EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://maisondesante.org.pe	Checks	9 pruebas
Dominio	maisondesante.org.pe	Hallazgos	15 totales
Fecha	16 de abril de 2026 a las 21:21	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio maisondesante.org.pe arrojo una puntuacion de 73/100, lo que equivale a una nota de C. El analisis se baso exclusivamente en 9 checks pasivos, de los cuales solo uno resulto satisfactorio, mientras que se registro un fallo critico de acceso y multiples errores de verificacion de protocolos. La imposibilidad de validar el cifrado SSL y las cabeceras de proteccion impide garantizar la integridad de la plataforma. Se concluye que el sitio es vulnerable debido a deficiencias severas en su configuracion de red y seguridad basica.

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

[CRITICAL] Conexion SSL: No se pudo establecer una conexion SSL/TLS valida, lo que impide el cifrado de datos entre el usuario y el servidor.
[HIGH] Cabeceras de Seguridad: Ausencia total de verificacion de cabeceras HTTP, dejando el sitio expuesto a ataques de intermediario y cross-site scripting.
[HIGH] Redireccion HTTPS: El servidor no garantiza el forzado de trafico seguro, permitiendo potenciales conexiones a traves de canales no cifrados.
[MEDIUM] Seguridad de Cookies: Incapacidad de validar atributos de seguridad en cookies, lo que podria permitir el robo de sesiones de usuario.
[LOW] robots.txt y sitemap.xml: Error al acceder a los archivos de indexacion, lo que indica una configuracion incorrecta o permisos de servidor mal establecidos.
[LOW] Deteccion de CMS: El sistema no permite identificar la tecnologia base, dificultando la gestion de parches y actualizaciones de seguridad conocidas.