EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://juice-shop.github.io/	Checks	9 pruebas
Dominio	juice-shop.github.io	Hallazgos	46 totales
Fecha	20 de mayo de 2026 a las 21:31	Problemas	11 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada sobre el sitio web arroja una puntuacion de 76/100 con una calificacion de nota B. Se ejecutaron un total de 9 checks pasivos, obteniendo como resultado 6 verificaciones exitosas, 1 advertencia y 2 fallos criticos en la configuracion. El analisis revela una base de cifrado solida, pero identifica carencias importantes en las politicas de seguridad del lado del cliente y en la gestion de recursos externos. Concluimos que el sitio es moderadamente seguro, aunque vulnerable a ataques especificos de inyeccion de codigo y secuestro de clics debido a la ausencia de cabeceras de proteccion esenciales.

Resumen de Riesgos

0	2	5	4	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 46 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	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
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 46 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  46 dias restantes (expira: 2026-07-05T23:32:35.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-06T23:32:36.000Z
- 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: GitHub.com — 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=31556952
- 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://juice-shop.github.io/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31556952
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31556952 (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
- BAJO **Meta generator**
  Expone: Jekyll v3.10.0

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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://shop.spreadshirt.com/juiceshop
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://shop.spreadshirt.de/juiceshop

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 de cabecera CSP, lo que permite la ejecucion de scripts no autorizados y aumenta el riesgo de ataques XSS.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[MEDIUM] Contenido Mixto: Se detectaron dos recursos cargados mediante HTTP (enlaces a spreadshirt) dentro de una conexion HTTPS, lo que debilita la integridad de la sesion.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podria interpretar archivos de forma incorrecta mediante MIME-type sniffing, facilitando la ejecucion de malware.
[MEDIUM] Referrer-Policy: La falta de control sobre la informacion de referencia puede exponer URLs privadas a dominios de terceros durante la navegacion.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la camara o el microfono, aumentando la superficie de ataque.
[LOW] Server header expuesto: El servidor revela el uso de GitHub.com, proporcionando informacion tecnica que podria ser util para un atacante en la fase de reconocimiento.
[LOW] Meta generator expuesto: El codigo fuente revela el uso de Jekyll v3.10.0, lo que permite identificar posibles vulnerabilidades especificas de esa version de software.
[LOW] Archivos de indexacion ausentes: No se encontraron los archivos robots.txt ni sitemap.xml, lo que afecta la gestion de rastreo y la visibilidad controlada del sitio.