EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://eventos-s.vercel.app	Checks	9 pruebas
Dominio	eventos-s.vercel.app	Hallazgos	44 totales
Fecha	21 de abril de 2026 a las 02:27	Problemas	8 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web eventos-s.vercel.app ha finalizado con una puntuación de 80/100 y una calificación de grado B. Se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración de seguridad del servidor. Aunque la base de cifrado es sólida, la ausencia de políticas de defensa en el navegador deja la plataforma expuesta a ataques de inyección. En conclusión, el sitio se considera moderadamente seguro, pero es vulnerable a ataques de Clickjacking y XSS debido a la falta de cabeceras de seguridad esenciales. La infraestructura de red y el manejo de HTTPS cumplen con los estándares actuales.

Resumen de Riesgos

0	2	3	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 36 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 36 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  36 dias restantes (expira: 2026-05-27T06:28:02.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-26T06:28:03.000Z
- 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

- BAJO **Server header expuesto**
  Server: Vercel — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000; 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 308 redirige a https://eventos-s.vercel.app/
- 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

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: Falta esta cabecera esencial que previene ataques de inyección de código como Cross-Site Scripting (XSS) al definir qué fuentes de contenido son de confianza.
[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado dentro de marcos o iframes, lo que facilita ataques de Clickjacking para engañar a los usuarios.

[MEDIUM] X-Content-Type-Options: No está configurada, permitiendo que el navegador intente adivinar el tipo de contenido (MIME-type sniffing), lo que puede derivar en la ejecución de scripts maliciosos disfrazados de otros archivos.
[MEDIUM] Referrer-Policy: Falta esta política que controla cuánta información de la URL de origen se comparte al navegar hacia otros enlaces, lo que podría exponer datos sensibles.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador, permitiendo potencialmente el acceso a hardware como cámara, micrófono o geolocalización sin un control estricto.
[LOW] Server header expuesto: La cabecera Server revela explícitamente el uso de tecnología Vercel, proporcionando información técnica valiosa que un atacante podría usar para buscar exploits específicos.
[LOW] robots.txt: El archivo no fue encontrado (404), lo que impide dar instrucciones claras a los rastreadores de motores de búsqueda sobre qué partes del sitio no deben indexarse.
[LOW] sitemap.xml: La ausencia de este archivo dificulta la indexación correcta del sitio y no cumple con las mejores prácticas de administración web.