EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://meetup-plannings.web.app/login	Checks	9 pruebas
Dominio	meetup-plannings.web.app	Hallazgos	44 totales
Fecha	8 de julio de 2026 a las 19:09	Problemas	10 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 80/100 con una calificación de grado B. Durante el proceso se ejecutaron 9 comprobaciones pasivas, de las cuales 7 resultaron satisfactorias y 2 presentaron fallos críticos relacionados con la configuración de seguridad y la exposición de archivos. Aunque el sitio cuenta con una base sólida en términos de cifrado y redirecciones, presenta vulnerabilidades en la protección contra ataques de inyección y una gestión deficiente de archivos informativos. En conclusión, el sitio es moderadamente seguro, pero se considera vulnerable ante ataques específicos de manipulación de interfaz y recolección de información.

Resumen de Riesgos

0	2	8	0	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 41 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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 41 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  41 dias restantes (expira: 2026-08-18T17:14:16.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-20T17:14:17.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31556926; includeSubDomains; preload
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://meetup-plannings.web.app/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31556926; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31556926 (365 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

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- 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
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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

- 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] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en iframes, facilitando ataques de clickjacking.
[MEDIUM] X-Content-Type-Options: Falta la configuración para evitar que el navegador realice MIME-type sniffing, lo que podría llevar a la ejecución de archivos no deseados.

[MEDIUM] Referrer-Policy: No existe una política definida, lo que puede provocar la fuga de información sensible en las cabeceras de referencia hacia sitios externos.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs del navegador como la cámara o el micrófono, aumentando la superficie de riesgo.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede revelar detalles técnicos o versiones del software base.
[MEDIUM] Archivo /README.txt: La exposición de este documento permite a terceros obtener información sobre la estructura o configuración del sitio.
[MEDIUM] Ruta /wp-login.php: Panel de acceso administrativo detectado y accesible de forma pública.
[MEDIUM] Ruta /administrator/: Directorio de gestión administrativa expuesto a usuarios no autorizados.
[MEDIUM] Ruta /user/login: Interfaz de autenticación accesible que podría ser objetivo de ataques de fuerza bruta.
[MEDIUM] Robots.txt y Sitemap: La falta de estos archivos dificulta el control de rastreo y puede exponer rutas que no deberían ser indexadas.