EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://noujoc.cat	Checks	9 pruebas
Dominio	noujoc.cat	Hallazgos	15 totales
Fecha	11 de agosto de 2026 a las 09:22	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio noujoc.cat ha dado como resultado una puntuación de 73/100, lo que equivale a una nota de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 1 resultó satisfactorio, no se detectaron advertencias y se registró 1 fallo crítico en la configuración de archivos base. No obstante, se detectaron múltiples errores técnicos que impidieron validar protocolos esenciales como el cifrado SSL/TLS y las cabeceras de seguridad. Debido a la incapacidad de establecer una conexión segura y la falta de visibilidad sobre los mecanismos de protección de datos, se concluye que el sitio es actualmente vulnerable. Se requiere una intervención técnica inmediata para garantizar la integridad de la plataforma.

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] Fallo de conexión SSL/TLS: No se pudo establecer una conexión cifrada, lo que impide proteger el intercambio de información entre el usuario y el servidor.
[CRITICAL] Ausencia de cabeceras de seguridad: El servidor no proporciona cabeceras críticas de respuesta, facilitando ataques de inyección y exposición de datos.
[HIGH] Error en redirección HTTPS: La falta de una redirección automática hacia protocolos seguros expone a los visitantes a conexiones vulnerables.
[MEDIUM] Configuración de cookies indeterminada: La imposibilidad de verificar los atributos de seguridad en las cookies supone un riesgo potencial para el secuestro de sesiones.
[LOW] Ausencia de archivos robots.txt y sitemap.xml: El error al acceder a estos archivos indica una configuración de servidor incompleta o permisos restrictivos incorrectos.