EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ww.google.com	Checks	9 pruebas
Dominio	ww.google.com	Hallazgos	52 totales
Fecha	2 de junio de 2026 a las 22:23	Problemas	10 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada sobre ww.google.com arroja una puntuación de 73/100, lo que corresponde a una calificación de C. El análisis consistió en 9 checks pasivos donde se obtuvieron 5 resultados satisfactorios, 2 advertencias y 2 fallos críticos en la configuración. Aunque el sitio web cuenta con un cifrado de conexión robusto, presenta carencias significativas en las políticas de defensa del navegador y protección de cookies. Con base en estos hallazgos, el sitio se considera actualmente vulnerable ante ataques de inyección y secuestro de sesiones. Es necesario implementar medidas correctivas inmediatas para elevar los estándares de seguridad a un nivel aceptable.

Resumen de Riesgos

0	4	3	3	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 69 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
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	89	AVISO	SOCS: falta HttpOnly
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 69 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  69 dias restantes (expira: 2026-08-10T18:35:27.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-18T18:35:28.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

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

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 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 — 89/100

Estado: AVISO

SOCS: falta HttpOnly

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: SOCS — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: SOCS — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: SOCS — SameSite**
  SameSite=lax
- INFO **Cookie: AEC — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: AEC — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: AEC — SameSite**
  SameSite=lax
- INFO **Cookie: __Secure-ENID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __Secure-ENID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __Secure-ENID — SameSite**
  SameSite=lax

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)
- 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] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] Strict-Transport-Security: Falta la configuración HSTS, lo que impide que el navegador obligue siempre al uso de conexiones HTTPS seguras.
[HIGH] Cookie SOCS (Falta HttpOnly): La cookie carece del flag de seguridad, permitiendo que sea accesible mediante scripts y aumentando el riesgo de robo de identidad.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría llevar a la ejecución de archivos no deseados.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a otros dominios, lo que puede exponer datos de navegación privados.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono por parte de terceros.
[LOW] Server header expuesto: El servidor revela el valor gws, proporcionando información técnica sobre la infraestructura que puede ser usada por atacantes.
[LOW] Archivos de rastreo faltantes: No se encontraron los archivos robots.txt ni sitemap.xml, lo que afecta la visibilidad y el control del rastreo web.