EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://script.google.com/macros/s/AKfycbz7Qx7j1bXb0Ps5srlgZqq20LpK9PoFjUc6H94wmy7dKAHSVK7mKV9D3MhgUVq-buii/exec	Checks	9 ejecutados
Dominio	script.google.com	Hallazgos	45 totales
Fecha	13 de septiembre de 2026 a las 02:11	Problemas	7 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de ciberseguridad ha otorgado al sitio una puntuación de 81/100, lo que equivale a una nota B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración de seguridad. El transporte de datos es robusto gracias a una implementación correcta de SSL, pero existen carencias importantes en las directivas de protección del navegador. Concluimos que el sitio es generalmente seguro en su infraestructura de red, pero vulnerable a ataques específicos de aplicación como inyección de código y clickjacking. Es imperativo corregir las omisiones en las cabeceras HTTP para elevar el nivel de protección al estándar óptimo.

Resumen de Riesgos

0	3	1	3	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 50 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
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 50 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  50 dias restantes (expira: 2026-11-02T08:37:41.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-10T08:37:42.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, Permissions-Policy

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

- 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)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://script.google.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000; includeSubdomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 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**
  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 — 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 **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 permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso al no restringir el origen de los recursos.

[HIGH] X-Frame-Options: Esta omisión hace que el sitio sea vulnerable a Clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar a los usuarios.
[HIGH] Strict-Transport-Security: Al no declarar HSTS, el servidor no obliga a los navegadores a usar conexiones HTTPS de forma estricta, aumentando el riesgo de ataques de degradación.
[MEDIUM] Permissions-Policy: La falta de esta directiva impide limitar el acceso de la web a funciones sensibles del navegador del usuario como la cámara, el micrófono o la ubicación.
[LOW] Server header expuesto: El encabezado revela la cadena "Server: ESF", proporcionando información técnica sobre la infraestructura que facilita el reconocimiento por parte de atacantes.
[LOW] robots.txt no encontrado: La carencia de este archivo impide gestionar correctamente el comportamiento de los rastreadores automáticos y bots en el sitio.
[LOW] sitemap.xml no encontrado: La ausencia de un mapa del sitio dificulta la auditoría de rutas indexadas y la organización lógica del contenido ante motores de búsqueda.