EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://forms.gle/LhEnqXVaxJENY9L7A	Checks	9 pruebas
Dominio	forms.gle	Hallazgos	46 totales
Fecha	16 de mayo de 2026 a las 22:20	Problemas	9 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 75/100, lo que corresponde a una calificación de nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 generó una advertencia y 3 terminaron en fallo. Aunque el cifrado de datos mediante SSL es robusto, la ausencia de cabeceras de protección esenciales y deficiencias en la configuración de cookies representan un riesgo. El pentest activo no fue ejecutado en esta instancia, por lo que la evaluación se limita a la superficie de exposición externa detectada. En conclusión, el sitio se considera vulnerable a ataques específicos como clickjacking y secuestro de sesiones debido a estas omisiones de configuración.

Resumen de Riesgos

0	4	2	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 65 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, Str...
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	33	FALLO	NID: falta Secure; NID: 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 65 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  65 dias restantes (expira: 2026-07-20T16:08:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-21T15:11:29.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: require-trusted-types-for 'script';report-uri https://csp.withgoogle.com/csp/doc...
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://forms.gle/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 400

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 — 33/100

Estado: FALLO

NID: falta Secure; NID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: NID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: NID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: NID — 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 400)
- BAJO **sitemap.xml**
  No encontrado (HTTP 400)
- 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

[LOW] Server header expuesto: El servidor responde con la cabecera Server: GSE, lo que revela información técnica sobre la infraestructura subyacente.

[HIGH] X-Frame-Options: Esta cabecera no está configurada, lo que permite que el sitio sea embebido en iframes y facilita ataques de clickjacking.
[HIGH] Strict-Transport-Security: La falta de la cabecera HSTS impide que el navegador fuerce conexiones seguras por defecto, aumentando el riesgo de ataques man-in-the-middle.
[MEDIUM] Permissions-Policy: No se han definido restricciones para las APIs del navegador, permitiendo potencialmente el acceso no deseado a funciones como cámara o micrófono.
[HIGH] HSTS no configurado: El mecanismo para obligar al navegador a usar siempre HTTPS está ausente, debilitando la política de transporte seguro.
[HIGH] Cookie NID (Falta flag Secure): La cookie no incluye el atributo Secure, lo que implica que podría ser transmitida a través de conexiones no cifradas.
[MEDIUM] Cookie NID (Falta SameSite): La ausencia del atributo SameSite hace que la cookie sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[LOW] robots.txt no encontrado: El servidor devuelve un error 400 al buscar este archivo, lo que dificulta la gestión del rastreo para motores de búsqueda.
[LOW] sitemap.xml no encontrado: La falta de un mapa del sitio impide una indexación estructurada y la auditoría de contenidos públicos.