EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://juice-shop.herokuapp.com/#/	Checks	9 pruebas
Dominio	juice-shop.herokuapp.com	Hallazgos	33 totales
Fecha	13 de mayo de 2026 a las 23:38	Problemas	7 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 71/100, lo que equivale a una nota C. El análisis se basó en 9 checks pasivos, identificando que 5 de ellos se superaron correctamente mientras que se detectó un fallo crítico en la configuración de seguridad del servidor. Aunque la cifrado de la conexión es robusto, la ausencia total de cabeceras de protección básicas deja la plataforma expuesta a ataques conocidos. Se concluye que el sitio es vulnerable y requiere ajustes técnicos inmediatos para alcanzar un nivel de seguridad aceptable.

Resumen de Riesgos

0	3	3	1	26
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 261 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Deteccion CMS	100	OK	No se detecto un CMS conocido
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 261 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  261 dias restantes (expira: 2027-01-29T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-01T00:00:00.000Z
- 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: Heroku — 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.)

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

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

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 indispensable que previene ataques de Cross-Site Scripting (XSS) y ataques de inyección de contenido.
[HIGH] X-Frame-Options: No se encuentra presente, lo que permite que el sitio sea cargado en marcos (iframes) y facilita ataques de clickjacking.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide forzar conexiones HTTPS, dejando a los usuarios vulnerables a ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: Falta la directiva que evita que el navegador realice MIME-type sniffing, lo que podría llevar a la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada, lo que podría filtrar datos de navegación a dominios externos.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono a través de políticas de permisos.
[LOW] Server header expuesto: El servidor revela el valor Server: Heroku, facilitando a posibles atacantes información sobre la infraestructura tecnológica utilizada.