EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://danimefle.com/	Checks	9 pruebas
Dominio	danimefle.com	Hallazgos	44 totales
Fecha	3 de junio de 2026 a las 16:13	Problemas	12 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web danimefle.com ha arrojado una puntuación de 59/100, lo que equivale a una calificación de nota D. El análisis se basó en la ejecución de 9 checks pasivos, resultando en 5 verificaciones correctas, 2 advertencias y 2 fallos críticos. Se han detectado carencias estructurales en la implementación de cabeceras de seguridad y en el forzado de conexiones cifradas. Debido a la falta de políticas de protección básicas y la exposición de puertos innecesarios, se concluye que el sitio es actualmente vulnerable ante ataques dirigidos.

Resumen de Riesgos

0	5	5	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  90 dias restantes (expira: 2026-09-01T14:26:09.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-03T13:27:46.000Z
- 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: 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
- 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

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1738 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- 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): 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] Content-Security-Policy: Falta — La ausencia de esta política facilita ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Falta — El sitio no previene el clickjacking, permitiendo que la interfaz sea cargada dentro de marcos no autorizados.
[HIGH] Strict-Transport-Security: Falta — No se obliga al navegador a usar conexiones HTTPS, permitiendo ataques de degradación de protocolo.
[HIGH] Redirección HTTP a HTTPS inexistente: El servidor responde con éxito (HTTP 200) a peticiones no cifradas, exponiendo los datos en tránsito.

[MEDIUM] X-Content-Type-Options: Falta — La falta de esta directiva permite el sniffing de tipos MIME, lo que puede derivar en la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: Falta — No hay control sobre la información de referencia que se envía a otros sitios, comprometiendo la privacidad de los usuarios.
[MEDIUM] Permissions-Policy: Falta — No se restringe el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Puerto 8080 (HTTP-Alt) ABIERTO: La exposición de un puerto de servidor alternativo o proxy aumenta la superficie de ataque.
[MEDIUM] Configuración de robots.txt: Se bloquea la indexación de todo el sitio con Disallow: /, lo cual es una práctica de visibilidad inusual y restrictiva.
[LOW] Server header expuesto: Se revela el uso de Cloudflare, proporcionando información técnica que ayuda a un atacante en la fase de reconocimiento.
[LOW] sitemap.xml no encontrado: La ausencia de este archivo dificulta la auditoría de la estructura del sitio y la gestión de contenidos.