EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://fortnite-shop-bot-0pxi.onrender.com/index.html	Checks	9 pruebas
Dominio	fortnite-shop-bot-0pxi.onrender.com	Hallazgos	44 totales
Fecha	28 de mayo de 2026 a las 11:27	Problemas	12 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha resultado en una puntuación de 68/100, lo que otorga una calificación de grado C. El análisis se basó en la ejecución de 9 checks pasivos, obteniendo 5 resultados satisfactorios, 2 advertencias por configuraciones incompletas y 2 fallos críticos en la infraestructura defensiva. Aunque el cifrado básico está presente, la ausencia total de cabeceras de seguridad y la exposición de puertos innecesarios comprometen la integridad de la plataforma. Se concluye que el sitio es vulnerable ante ataques de inyección y técnicas de suplantación debido a una configuración de servidor deficiente.

Resumen de Riesgos

0	4	4	4	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 88 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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 88 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  88 dias restantes (expira: 2026-08-24T22:01:50.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-26T21:02:15.000Z
- 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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Express — Revela framework/lenguaje
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://fortnite-shop-bot-0pxi.onrender.com/
- 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
- INFO **Tecnologias detectadas**
  Express

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 — 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 la ejecución de scripts no autorizados y ataques de Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Al no estar configurada, el sitio permite ser cargado en frames externos, facilitando ataques de clickjacking contra los usuarios.

[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones HTTPS, dejando la sesión expuesta a ataques de degradación de protocolo.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La disponibilidad de este puerto alternativo incrementa la superficie de ataque y sugiere servicios internos expuestos.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría llevar a la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a terceros, lo que puede derivar en la fuga de datos sensibles de la URL.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones del navegador como cámara o geolocalización, aumentando el riesgo de privacidad.
[LOW] Server header expuesto: Se detectó el valor Cloudflare, lo que revela información sobre la infraestructura de red a posibles atacantes.
[LOW] X-Powered-By expuesto: El valor Express revela el framework de desarrollo utilizado, permitiendo ataques dirigidos a vulnerabilidades conocidas de esa tecnología.
[LOW] robots.txt no encontrado: La ausencia de este archivo impide gestionar correctamente qué áreas del sitio deben ser rastreadas por motores de búsqueda.
[LOW] sitemap.xml no encontrado: La falta de este recurso dificulta la indexación estructurada y el control de los endpoints públicos del sitio.