EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://apis.roblox.com/user-heartbeats-api/pulse	Checks	9 pruebas
Dominio	apis.roblox.com	Hallazgos	42 totales
Fecha	16 de junio de 2026 a las 18:11	Problemas	10 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría técnica, el endpoint apis.roblox.com ha obtenido una puntuación de 72/100, lo que resulta en una calificación de grado C. El análisis pasivo ejecutó un total de 9 comprobaciones, de las cuales 6 resultaron satisfactorias, se identificó 1 advertencia y se registraron 2 fallos críticos en la configuración. Aunque el cifrado de la comunicación es sólido, la ausencia total de cabeceras de protección defensiva compromete la integridad del servicio. Se concluye que el sitio es vulnerable ante ataques de inyección y suplantación debido a una configuración de seguridad incompleta. El estado actual requiere una intervención inmediata para mitigar los riesgos identificados.

Resumen de Riesgos

0	4	3	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 252 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 252 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  252 dias restantes (expira: 2027-02-23T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-23T00:00:00.000Z
- 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: public-gateway — 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 307 redirige a https://apis.roblox.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 404

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 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica 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 que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de esta directiva hace que el sitio sea vulnerable a ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce conexiones seguras HTTPS permanentemente.
[HIGH] HSTS (Strict-Transport-Security): El mecanismo de forzado no está activo, permitiendo posibles degradaciones de seguridad en la conexión.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, facilitando la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a otros sitios web.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, lo que podría permitir el acceso no autorizado a funciones del dispositivo.
[LOW] Server header expuesto: La cabecera Server: public-gateway revela información técnica sobre la infraestructura interna.

[LOW] robots.txt: El archivo de directrices para rastreadores no fue encontrado, dificultando el control de indexación.
[LOW] sitemap.xml: La ausencia de este archivo limita la visibilidad estructurada del sitio para herramientas de análisis.