EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://search.google.com/local/writereview?placeid=ChIJU4LP1R4pQggRLntuyZ9MaIo	Objetivo	Pruebas
Dominio	search.google.com	Hallazgos	46 totales
Fecha	16 de abril de 2026 a las 20:00	Problemas	6 detectados

B

86/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad del dominio evaluado ha arrojado una puntuación de 86/100, lo que otorga una nota B. Se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue calificado como fallo. La infraestructura muestra un sólido manejo del cifrado SSL, pero presenta deficiencias en la configuración de cabeceras de seguridad y políticas de transporte. En conclusión, el sitio se considera mayoritariamente seguro, aunque presenta vulnerabilidades específicas que deben corregirse para mitigar riesgos de interceptación y ataques de sesión.

Resumen de Riesgos

0	1	2	3	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 67 dias
Cabeceras de Seguridad	90	AVISO	5/6 presentes. Faltan: Referrer-Policy
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	67	AVISO	__Host-GAPS: falta SameSite
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: 2026-06-22T08:35:16.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-30T08:35:17.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 90/100

Estado: AVISO

5/6 presentes. Faltan: Referrer-Policy

- BAJO **Server header expuesto**
  Server: ESF — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: require-trusted-types-for 'script';report-uri /v3/signin/_/AccountsSignInUi/cspr...
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- INFO **Permissions-Policy**
  Presente: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.google.com/
- 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**
  Next.js

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 — 67/100

Estado: AVISO

__Host-GAPS: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: __Host-GAPS — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __Host-GAPS — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __Host-GAPS — 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 **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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

[HIGH] HSTS (Strict-Transport-Security): HSTS no configurado, lo que impide que el navegador fuerce el uso exclusivo de HTTPS y permite ataques de degradación de protocolo.

[MEDIUM] Cookie: __Host-GAPS: Falta el atributo SameSite, lo que hace a la cookie vulnerable a ataques de Falsificación de Petición en Sitios Cruzados (CSRF).
[MEDIUM] Referrer-Policy: La ausencia de esta cabecera impide controlar qué información de procedencia se envía a otros sitios al navegar.
[LOW] Server header expuesto: La cabecera Server revela el valor ESF, facilitando a un atacante el reconocimiento de la tecnología del servidor.
[LOW] robots.txt: No encontrado (HTTP 404), lo que impide dar instrucciones claras a los rastreadores sobre qué partes del sitio indexar.
[LOW] sitemap.xml: No encontrado (HTTP 404), dificultando la comprensión de la estructura del sitio y su indexación.