EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cinq.cloud	Checks	9 pruebas
Dominio	cinq.cloud	Hallazgos	12 totales
Fecha	12 de mayo de 2026 a las 12:59	Problemas	3 detectados

F

20/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al dominio cinq.cloud ha arrojado una puntuación de 20/100, lo que corresponde a una calificación de F. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 1 fallo crítico por exposición de puertos y múltiples errores por tiempo de espera en las validaciones de identidad y cifrado. La presencia de servicios de base de datos y transferencia de archivos abiertos sin restricciones representa un vector de ataque inmediato. Por lo tanto, se concluye que el sitio es actualmente vulnerable y requiere intervención urgente para proteger su infraestructura.

Resumen de Riesgos

1	1	1	0	9
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
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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] Puerto 3306 (MySQL) abierto: La base de datos principal se encuentra expuesta directamente a internet, permitiendo intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP) abierto: El servicio de transferencia de archivos opera sin cifrado, lo que facilita la interceptación de credenciales y datos sensibles en la red.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de administración remota es visible públicamente, lo que aumenta la superficie de ataque para accesos no autorizados al servidor.
[ERROR] Fallo en verificación de cabeceras y SSL: No se detectaron parámetros de seguridad básicos como HSTS o políticas de protección contra Clickjacking, dejando el tráfico sin validación defensiva.