

Escanear Vulnerabilidades

Informe de Seguridad Web

URL <https://impact-sprint-hub.lovable.app>
Dominio impact-sprint-hub.lovable.app
Fecha 20 de mayo de 2026 a las 16:49

Checks 9 pruebas
Hallazgos 47 totales
Problemas 7 detectados

B

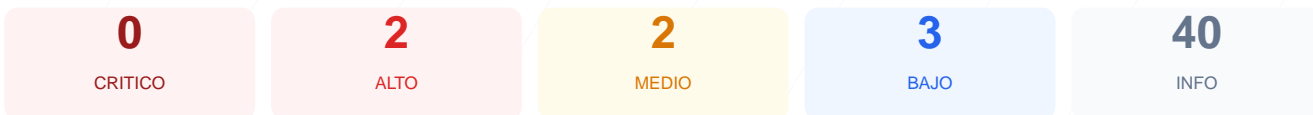
81/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a la plataforma arroja una puntuación exacta de 81/100, lo que le otorga una calificación de grado B. De los 9 checks pasivos ejecutados, 6 resultaron satisfactorios, mientras que se identificaron 1 advertencia y 2 fallos en la configuración de cabeceras y archivos del sistema. Aunque el cifrado SSL y la gestión de cookies son correctos, la ausencia de políticas de seguridad de contenido y la exposición de un puerto alternativo representan un riesgo moderado. En conclusión, el sitio web cuenta con una base de seguridad sólida pero se considera vulnerable ante ataques de inyección y suplantación de interfaz por falta de endurecimiento en sus configuraciones.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 56 dias
Cabeceras de Seguridad	45	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	1 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 56 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
56 dias restantes (expira: 2026-07-15T18:48:10.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-16T17:48:26.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, 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
- **INFO** **Strict-Transport-Security**
Presente: max-age=31536000; includeSubDomains
- **INFO** **X-Content-Type-Options**
Presente: nosniiff
- **INFO** **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- **MEDIO** **Permissions-Policy**
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://impact-sprint-hub.lovable.app/
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000; includeSubDomains
- **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

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

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
SameSite=none

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
No encontrado (HTTP 404)
- 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 cabecera que previene ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.

[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea embebido en otros dominios, facilitando ataques de clickjacking.

[MEDIUM] Permissions-Policy: No se restringe el uso de APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.

[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto y expone un servidor web alternativo o proxy que puede ser explotado como vector de entrada.

[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando información técnica innecesaria a posibles atacantes.

[LOW] robots.txt: El archivo no fue encontrado, lo que impide gestionar correctamente qué partes del sitio deben ser rastreadas por buscadores.

[LOW] sitemap.xml: La falta de este archivo dificulta el análisis de la estructura del sitio y su correcta indexación.