Database Structure

user information, login, personal information
1. users
user_id (PK)
name
email
role (corporate_employee, university_student, it_staff, incident_responder, security_manager)
created_at

the game name, and its content and text
2. games
game_id (PK)
game_name (e.g., "Phishing Detection", "Firewall Config", "Incident Response")
description
acceptance_criteria

the clear conditions of the game how we will decide whether or not the user finished the game
3. challenges
challenge_id (PK)
game_id (FK → games)
challenge_type (phishing, firewall, incident_response)
content (the email text, firewall config task, or IR scenario step)
correct_answer (could be text/JSON depending on challenge)

session specific data
4. game_sessions
session_id (PK)
user_id (FK → users)
game_id (FK → games)
start_time
end_time
score (percentage or numeric score)
completed (boolean)

user responses in the game
5. responses
response_id (PK)
session_id (FK → game_sessions)
challenge_id (FK → challenges)
user_answer
is_correct (boolean)
response_time (time taken to answer)

user analytics
6. analytics
analytics_id (PK)
user_id (FK → users)
game_id (FK → games)
avg_score
avg_completion_time
top_failed_challenges (could be a JSON/text array of challenge IDs)
Last_updated

Data Flow Chart