EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://logiqd.me/	Checks	9 pruebas
Dominio	logiqd.me	Hallazgos	48 totales
Fecha	5 de mayo de 2026 a las 17:08	Problemas	5 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 81/100, lo que corresponde a una calificación de grado B. Durante el proceso se ejecutaron 9 verificaciones pasivas, de las cuales 7 resultaron satisfactorias, 1 generó una advertencia y 1 se marcó como fallo crítico. Aunque el sitio presenta una excelente implementación de cabeceras de seguridad y cifrado, la ausencia de una redirección forzada al protocolo seguro compromete la integridad de la conexión. No se ejecutó un pentest activo, por lo que los hallazgos se limitan a la configuración expuesta y de red. En conclusión, el sitio se considera moderadamente seguro, pero es vulnerable a ataques de interceptación de tráfico y reconocimiento de infraestructura.

Resumen de Riesgos

0	1	1	3	43
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 85 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	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 85 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  85 dias restantes (expira: 2026-07-29T07:20:53.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-30T07:20:54.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; base-uri 'self'; object-src 'none'; frame-ancestors 'none'; ...
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: camera=(), microphone=(), geolocation=(), payment=(), usb=(), interest-cohort=()

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; preload
- 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

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
- BAJO **Meta generator**
  Expone: Astro v5.18.1
- INFO **Tecnologias detectadas**
  Astro

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (968 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 17 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://logiqd.me/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] Falta de redirección HTTPS: El servidor no redirige automáticamente las peticiones HTTP a HTTPS (responde con código 200), lo que permite conexiones no cifradas y facilita ataques de intermediario (MitM).
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo sugiere la presencia de un servidor web secundario o una interfaz de administración que podría ser blanco de ataques dirigidos.
[LOW] Exposición de cabecera Server: El servidor revela el uso de Cloudflare, proporcionando información valiosa a un atacante sobre el proveedor de infraestructura de borde.
[LOW] Divulgación de versión en Meta generator: El sitio expone el uso de Astro v5.18.1, lo cual permite a un atacante buscar vulnerabilidades específicas asociadas a dicha versión del framework.
[LOW] Ruta sensible en robots.txt: Se ha detectado una referencia directa a la ruta admin, lo que facilita el descubrimiento de directorios de gestión internos por parte de agentes maliciosos.