EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.umcp.edu.pa	Checks	9 pruebas
Dominio	www.umcp.edu.pa	Hallazgos	15 totales
Fecha	6 de julio de 2026 a las 23:42	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al dominio arrojó una puntuación de 73/100, lo que corresponde a una calificación de grado C. El proceso consistió en 9 checks pasivos ejecutados, resultando en 1 validación correcta, 0 advertencias y 1 fallo crítico de seguridad. No se ejecutó un pentest activo durante este ciclo de inspección. En base a los resultados obtenidos, el sitio se considera vulnerable debido a la incapacidad de establecer conexiones cifradas seguras y la ausencia de parámetros de configuración básicos.

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 fue posible establecer una conexión segura con el servidor, lo que impide el cifrado de datos entre el usuario y la plataforma.
[CRITICAL] Cabeceras de Seguridad: El sistema no pudo verificar la presencia de cabeceras HTTP esenciales para mitigar ataques como XSS o Clickjacking.
[LOW] Archivos de Indexación: Se detectó un fallo en el acceso a robots.txt y sitemap.xml, comprometiendo la visibilidad y el control de rastreo del sitio.
[MEDIUM] Redirección HTTPS: No se pudo validar que el servidor redirija automáticamente el tráfico inseguro hacia una conexión protegida.