

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://punto-de-venta-demo.onrender.com	Checks	9 pruebas
Dominio	punto-de-venta-demo.onrender.com	Hallazgos	45 totales
Fecha	23 de septiembre de 2026 a las 17:31	Problemas	15 detectados

C

68/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el activo arrojó una puntuación de 68/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 terminaron en fallo crítico por deficiencias de configuración. Aunque el cifrado de datos es robusto, la ausencia total de cabeceras de protección y la exposición de rutas técnicas elevan significativamente el riesgo. Se concluye que el sitio es vulnerable ante ataques de inyección y manipulación de sesiones debido a una superficie de exposición innecesariamente amplia.

Resumen de Riesgos

0 CRITICO	4 ALTO	9 MEDIO	2 BAJO	30 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: 2026-12-20T23:04:28.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-21T22:04:31.000Z
- 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://punto-de-venta-demo.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

- MEDIO

Archivo /readme.html
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Archivo /README.txt
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Ruta /wp-login.php
Panel de login accesible publicamente

- MEDIO

Ruta /administrator/
Panel de login accesible publicamente
- MEDIO

Ruta /user/login
Panel de login accesible publicamente
- 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

- INFO

security.txt
Presente en /.well-known/security.txt — Buena practica

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 facilita la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).

[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking donde un atacante puede camuflar la interfaz.

[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS a nivel de navegador, permitiendo ataques de degradación de conexión.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que puede llevar a la ejecución de archivos inesperados.

[MEDIUM] Referrer-Policy: No se controla la información de navegación que se envía a terceros al seguir enlaces externos.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del navegador como la ubicación, cámara o micrófono.

[MEDIUM] Rutas administrativas expuestas: Se detectó acceso público a /wp-login.php, /administrator/ y /user/login, facilitando intentos de acceso no autorizado.

[MEDIUM] Archivos de información accesibles: Los archivos /readme.html y /README.txt están expuestos y pueden revelar detalles técnicos del desarrollo.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La disponibilidad de este puerto alternativo incrementa la superficie de ataque del servidor.

[LOW] Server header expuesto: El servidor revela que utiliza Cloudflare, proporcionando información útil para perfilar ataques dirigidos.

[LOW] X-Powered-By expuesto: Se divulga el uso del framework Express, lo cual permite a un atacante buscar vulnerabilidades específicas de esa tecnología.

[LOW] Ausencia de robots.txt y sitemap: La falta de estos archivos dificulta el control de indexación y el rastreo estructurado por motores de búsqueda.