EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Transacional.saludtotal.com.co	Checks	9 pruebas
Dominio	transacional.saludtotal.com.co	Hallazgos	15 totales
Fecha	2 de junio de 2026 a las 11:41	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 73/100, lo que corresponde a una calificación de C. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 1 validación correcta, 0 advertencias y 1 fallo directo, además de múltiples errores de comunicación con el servidor. La imposibilidad de verificar el cifrado SSL/TLS y las cabeceras de seguridad básicas sugiere una configuración técnica inestable o restrictiva. Debido a estos hallazgos, se concluye que el sitio es actualmente vulnerable y presenta riesgos significativos para la integridad de los datos.

Resumen de Riesgos

1	0	0	2	12
CRITICO	ALTO	MEDIO	BAJO	INFO

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 — Envio 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 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

[CRITICA] Conexion SSL/TLS: No se pudo establecer o verificar una conexion segura, lo que impide garantizar que la informacion viaje cifrada.
[ALTA] Cabeceras de Seguridad: No se detectaron encabezados de proteccion HTTP, dejando el sitio expuesto a ataques de intermediario y secuestro de sesiones.
[ALTA] Redireccion HTTPS: El servidor no confirma el redireccionamiento automatico a una navegacion segura, permitiendo conexiones vulnerables.
[MEDIA] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos dificulta la gestion del rastreo y puede exponer rutas no deseadas a motores de busqueda.
[MEDIA] Seguridad de Cookies: No se pudo validar la presencia de atributos de seguridad en las cookies, lo que podria comprometer la identidad de los usuarios.
[BAJA] Deteccion de CMS: La infraestructura no permite identificar el sistema de gestion de contenidos, lo que aunque dificulta ataques especificos, tambien impide verificar parches de seguridad.