

Escanear Vulnerabilidades

Informe de Seguridad Web

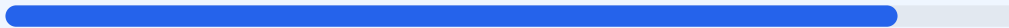
URL https://kilaritys.com
Dominio kilaritys.com
Fecha 11 de mayo de 2026 a las 14:49

Checks 9 pruebas
Hallazgos 45 totales
Problemas 6 detectados

B

88/100

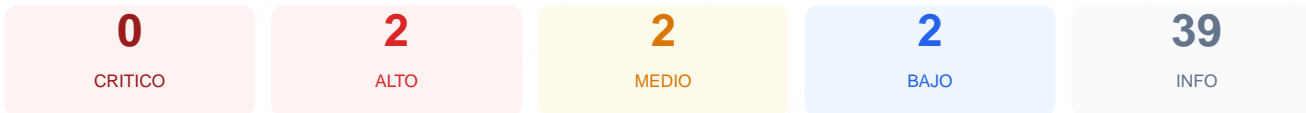
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio kilaritys.com arroja una puntuación de 88/100 con una calificación final de nota B. Se ejecutaron 9 checks pasivos, resultando en 6 verificaciones exitosas y 3 advertencias importantes por corregir. No se detectaron fallos críticos directos, aunque la ausencia de ciertas políticas de transporte estricto y la exposición de puertos alternativos elevan el riesgo residual. Se concluye que el sitio es generalmente seguro para el usuario final, pero presenta vulnerabilidades de configuración que deben ser mitigadas para prevenir ataques de reconocimiento o interceptación.

Resumen de Riesgos



Resumen de Checks

| | | | |
|------------------------|-----|-------|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 89 dias |
| Cabeceras de Seguridad | 80 | AVISO | 5/6 presentes. Faltan: Strict-Transport-Security |
| 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 | 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 89 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
89 dias restantes (expira: 2026-08-08T21:28:54.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-05-10T21:28:55.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

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

- INFO **Content-Security-Policy**
Presente: default-src 'none'; script-src 'nonce-iqnpaxyxOIQeHDdgZtr7Uh' 'unsafe-eval' http...
- INFO **X-Frame-Options**
Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
Presente: nosniiff
- INFO **Referrer-Policy**
Presente: same-origin
- INFO **Permissions-Policy**
Presente: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://kilaritys.com/
- ALTO **HSTS (Strict-Transport-Security)**
HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
HTTPS responde con status 403

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
Presente (2176 bytes)
- INFO **Reglas robots.txt**
16 Disallow, 2 Allow
- MEDIO **Bloqueo total**
robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
http://kiliarys.com/sitemap_index.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] Strict-Transport-Security: La cabecera HSTS no está configurada, lo que impide que el navegador fuerce siempre una conexión cifrada y permite ataques de degradación de protocolo.

[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó el puerto 8080 abierto, lo cual indica la presencia de un servidor web alternativo o proxy que aumenta la superficie de ataque.

[MEDIUM] Bloqueo total y rutas sensibles en robots.txt: El archivo bloquea la indexación de todo el sitio y referencia la ruta admin, facilitando a posibles atacantes el descubrimiento de directorios de gestión.

[LOW] Server header expuesto: La cabecera de respuesta revela el uso de Cloudflare, proporcionando información sobre la infraestructura tecnológica que podría ser aprovechada en ataques dirigidos.

[INFO] Respuesta HTTPS 403: El servidor responde con un código de prohibido al intentar acceder vía HTTPS directamente, lo que sugiere una configuración de permisos restrictiva que debe ser revisada.