS, lo que impide que el navegador fuerce conexiones HTTPS automáticas, facilitando ataques de degradación de SSL.

[MEDIA] Referrer-Policy: Esta cabecera no está configurada, lo que impide controlar qué información de origen se envía a otros dominios durante la navegación.
[MEDIA] Permissions-Policy: Ausencia de restricciones para APIs del navegador, lo que permite potencialmente el acceso no autorizado a funciones como la cámara, micrófono o geolocalización.
[MEDIA] Contenido Mixto: Se detectó un recurso (http://www.lawrencegmcdonald.com) cargado mediante HTTP dentro de la página protegida por HTTPS, lo que debilita el cifrado general.
[MEDIA] Rutas administrativas expuestas: Se identificaron paneles de login accesibles en /wp-login.php, /administrator/ y /user/login, aumentando el riesgo de ataques de fuerza bruta.
[MEDIA] Archivos de información expuestos: Los archivos /readme.html y /README.txt son públicos, lo que puede revelar detalles técnicos sobre la configuración interna del sitio.
[WARN] Ausencia de Robots.txt: El sitio no cuenta con un archivo robots.txt, lo que dificulta la gestión de la indexación por parte de los motores de búsqueda.
[BAJA] Server Header expuesto: El servidor revela el uso de Sucuri/Cloudproxy, proporcionando información valiosa a un atacante sobre la tecnología de defensa empleada.