EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ckadron.co.in	Checks	9 pruebas
Dominio	ckadron.co.in	Hallazgos	15 totales
Fecha	23 de abril de 2026 a las 15:50	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de ciberseguridad realizada al sitio web arroja una puntuacion de 73/100, lo que corresponde a una nota C. El analisis se baso en 9 checks pasivos, de los cuales solo 1 resulto satisfactorio, mientras que se registro 1 fallo critico de acceso y multiples errores de conexion. Debido a la imposibilidad de verificar el cifrado SSL y las cabeceras de seguridad, el sitio se considera actualmente vulnerable y de alto riesgo para la integridad de los datos. Se requiere una intervencion tecnica inmediata para validar la infraestructura de seguridad basica.

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, lo que impide garantizar el cifrado de la informacion entre el usuario y el servidor.
[CRITICAL] Cabeceras de Seguridad: No se detectaron encabezados HTTP esenciales, dejando el sitio expuesto a ataques de cross-site scripting y clickjacking.
[LOW] robots.txt: El archivo no fue encontrado o es inaccesible, lo que afecta la gestion de la indexacion por parte de motores de busqueda.
[LOW] sitemap.xml: La ausencia de este archivo dificulta la auditoria de rutas expuestas y la navegacion estructurada del sitio.