EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.ncru.inf.ua	Checks	9 pruebas
Dominio	www.ncru.inf.ua	Hallazgos	16 totales
Fecha	7 de mayo de 2026 a las 10:39	Problemas	6 detectados

D

47/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al dominio ncru.inf.ua ha resultado en una puntuación de 47/100, lo que equivale a una nota D. Los resultados de los 9 checks pasivos ejecutados revelan deficiencias críticas, incluyendo la ausencia total de cifrado y la exposición de puertos administrativos. Se identificó un fallo importante en la gestión de protocolos de transferencia y una advertencia de riesgo en los servicios de acceso remoto. Por todo lo anterior, se concluye que el sitio es vulnerable y presenta un riesgo alto para la integridad de los datos.

Resumen de Riesgos

1	2	1	2	10
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	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS

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 — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- 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)**
  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

[CRITICAL] Conexion SSL: No se pudo establecer una conexión cifrada, lo que permite que cualquier dato transmitido sea capturado en texto plano.
[HIGH] HTTP a HTTPS redireccion: El servidor responde con éxito en conexiones no seguras sin forzar el cifrado, facilitando ataques de hombre en el medio.
[HIGH] Puerto 21 (FTP) ABIERTO: El servicio de transferencia de archivos está expuesto y no utiliza cifrado, permitiendo el robo de credenciales de acceso.
[MEDIUM] Puerto 22 (SSH) ABIERTO: Existe una interfaz de acceso remoto segura activa que, al estar expuesta públicamente, es susceptible a ataques de fuerza bruta.
[HIGH] Cabeceras de Seguridad: No se detectaron cabeceras HTTP de protección, dejando el sitio vulnerable ante ataques de inyección y suplantación de identidad.
[LOW] robots.txt: El archivo de directrices para buscadores no es accesible, lo que impide un control adecuado del rastreo web.
[LOW] sitemap.xml: La ausencia de un mapa del sitio dificulta la auditoría de rutas y la indexación correcta de la estructura web.