EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://labsync.lat/	Checks	9 pruebas
Dominio	labsync.lat	Hallazgos	48 totales
Fecha	28 de julio de 2026 a las 19:49	Problemas	11 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al dominio labsync.lat arroja una puntuación de 73/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 comprobaciones pasivas, de las cuales 5 resultaron satisfactorias, 3 generaron advertencias y una fue identificada como un fallo crítico de configuración. Aunque el sitio cuenta con un cifrado de datos válido, presenta carencias importantes en la implementación de cabeceras de seguridad y en la gestión de redirecciones de tráfico. En conclusión, el sitio web se considera vulnerable debido a que permite conexiones no cifradas y expone vectores de ataque que facilitan el secuestro de sesiones y el reconocimiento de la infraestructura.

Resumen de Riesgos

0	2	8	1	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 dias
Cabeceras de Seguridad	70	AVISO	4/6 presentes. Faltan: X-Frame-Options, Permissi...
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): 22 (SSH)

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: 2026-10-26T16:38:56.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-28T16:38:57.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 70/100

Estado: AVISO

4/6 presentes. Faltan: X-Frame-Options, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net h...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer
- 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 200 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (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

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (26 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 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): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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] HTTP -> HTTPS redireccion: El servidor responde con éxito a peticiones bajo el protocolo HTTP sin redirigir al usuario a la versión segura, permitiendo la interceptación de datos.
[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking para engañar a los usuarios.
[MEDIUM] Puerto 22 (SSH) ABIERTO: El servicio de acceso remoto está expuesto públicamente, lo que representa un riesgo de ataques de fuerza bruta si no existe un filtrado de IPs.
[MEDIUM] Rutas de login expuestas: Se detectó acceso público a paneles administrativos en /wp-login.php, /administrator/ y /user/login, aumentando la superficie de ataque para accesos no autorizados.
[MEDIUM] Archivos de documentación expuestos: Los archivos /readme.html y /README.txt son accesibles y podrían revelar información técnica sobre el despliegue del sitio.
[MEDIUM] Permissions-Policy: No se han definido restricciones para las APIs del navegador, dejando abierta la posibilidad de que scripts de terceros accedan a funciones como la cámara o el micrófono.
[MEDIUM] Configuración de robots.txt: El archivo bloquea el rastreo de todo el sitio mediante Disallow: /, lo cual, sumado a la falta de un sitemap, sugiere una configuración de visibilidad deficiente.
[LOW] Server header expuesto: El servidor revela el uso de la tecnología nginx, proporcionando información útil para que un atacante busque vulnerabilidades específicas de dicho software.