

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://adsync-sms-ops.lat/
Dominio adsync-sms-ops.lat
Fecha 22 de agosto de 2026 a las 04:21

Checks 9 pruebas
Hallazgos 43 totales
Problemas 13 detectados

D

59/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio adsync-sms-ops.lat ha arrojado una puntuación de 59/100, lo que resulta en una calificación de grado D. Los resultados de los 9 checks pasivos ejecutados muestran una infraestructura debilitada, con 2 fallos críticos y 2 advertencias importantes que comprometen la integridad del servicio. A pesar de contar con un certificado SSL válido, la ausencia total de cabeceras de seguridad y la falta de redirección forzada a HTTPS exponen a los usuarios a múltiples vectores de ataque. El análisis concluye que el sitio es actualmente vulnerable y requiere una intervención inmediata para corregir configuraciones básicas de servidor. La exposición de puertos no estándar y archivos de información técnica agrava el perfil de riesgo de la plataforma.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
90 dias restantes (expira: 2026-11-19T22:05:44.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-21T21:08:16.000Z
- 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

- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion
HTTP 303 — No redirige a HTTPS
- 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

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
- 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO

robots.txt
Presente (1836 bytes)
- INFO

Reglas robots.txt
9 Disallow, 1 Allow
- MEDIO

Bloqueo total
robots.txt bloquea todo el sitio con Disallow: /
- 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] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).

[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar al usuario.

[HIGH] Falta de Strict-Transport-Security: No se utiliza HSTS, lo que permite ataques de degradación de conexión de HTTPS a HTTP.

[HIGH] Fallo en Redirección HTTPS: El servidor no redirige el tráfico inseguro al puerto seguro, dejando los datos en tránsito expuestos a interceptación.

[MEDIUM] Puerto 8080 (HTTP-Alt) Abierto: La exposición de este puerto alternativo puede revelar servicios internos o paneles de administración no protegidos.

[MEDIUM] X-Content-Type-Options ausente: El navegador podría interpretar archivos de forma incorrecta, facilitando la ejecución de malware mediante MIME-sniffing.

[MEDIUM] Archivos /readme.html y /README.txt expuestos: Estos archivos son accesibles públicamente y pueden filtrar versiones de software o detalles de configuración.

[MEDIUM] Bloqueo total en Robots.txt: La directiva Disallow: / impide el rastreo legítimo y suele indicar una configuración de entorno de desarrollo expuesta por error.

[MEDIUM] Referrer-Policy y Permissions-Policy ausentes: No hay control sobre la información de navegación compartida ni restricciones sobre el uso de hardware del usuario.

[LOW] Cabecera Server expuesta: Se revela el uso de Cloudflare, lo que ayuda a un atacante a identificar la infraestructura y buscar exploits específicos.