

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://altheaespaisaluyt.com/
Dominio altheaespaisaluyt.com
Fecha 12 de mayo de 2026 a las 15:57

Checks 9 pruebas
Hallazgos 15 totales
Problemas 3 detectados

C

73/100

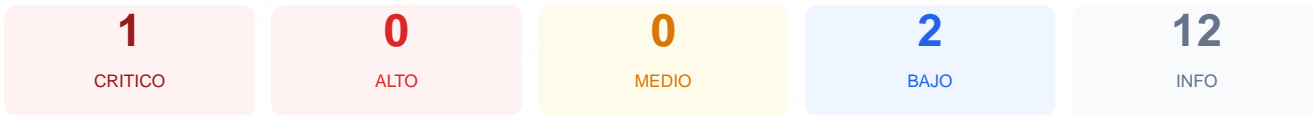
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del sitio web altheaespaisaluyt.com ha resultado en una puntuación exacta de 73/100, lo que otorga una calificación de C. Los resultados de los checks pasivos muestran un escenario preocupante donde, de 9 pruebas ejecutadas, solo una resultó satisfactoria, una falló directamente y el resto presentaron errores críticos de conectividad. No se pudo verificar la presencia de cifrado ni de cabeceras de seguridad esenciales debido a problemas técnicos en el servidor. En su estado actual, el sitio se considera vulnerable debido a la imposibilidad de garantizar una navegación privada y segura para los usuarios.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- **CRITICO** Conexion SSL
No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- **BAJO** robots.txt
Error al acceder
- **BAJO** sitemap.xml
Error al acceder

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- **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)**
Cerrado — 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 autenticación 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

- [CRITICAL] Conexion SSL: No se pudo establecer una conexion SSL/TLS, lo que impide el cifrado de datos entre el usuario y el servidor.
- [LOW] robots.txt y sitemap.xml: Error al acceder a estos archivos, lo que dificulta la indexación correcta y puede ocultar configuraciones de acceso erróneas.
- [HIGH] Cabeceras de Seguridad: Imposibilidad de verificar cabeceras HTTP, lo que sugiere una exposición potencial a ataques de inyección y suplantación.
- [MEDIUM] Redireccion HTTPS: No se pudo confirmar que el tráfico inseguro se redirija automáticamente a una versión protegida del sitio.
- [MEDIUM] Seguridad de Cookies: La falta de verificación impide confirmar si los datos de sesión viajan de forma cifrada y protegida contra scripts maliciosos.