EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.jotform.com/assign/251398576034868/252823426103045	Checks	9 pruebas
Dominio	www.jotform.com	Hallazgos	54 totales
Fecha	15 de agosto de 2026 a las 01:36	Problemas	5 detectados

B

84/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado arroja una puntuación de 84/100 con una calificación de grado B. Se ejecutaron un total de 9 verificaciones pasivas, de las cuales 8 resultaron satisfactorias y una presentó fallos críticos en la configuración. El sitio demuestra un manejo excelente del cifrado de datos y la seguridad de las sesiones mediante cookies. Sin embargo, la carencia de cabeceras de protección en el servidor aumenta el riesgo de ataques dirigidos a los usuarios finales. En conclusión, el sitio es mayoritariamente seguro en su infraestructura básica, pero vulnerable a ataques de inyección y suplantación de interfaz.

Resumen de Riesgos

0	2	3	0	49
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 190 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	3 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 190 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  190 dias restantes (expira: 2027-02-20T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-06T00:00:00.000Z
- 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=31536000;
- 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://www.jotform.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (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
- INFO **Tecnologias detectadas**
  React

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

3 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- INFO **Cookie: guest — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: guest — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: guest — SameSite**
  SameSite=none
- INFO **Cookie: guest — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: guest — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: guest — SameSite**
  SameSite=none
- INFO **Cookie: guest — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: guest — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: guest — SameSite**
  SameSite=none

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (12030 bytes)
- INFO **Reglas robots.txt**
  425 Disallow, 9 Allow
- INFO **Sitemap en robots.txt**
  https://www.jotform.com/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

[ALTA] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS).
[ALTA] X-Frame-Options: Al no estar presente, el sitio puede ser embebido en marcos externos maliciosos, permitiendo ataques de clickjacking para engañar al usuario.
[MEDIA] X-Content-Type-Options: La falta de esta directiva permite que el navegador intente adivinar el tipo de contenido, lo que facilita la ejecución de archivos maliciosos mediante MIME-sniffing.
[MEDIA] Referrer-Policy: No existe un control sobre la información de origen que se envía a otros dominios, lo que podría filtrar URLs privadas o sensibles.
[MEDIA] Permissions-Policy: El servidor no restringe el acceso a funciones sensibles del navegador como la cámara, el micrófono o la geolocalización desde el código del sitio.