EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://share.google/CVronZtOo9vk11tFM	Checks	9 pruebas
Dominio	share.google	Hallazgos	45 totales
Fecha	12 de mayo de 2026 a las 11:11	Problemas	16 detectados

D

43/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el sitio share.google/CVronZtOo9vk11tFM ha arrojado una puntuación de 43/100, lo que resulta en una calificación de grado D. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios y 5 presentaron fallos críticos. La ausencia de un pentest activo limita el informe a vulnerabilidades detectables por observación externa, pero los hallazgos actuales son suficientes para identificar riesgos graves. Se ha detectado una exposición innecesaria de versiones de software y una carencia absoluta de cabeceras de seguridad. Por tanto, se concluye que el sitio es actualmente vulnerable y requiere medidas correctivas urgentes.

Resumen de Riesgos

0	8	6	2	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 62 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	20	FALLO	WordPress 1.2.3 expuesta
Seguridad de Cookies	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
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 62 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  62 dias restantes (expira: 2026-07-13T08:35:57.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-20T08:35:58.000Z
- 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: nginx — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.4.33, PleskLin — Revela framework/lenguaje
- 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
- INFO **Tecnologias detectadas**
  PHP/7.4.33, PleskLin

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1.2.3 expuesta

- ALTO **WordPress version**
  Version 1.2.3 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- 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

Seguridad de Cookies — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

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] Versión de WordPress expuesta: Se detectó la versión 1.2.3, lo cual permite a potenciales atacantes identificar y explotar CVEs específicos de una versión obsoleta.

[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a clickjacking, permitiendo que sea cargado en iframes para engañar a los usuarios.
[HIGH] Falta de Strict-Transport-Security: La carencia de HSTS impide obligar al navegador a usar siempre conexiones seguras.
[HIGH] Redirección HTTPS inexistente: El servidor responde por HTTP (200 OK) sin redirigir al protocolo seguro, exponiendo datos en tránsito.
[HIGH] Cookie PHPSESSID insegura: Faltan los atributos HttpOnly y Secure, permitiendo el acceso a la sesión mediante scripts y el envío de datos por canales no cifrados.
[MEDIUM] X-Content-Type-Options ausente: El servidor no previene el sniffing de tipos MIME, lo que podría llevar a la ejecución de contenido inesperado.
[MEDIUM] Archivos de información expuestos: Los archivos /readme.html y /README.txt son accesibles, revelando detalles sobre la infraestructura interna.
[MEDIUM] Cookie PHPSESSID sin SameSite: La falta de este atributo hace que las sesiones de los usuarios sean vulnerables a ataques de falsificación de peticiones en sitios cruzados (CSRF).
[MEDIUM] Referrer-Policy y Permissions-Policy faltantes: No se controla la información de procedencia enviada a terceros ni se restringen las APIs del navegador como cámara o micrófono.
[LOW] Cabecera Server expuesta: Se revela el uso de nginx, lo que ayuda a los atacantes a acotar las técnicas de explotación según el software del servidor.
[LOW] X-Powered-By expuesto: El banner revela el uso de PHP/7.4.33 y PleskLin, ofreciendo información técnica sensible sobre el framework de ejecución.