EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://circuito.campestre.edu.co:85/general/	Checks	9 pruebas
Dominio	circuito.campestre.edu.co	Hallazgos	15 totales
Fecha	21 de mayo de 2026 a las 12:37	Problemas	2 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 73/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales únicamente 1 resultó exitoso, 1 presentó un fallo crítico y el resto no pudieron completarse debido a tiempos de espera agotados. Esta falta de respuesta del servidor impidió verificar configuraciones esenciales como cabeceras de seguridad y cifrado. Debido a la ausencia de archivos de configuración básicos y la imposibilidad de validar protocolos de protección, se concluye que el sitio es vulnerable y presenta un riesgo operativo moderado.

Resumen de Riesgos

0	0	0	2	13
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

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	1 puerto(s) abierto(s), todos esperados

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 307 redirige a https://circuito.campestre.edu.co:10443/

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

1 puerto(s) abierto(s), todos esperados

- 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)**
  Abierto (esperado) — 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

[BAJA] Ausencia de archivo robots.txt: La falta de este archivo impide dar instrucciones a los motores de búsqueda sobre qué partes del sitio no deben ser rastreadas.
[BAJA] Ausencia de archivo sitemap.xml: No existe una estructura definida para los indexadores, lo que dificulta el mapeo organizado de los directorios del sitio.
[MEDIA] Errores de conexión (Timeout): El servidor no respondió a las solicitudes de validación de cabeceras, cookies y redirecciones, lo cual es indicativo de una configuración de red inestable o restrictiva que oculta posibles fallos de seguridad.
[MEDIA] Falta de verificación de cabeceras: No se pudo confirmar la presencia de protecciones contra ataques XSS, Clickjacking o inyección de contenido.