

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://web-production-dead5.up.railway.app/	Checks	9 pruebas
Dominio	web-production-dead5.up.railway.app	Hallazgos	42 totales
Fecha	2 de octubre de 2026 a las 18:44	Problemas	10 detectados

C

72/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web-production-dead5.up.railway.app ha dado como resultado una puntuación de 72/100, lo que corresponde a una nota de C. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 terminaron en fallo crítico. Aunque el cifrado de datos es correcto, la ausencia total de cabeceras de seguridad representa un riesgo significativo. En su estado actual, el sitio se considera vulnerable a ataques de inyección y suplantación debido a la falta de protecciones en la configuración del servidor.

Resumen de Riesgos

0 CRITICO	4 ALTO	3 MEDIO	3 BAJO	32 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 84 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
84 dias restantes (expira: 2026-12-26T03:01:42.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-27T03:01:43.000Z
- 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: railway-hikari — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://web-production-dead5.up.railway.app/
- ALTO

HSTS (Strict-Transport-Security)
HSTS no configurado — El navegador no fuerza HTTPS
- INFO

Respuesta HTTPS
HTTPS responde con status 429

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 — 20/100

Estado: FALLO
Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
No encontrado (HTTP 429)
- BAJO **sitemap.xml**
No encontrado (HTTP 429)
- BAJO **security.txt**
No encontrado — Recomendado para política de divulgacion

Puertos Abiertos — 100/100

Estado: OK
2 puerto(s) abierto(s), todos esperados

- 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
- INFO **Puerto 8080 (HTTP-Alt)**
Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: Falta esta cabecera esencial, lo que permite la ejecución de ataques XSS y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de esta directiva deja al sitio desprotegido contra ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se utiliza HSTS, lo que impide que el navegador fuerce conexiones HTTPS y permite ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría interpretar archivos de forma incorrecta mediante MIME-type sniffing.
[MEDIUM] Referrer-Policy: No se define el control sobre la información de referencia enviada a otros sitios web.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del navegador como la cámara, el micrófono o la ubicación.
[LOW] Server header expuesto: La cabecera Server revela el uso de railway-hikari, facilitando información técnica sobre la infraestructura a posibles atacantes.
[LOW] Robots.txt y Sitemap: El servidor devuelve un error 429 al intentar acceder a estos recursos, impidiendo una indexación y auditoría de rutas adecuada.