EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://gen-lang-client-0604858335.web.app/	Checks	9 pruebas
Dominio	gen-lang-client-0604858335.web.app	Hallazgos	45 totales
Fecha	24 de mayo de 2026 a las 11:24	Problemas	5 detectados

A

96/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada sobre el sitio web arroja una puntuacion de 96/100, lo que equivale a una nota A. Durante el analisis se ejecutaron 9 checks pasivos, de los cuales 8 resultaron satisfactorios y solo uno presento un fallo en la configuracion de archivos de navegacion. El sitio demuestra un alto compromiso con la seguridad en sus comunicaciones y configuracion de cabeceras. Sin embargo, la exposicion de rutas administrativas y archivos de informacion tecnica representa un riesgo moderado. En conclusion, el sitio es seguro frente a amenazas externas comunes, pero requiere ajustes de endurecimiento en la visibilidad de sus directorios.

Resumen de Riesgos

0	0	5	0	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 86 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	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 86 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  86 dias restantes (expira: 2026-08-18T17:14:16.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-20T17:14:17.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' https://www.gstatic.com https://apis.googl...

- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=31556926; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: camera=(self), microphone=(self), geolocation=(self), payment=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://gen-lang-client-0604858335.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
- INFO **Tecnologias detectadas**
  React

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

[MEDIUM] Archivo /readme.html: Este archivo es accesible publicamente y puede revelar informacion sobre la tecnologia subyacente.

[MEDIUM] Archivo /README.txt: La presencia de este archivo permite a atacantes obtener datos tecnicos sobre la infraestructura del sitio.
[MEDIUM] Ruta /wp-login.php: El panel de inicio de sesion es visible para cualquier usuario, permitiendo ataques dirigidos de fuerza bruta.
[MEDIUM] Ruta /administrator/: El directorio de administracion esta expuesto, lo que facilita el reconocimiento de puntos de entrada criticos.
[MEDIUM] Ruta /user/login: Se ha detectado un punto de acceso de usuarios que carece de restricciones de visibilidad a nivel de servidor.
[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos impide un control adecuado sobre el rastreo de motores de busqueda y puede ocultar errores de estructura.