

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://OrbixPay.lovable.app	Checks	9 pruebas
Dominio	orbixpay.lovable.app	Hallazgos	49 totales
Fecha	8 de agosto de 2026 a las 14:22	Problemas	3 detectados

A

94/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre OrbixPay.lovable.app arrojó una puntuación de 94/100, lo que otorga al sitio una calificación de Grado A. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 7 validaciones exitosas, 2 advertencias menores y ningún fallo crítico. No se detectaron brechas de seguridad que comprometan la integridad de los datos de forma inmediata. Se concluye que el sitio web es altamente seguro, aunque requiere ajustes específicos en la configuración de puertos y metadatos del servidor. La implementación de protocolos de cifrado y cabeceras de seguridad es sobresaliente.

Resumen de Riesgos

0 CRITICO	0 ALTO	1 MEDIO	2 BAJO	46 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 35 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	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 35 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
35 dias restantes (expira: 2026-09-12T20:53:58.000Z)
- INFO Fecha de emision
Emitido desde: 2026-06-14T19:54:11.000Z
- 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
- 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=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://orbixpay.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
- INFO

Tecnologias detectadas
React

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 — 60/100

Estado: AVISO

Falta sitemap.xml

INFO

robots.txt

Presente (39 bytes)

INFO

Reglas robots.txt

1 Disallow, 1 Allow

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

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un servidor web alternativo o proxy puede ser aprovechada para intentar accesos no autorizados a servicios internos.

[LOW] Server header expuesto: El encabezado revela el uso de Cloudflare, lo cual facilita información técnica a posibles atacantes durante la fase de reconocimiento.

[LOW] Ausencia de sitemap.xml: El archivo no fue localizado, lo que impide una correcta visibilidad de la estructura del sitio y afecta la transparencia de la plataforma.