

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sdlc.ai.vasscompany.com/#!/sdlc/project-summary	Checks	9 pruebas
Dominio	sdlc.ai.vasscompany.com	Hallazgos	41 totales
Fecha	14 de septiembre de 2026 a las 09:34	Problemas	10 detectados

C

72/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el activo digital arroja una puntuación exacta de 72/100 con una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, no hubo advertencias y 2 finalizaron con fallos críticos. A pesar de contar con una implementación de cifrado SSL robusta, la plataforma carece de las protecciones de cabeceras necesarias para mitigar ataques modernos. El estado actual del sitio se clasifica como vulnerable ante vectores de ataque de inyección y suplantación de identidad. Se requiere una intervención técnica inmediata para corregir las deficiencias encontradas en la configuración del servidor y la capa de aplicación.

Resumen de Riesgos

0	3	3	4	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 140 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 140 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
140 dias restantes (expira: 2027-01-31T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-07-17T00:00:00.000Z
- 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: nginx — 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.)

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 política de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 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 — Envío de correo
- INFO

Puerto 80 (HTTP)

Cerrado — 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

Análisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).

[HIGH] X-Frame-Options: La falta de esta directiva hace que el sitio sea susceptible a ataques de clickjacking, permitiendo que la web sea cargada en marcos externos.

[HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones seguras mediante HSTS, facilitando posibles ataques de degradación de protocolo SSL/TLS.

[MEDIUM] X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría permitir al navegador interpretar archivos de forma incorrecta y peligrosa.

[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia que se envía al navegar hacia otros dominios, lo que puede filtrar datos de la URL.

[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, permitiendo potencialmente el acceso a componentes como cámara, micrófono o geolocalización.

[LOW] Server header expuesto: La cabecera revela el uso de nginx, proporcionando información técnica que facilita la búsqueda de exploits específicos para ese software.

[LOW] X-Powered-By expuesto: Se expone el framework Express, revelando detalles sobre la tecnología de desarrollo utilizada en el backend.

[LOW] robots.txt no encontrado: La ausencia de este archivo genera un error 404 y dificulta la gestión de la indexación por parte de los motores de búsqueda.

[LOW] sitemap.xml no encontrado: No se detectó el mapa del sitio, lo cual afecta la estructura de rastreo y visibilidad controlada de la plataforma.