EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://speedssj.gg	Checks	9 pruebas
Dominio	speedssj.gg	Hallazgos	41 totales
Fecha	23 de junio de 2026 a las 23:15	Problemas	11 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre la plataforma web ha resultado en una puntuación de 57/100, lo que otorga una calificación final de grado D. Durante el proceso se ejecutaron un total de 9 checks pasivos, obteniendo 5 resultados satisfactorios, 1 advertencia y 3 fallos críticos en la configuración de seguridad. El análisis revela deficiencias severas en la implementación de cabeceras de protección y en la gestión del tráfico cifrado. Debido a la ausencia de políticas contra ataques de inyección y secuestro de clics, se concluye que el sitio es actualmente vulnerable. Es necesaria una intervención técnica inmediata para mitigar los riesgos identificados y alcanzar un nivel de protección aceptable.

Resumen de Riesgos

0	5	4	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 60 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 60 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  60 dias restantes (expira: 2026-08-23T02:43:06.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-25T02:43:07.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — 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)
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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 **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — 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 scripts cruzados (XSS) e inyección de contenido malicioso en el navegador del usuario.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking, permitiendo que terceros carguen la página en marcos invisibles para engañar a los usuarios.
[HIGH] Strict-Transport-Security: La falta de esta política impide que el navegador fuerce conexiones seguras, facilitando ataques de degradación de SSL y robo de sesiones.
[HIGH] Redirección HTTPS: El servidor responde exitosamente en el puerto 80 sin redirigir automáticamente al tráfico cifrado, exponiendo los datos transmitidos a interceptaciones.
[MEDIUM] X-Content-Type-Options: La falta de esta instrucción permite que el navegador realice sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No se controla la cantidad de información de navegación que se envía a otros dominios, lo que representa un riesgo para la privacidad de los usuarios.
[MEDIUM] Permissions-Policy: El sitio no define restricciones sobre el uso de APIs sensibles del navegador como la cámara, el micrófono o la ubicación.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este servidor web alternativo incrementa la superficie de ataque y puede revelar servicios internos no protegidos.
[LOW] Server header expuesto: El encabezado revela el uso de Cloudflare, proporcionando información técnica que ayuda a un atacante en la fase de reconocimiento.
[LOW] Ausencia de sitemap.xml y robots.txt: La inexistencia de estos archivos dificulta la indexación correcta y la gestión de permisos para rastreadores automáticos.