1. Table : scans

Champ	Type	Description
id	INT (Primary Key)	Identifiant unique du scan
tool	VARCHAR(32)	Nom de l'outil utilisé (ex: Nessus)
target	VARCHAR(255)	Cible analysée (IP, domaine, plage réseau)
start_time	DATETIME	Heure de début du scan
end_time	DATETIME	Heure de fin du scan
status	ENUM('running','done','error')	Statut du scan
created_at	DATETIME	Date de création de l'enregistrement

2. Table : findings

Champ	Type	Description
id	INT (Primary Key)	Identifiant unique de la faille
scan_id	INT (Foreign Key)	Référence au scan associé
severity	ENUM('LOW','MEDIUM','HIGH','CRITICAL')	Niveau de gravité de la faille
title	VARCHAR(255)	Titre de la faille détectée
description	TEXT	Description détaillée de la vulnérabilité
target	VARCHAR(255)	Système ou service concerné
cve	VARCHAR(64)	Identifiant CVE associé (s'il existe)
evidence	TEXT	Preuve ou trace de la vulnérabilité
raw_data	MEDIUMTEXT	Données brutes du rapport Nessus
plugin_id	INT	Identifiant du plugin Nessus
cvss	DECIMAL(3,1)	Score CVSS de la faille
port	INT	Port concerné
protocol	VARCHAR(8)	Protocole utilisé (TCP/UDP)
created_at	DATETIME	Date d'enregistrement

3. Table : scan_exports

Champ	Type	Description
id	INT (Primary Key)	Identifiant unique du fichier exporté
scan_id	INT (Foreign Key)	Scan auquel appartient le fichier
file_type	ENUM('csv','nessus','json')	Type de fichier exporté
file_id	INT	Identifiant du fichier dans l'API Nessus
storage	VARCHAR(512)	Chemin ou URL de stockage du fichier
created_at	DATETIME	Date de création de l'enregistrement

Exemple de données

Table	Exemple de données
scans	1 | Nessus | 192.168.1.0/24 | 2025-11-10 10:00 | 2025-11-10 10:15 | done
findings	1 | scan_id=1 | HIGH | Apache vulnérable | CVE-2021-41773 | port 80/tcp
scan_exports	1 | scan_id=1 | type=csv | file_id=123 | /exports/scan1.csv