EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://mediservicio.org.gt	Checks	9 pruebas
Dominio	mediservicio.org.gt	Hallazgos	15 totales
Fecha	21 de abril de 2026 a las 15:56	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada sobre el dominio mediservicio.org.gt arroja una puntuacion exacta de 73/100, otorgando una nota C. Durante la evaluacion se ejecutaron 9 checks pasivos, de los cuales 1 resulto en estado satisfactorio y 1 presento fallos criticos, mientras que el resto no pudo completarse por errores de conexion. Los resultados indican una imposibilidad tecnica para validar protocolos basicos de cifrado y cabeceras de proteccion. En consecuencia, el sitio se considera actualmente vulnerable y no confiable para el intercambio de informacion sensible. La infraestructura requiere una revision inmediata para permitir la correcta validacion de sus medidas de defensa.

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

[CRITICO] Conexion SSL/TLS: No se pudo establecer una comunicacion cifrada con el servidor, lo que impide asegurar la privacidad y la integridad de los datos de los usuarios.
[BAJO] Ausencia de archivos de indexacion: No se encontraron los archivos robots.txt ni sitemap.xml, lo cual dificulta la navegacion de motores de busqueda y puede exponer directorios internos por descuido.
[INFORMACION] Cabeceras de seguridad no verificables: La ausencia de respuesta en las cabeceras impide mitigar ataques de tipo Clickjacking o Cross-Site Scripting (XSS).
[INFORMACION] Configuracion de Cookies desconocida: Al no poder analizar las cookies, existe un riesgo latente de secuestro de sesion si no se utilizan los atributos Secure y HttpOnly.