COMP3335:DATABASE SECURITY PROJECT

Group#1

Project Setup Instructions

Prerequisites

- Ensure the following tools are installed on your computer: Docker, Python, Pip.
- Ensure your user has the necessary permissions to execute Docker commands.

Steps to Set Up the Project

1. Navigate to the COMP3335-TermProject folder on your computer. Open the folder with your preferred IDE (e.g., Visual Studio Code) or terminal.

2. Install the requirements (Tip: Please create a new python environment for this project by Conda or Venv):
   pip install -r requirements.txt

3. Run the following command to build and start the Docker containers:
   docker-compose up -d –build

4. If every container is either *Healthy* or *Started,* please open another terminal and do below for our alert system to work.
   python alert_page.py

5. To test the Alert System, simulate attacks by running the simulate_attack.py script in another terminal:
   python simulate_attack.py

Access the System Components

1. **Website**: : URL: http://localhost/
2. **phpMyAdmin** : URL: http://localhost:8081/
3. **Grafana** (Monitoring Dashboard): URL: http://localhost:3000/dashboards (username: admin, password: admin)
4. **Alert System**: URL: http://localhost:3200/alerts

How to Use Our Website

Our website offers different dashboards and functionalities based on the type of user. To simplify testing and exploration, we have provided pre-configured accounts for three types of users: **Patient**, **Lab Staff**, and **Secretary**. Each type of user has access to specific features and dashboards.

Go to Website: http://localhost/

User Accounts

Below is a list of user accounts. Each account is pre-configured with the password 123456 for ease of use.

Patient Accounts

Patients can view their test results, appointments, and billing information.
patient_1@gmail.com - 123456
patient_2@gmail.com - 123456
patient_3@gmail.com - 123456

Lab Staff Accounts

Lab Staff can manage test orders, input test results.
labStaff_1@gmail.com - 123456
labStaff_2@gmail.com - 123456

Secretary Accounts

Secretaries are responsible for managing appointments, and handling billing-related tasks. They can also see test results to print out.
secretary_1@gmail.com - 123456
secretary_2@gmail.com - 123456

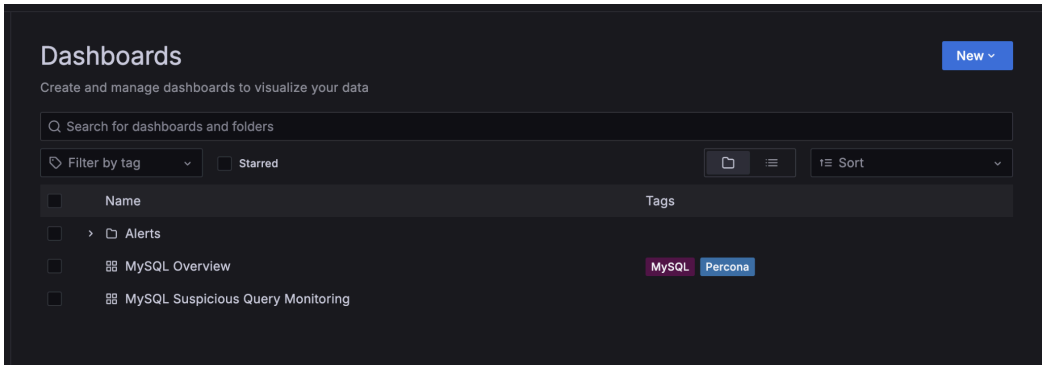
For comprehensive information about our webpage, its functionalities, and detailed explanations, please refer to our **Report**.

How To Use Grafana

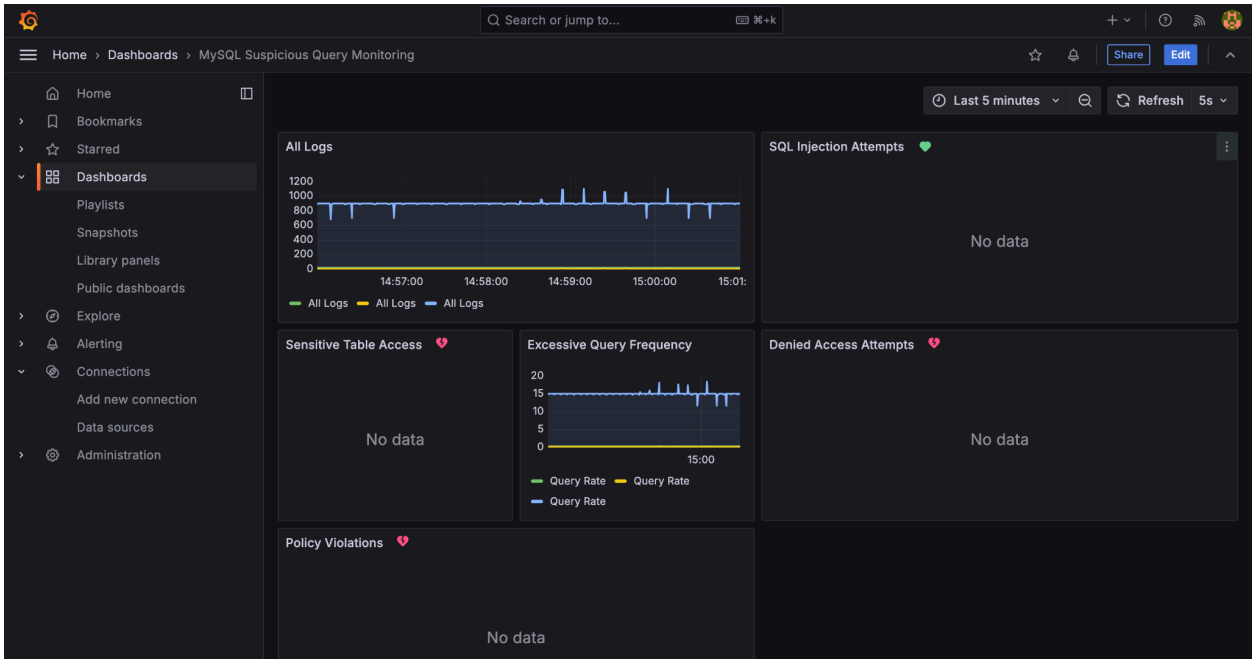
Grafana is a monitoring and analytics platform that provides insights into the system's activities. In this project, Grafana is used for monitoring suspicious MySQL queries and visualizing activity data. Follow the steps below to access and explore Grafana.
Log in to the Grafana with the information that are given below:
Grafana (Monitoring Dashboard): URL: http://localhost:3000/dashboards (username: admin, password: admin)

Dashboards

Grafana provides two types of dashboards to monitor activities, you can visit both:



For MySQL Suspicious Query Monitoring dashboard, if you did not run the *simulate_attack.py script (*as stated in Step 6 of the Setup Instructions). You'll see below page:



Once you run the simulate_attack.py script in another terminal, Grafana will start showing suspicious MySQL queries on the dashboard.

- To clearly see the latest activity, set the time filter in Grafana:
    - **Recommended Time Periods**: Last 5 minutes or 10 minutes.
    - You can adjust this in the top-right corner of the dashboard interface.

How To Use Alert System

The Alerts System is a crucial part of the project, designed to display notifications about suspicious activities detected in the system. After running the necessary scripts to simulate attacks (see Steps 5 and 6 in Setup Instructions), you can access the Alerts System to view these alerts.