EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://dmujeres.com.ec:8443/MyBusinessWeb/	Checks	9 pruebas
Dominio	dmujeres.com.ec	Hallazgos	15 totales
Fecha	2 de abril de 2026 a las 14:30	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio web ha resultado en una puntuación de 73/100, obteniendo una calificación final de nota C. Durante la evaluación se ejecutaron un total de 9 checks pasivos, de los cuales 1 resultó satisfactorio y 1 fue identificado como fallo crítico, mientras que el resto de parámetros no pudieron ser validados debido a errores de conexión. La imposibilidad de verificar el cifrado SSL/TLS y las cabeceras de seguridad representa un riesgo significativo para la integridad de los datos. Se concluye que el sitio es vulnerable y requiere una intervención inmediata para asegurar las comunicaciones de los usuarios. Actualmente, la plataforma no cumple con los estándares mínimos de seguridad web para el manejo de información corporativa.

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 en el puerto 8443, lo que significa que los datos transferidos podrian ser interceptados por terceros.
[LOW] robots.txt: El archivo de directivas para buscadores no es accesible, lo que impide gestionar correctamente que partes del sitio deben ser indexadas.
[LOW] sitemap.xml: No se encontro el mapa del sitio, dificultando la auditoria de paginas expuestas y la navegacion estructurada del portal.
[INFO] Cabeceras de Seguridad: Error en la verificacion de cabeceras HTTP, lo que sugiere una falta de protecciones contra ataques de clickjacking o inyeccion de codigo.