EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://vmdbeni.compensar.ccf/frmlogin.aspx	Checks	9 pruebas
Dominio	vmdbeni.compensar.ccf	Hallazgos	15 totales
Fecha	7 de abril de 2026 a las 20:33	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio web ha arrojado una puntuación de 73/100, lo que equivale a una nota C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 1 resultó satisfactorio y 1 se registró como un fallo crítico de conectividad, impidiendo la validación de múltiples parámetros. Al no haberse ejecutado un pentest activo, los resultados se limitan a la configuración externa y visibilidad del servidor. Debido a la imposibilidad de verificar el cifrado y las cabeceras de protección, se concluye que el sitio es vulnerable y presenta un riesgo elevado 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

[CRITICAL] Conexión SSL/TLS: No se pudo establecer una comunicación cifrada, lo que expone cualquier información transmitida a interceptaciones por terceros.
[MEDIUM] Cabeceras de Seguridad: Ausencia de verificación de cabeceras HTTP, lo que sugiere que el sitio carece de protecciones contra ataques de Cross-Site Scripting y Clickjacking.
[MEDIUM] Seguridad de Cookies: No se pudo validar la presencia de atributos de seguridad en las cookies, aumentando el riesgo de robo de sesiones.
[LOW] Archivo robots.txt: El servidor no permite el acceso o carece de este archivo, dificultando la gestión del rastreo por motores de búsqueda.
[LOW] Archivo sitemap.xml: No se localizó el mapa del sitio, lo que afecta la visibilidad y el control de los endpoints expuestos de la aplicación.