EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://live-sound-patterns.web.app	Checks	9 pruebas
Dominio	live-sound-patterns.web.app	Hallazgos	44 totales
Fecha	26 de marzo de 2026 a las 09:49	Problemas	10 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar el análisis de seguridad en el sitio https://live-sound-patterns.web.app, se ha obtenido una puntuación de 80/100 con una calificación de nota B. La auditoría se basó en la ejecución de 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración del servidor. El cifrado SSL y la gestión de redirecciones HTTPS son excelentes, garantizando la privacidad de los datos en tránsito. Sin embargo, la ausencia de cabeceras de seguridad y la exposición de rutas sensibles incrementan la superficie de ataque. En su estado actual, el sitio se considera parcialmente vulnerable ante ataques de inyección y suplantación de identidad.

Resumen de Riesgos

0	2	8	0	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	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: 2026-06-18T16:23:06.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-20T16:23:07.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- 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=31556926; includeSubDomains; preload
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://live-sound-patterns.web.app/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31556926; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31556926 (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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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

[ALTA] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[ALTA] X-Frame-Options: La ausencia de esta protección hace que el sitio sea vulnerable a ataques de clickjacking, permitiendo que sea embebido en marcos externos no autorizados.
[MEDIA] X-Content-Type-Options: Al no estar configurada, el navegador podría realizar MIME-type sniffing, aumentando el riesgo de ejecución de scripts disfrazados de otros formatos.

[MEDIA] Referrer-Policy: La falta de control sobre la información de referencia puede filtrar datos sensibles de la URL hacia dominios externos.
[MEDIA] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente que scripts externos accedan a funciones como la cámara o el micrófono.
[MEDIA] Archivos de información expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente y pueden revelar detalles técnicos de la infraestructura.
[MEDIA] Rutas de administración detectadas: Se identificaron rutas activas como /wp-login.php, /administrator/ y /user/login, lo que facilita intentos de acceso no autorizado o ataques de fuerza bruta.
[BAJA] Ausencia de robots.txt y sitemap.xml: El sitio carece de archivos de indexación estándar, lo que dificulta la gestión del rastreo por parte de motores de búsqueda.