EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://share.google/rCoAovmNTMg9Eupfn	Checks	9 pruebas
Dominio	share.google	Hallazgos	39 totales
Fecha	11 de junio de 2026 a las 01:38	Problemas	10 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha resultado en una puntuación de 61/100, lo que equivale a una nota de C. De los 9 checks pasivos ejecutados, 6 se completaron con éxito, mientras que se identificaron 3 fallos críticos relacionados con la configuración del servidor. El certificado SSL es correcto, pero la ausencia total de cabeceras de seguridad y de redirección automática hacia HTTPS debilita la postura defensiva. En su estado actual, el sitio se considera vulnerable debido a que carece de protecciones básicas contra ataques comunes de interceptación e inyección.

Resumen de Riesgos

0	5	5	0	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 67 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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 67 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  67 dias restantes (expira: 2026-08-17T08:37:32.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-25T08:37:33.000Z
- 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

- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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
- 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 **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] Redirección HTTP a HTTPS: El servidor no redirige automáticamente el tráfico inseguro a la versión cifrada, permitiendo el acceso vía HTTP.
[HIGH] Strict-Transport-Security: Falta la cabecera HSTS, lo que impide que el navegador fuerce conexiones seguras de forma permanente.
[HIGH] Content-Security-Policy: Ausente. Esta vulnerabilidad permite la ejecución de scripts maliciosos (XSS) y ataques de inyección de contenido.
[HIGH] X-Frame-Options: Ausente. El sitio no tiene protección contra ataques de clickjacking, permitiendo que sea cargado en iframes externos.
[MEDIUM] X-Content-Type-Options: Ausente. El navegador podría intentar adivinar el tipo de contenido (MIME-sniffing), facilitando la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: Ausente. No se controla la cantidad de información que el navegador envía al navegar desde este sitio hacia otros enlaces.
[MEDIUM] Permissions-Policy: Ausente. No existen restricciones sobre qué funciones del navegador (cámara, micrófono, geolocalización) pueden ser activadas por el sitio.
[MEDIUM] Archivos técnicos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, lo que puede revelar información sobre la infraestructura interna.
[LOW] Ausencia de robots.txt y sitemap.xml: El sitio carece de archivos de indexación, lo que dificulta la gestión del rastreo por parte de buscadores.