Semester Project

DATABASE SYSTEM

Submitted by: Muhammad Ammar Kalim (242776)

Muhammad Abdullah Nasir (242779)

Section: BsCs_2B

Submitted to: Ms. Kainat Nazir

Deadline: 01-06-2025

Cyber Threat Tracker

A Comprehensive Database Management System for Cyber Threat Reporting and Analysis

1. Introduction

Overview

Cyber Threat Tracker is a web-based system designed to help users and organizations report, track, and manage cyber threats in a secure and organized way. It allows different types of users—such as students, IT professionals, and government employees—to submit reports about threats they encounter, including malware, ransomware, or suspicious online activity.

The system also provides a powerful admin panel where administrators can manage all users, view reported threats, send out alerts, and monitor system activity through logs. This helps keep the platform safe and reliable. By using this system, cybersecurity awareness can be improved, and users can take faster action to respond to new and ongoing threats. It creates a shared environment where information about threats is stored in one place and can be easily accessed when needed.

Goals

- Central platform to share cyber threat information.
- Role-based access for different types of users.
- Easy reporting, tracking, and viewing of threats.
- Secure system with logs of all important actions.

---

2. System Analysis

Users

- **Students**: Can submit and search threats.
- **IT Professionals & Government Staff**: Can analyze and report threats.
- **Admins**: Manage users, threats, alerts, and logs.

Main Functions

- Register and login users.
- Submit, view, search, and manage threats.
- Send alerts to all users.
- Track actions in logs.

(Insert Use Case Diagram here)

---

3. System Design

Architecture

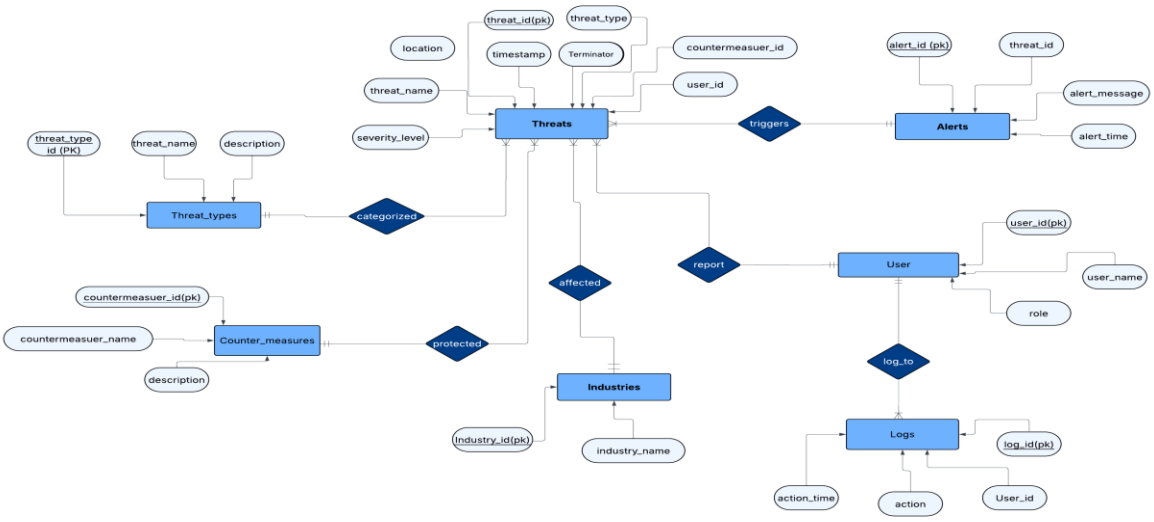
- **Frontend**: HTML, CSS+ Bootstrap
- **Backend**: PHP
- **Database**: MySQL

Entities

System uses the following main tables:

- Users
- Threats
- Alerts
- Logs
- Countermeasures
- Industries
- Threat Types

Erd diagram



---

4. Database Design

Table 1: users

Stores all registered users.

Column	Type
user_id	INT, Primary Key
full_name	VARCHAR(255)
username	VARCHAR(100)
email	VARCHAR(255)
password	VARCHAR(255)
user_role	ENUM
created_at	DATETIME

Table 2: threats

Stores details of reported threats.

Column	Type
id	INT, PK

Column	Type
threat_name	VARCHAR(255)
description	TEXT
severity	VARCHAR(50)
affected_industry	VARCHAR(100)
reported_date	DATE
submitted_by	VARCHAR(100)

Table 3: alerts

Stores system alerts.

Column	Type
id	INT, PK
title	VARCHAR(255)
message	TEXT
type	VARCHAR(50)
created_at	DATETIME

Table 4: logs

Stores action history of users.

Column	Type
log_id	INT, PK
user_id	INT, FK
action	VARCHAR(255)
action_timestamp	DATETIME

Table 5: countermeasures

Stores solutions or actions taken to prevent threats.

Column	Type
countermeasure_id	INT, PK
countermeasure_name	VARCHAR(255)

Column	Type
description	TEXT

Table 6: industries

Stores industry names affected by threats.

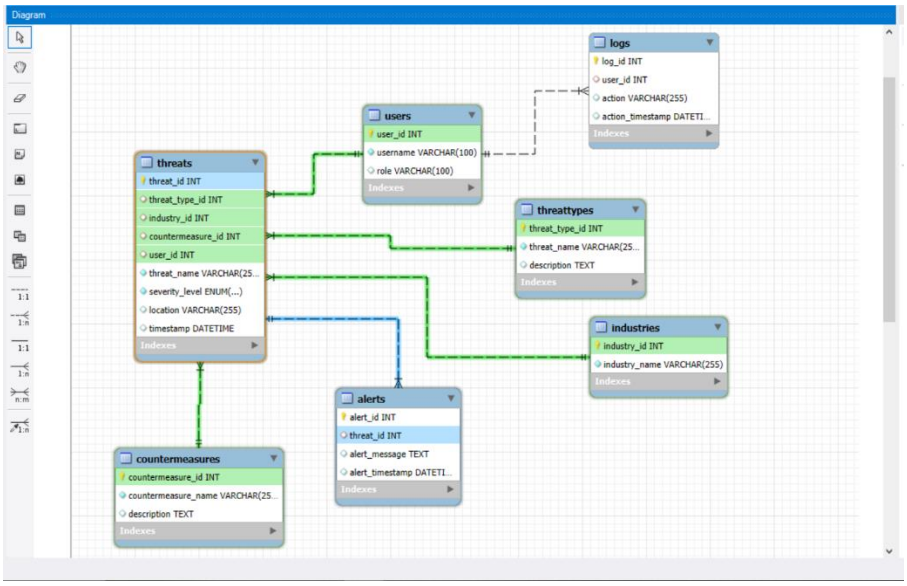
Column	Type
industry_id	INT, PK
industry_name	VARCHAR(255)

Table 7: threattypes

Stores different types of threats.

Column	Type
threat_type_id	INT, PK
threat_name	VARCHAR(255)
description	TEXT

Relational schema

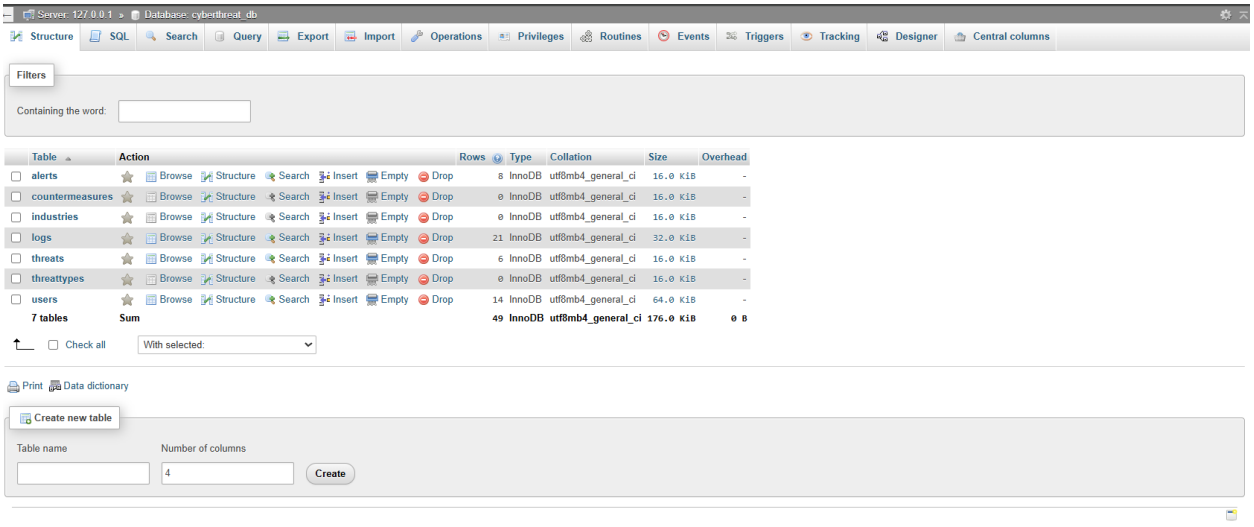


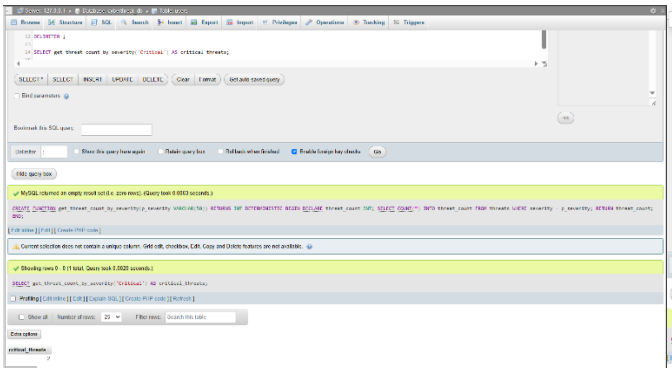
Normalization

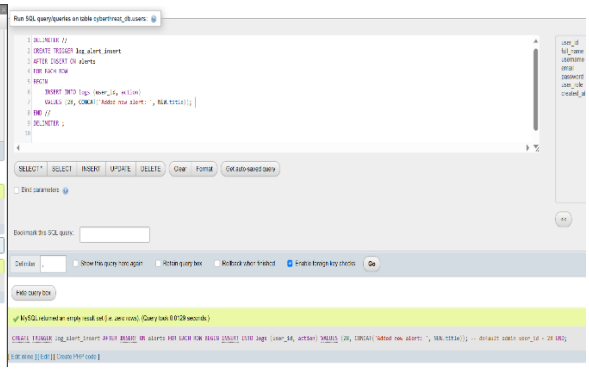
All tables are in 3rd Normal Form (3NF):

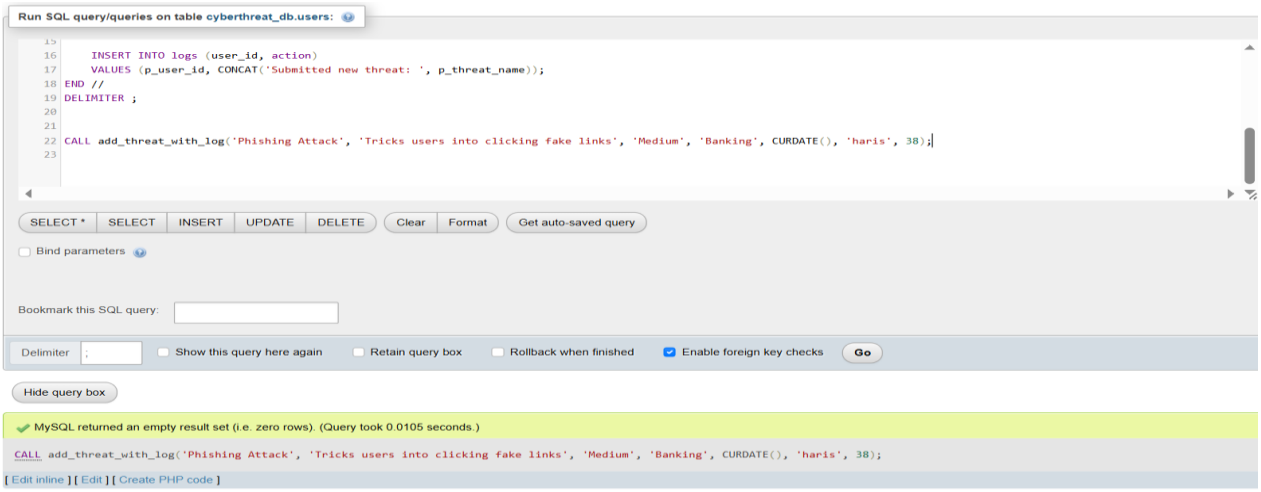
- No duplicate or repeating data.
- Each table has a unique primary key.
- All columns depend only on the primary key.

Database Screenshots









---

5. Implementation

Main Features

- **Login/Register**: For users and admins.
- **Threat Management**: Add, update, delete threats.
- **Alert Management**: Admins can create alerts for users.
- **User Management**: Admins can view and manage users.
- **Log History**: Every action is recorded for tracking.

Tools Used

- XAMPP for local server.
- PHP for backend code.
- MySQL for database.
- HTML, CSS, Bootstrap for responsive design.

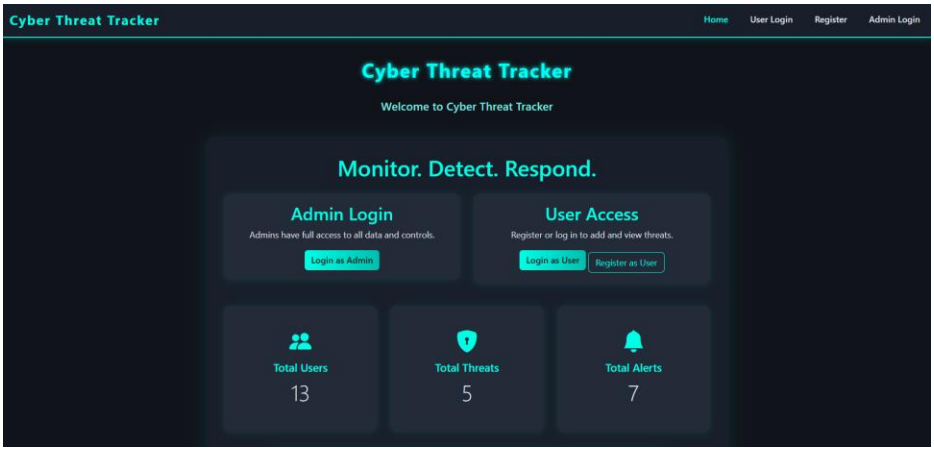
---

6. User Guide

How to Use the System

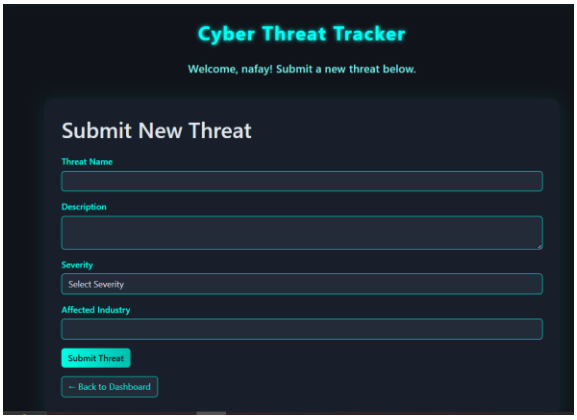
1. Register / Login

- Open the website and click "Register".
- After registration, log in using your username and password.



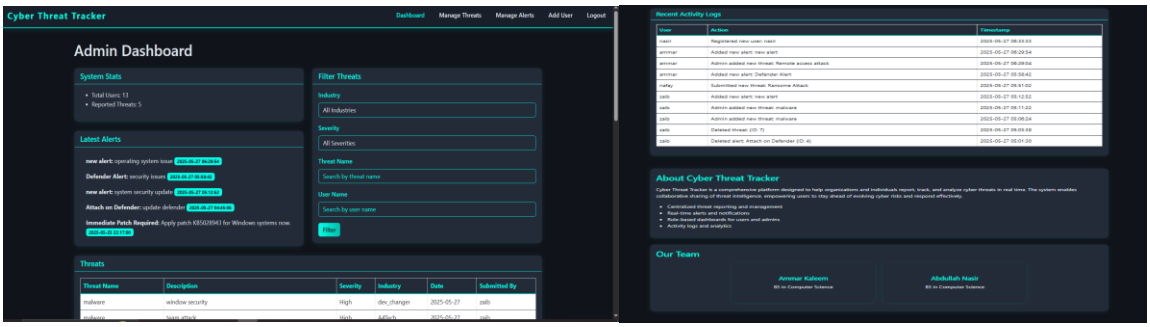
2. Submit a Threat

- Click on "Add Threat".
- Fill in the threat name, description, severity, and submit.



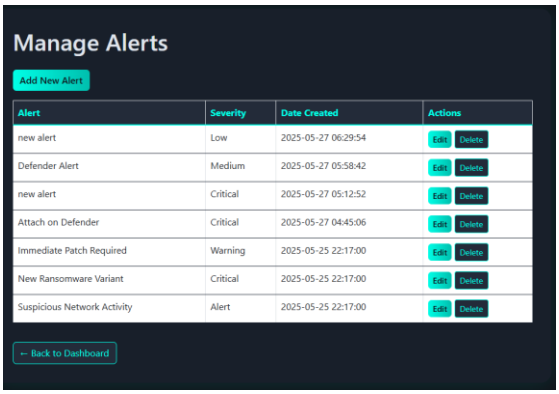
3. Admin Dashboard

- Admins can log in to see the dashboard.
- They can manage users, threats, alerts, and logs.



4. View Alerts and Logs

- Users can view system alerts.
- Admins can view all logs from the dashboard.



---

7. Conclusion

Summary

This project helps people report and manage cyber threats in one place. It is useful for both regular users and admins. Users can add and search for threat information, while admins can control everything and make the system safe.

The system is simple to use, works well, and supports different types of users. It also saves all actions in logs, which helps in checking any activity in the system.

Even though the system works fine, there are still some features that can be added later, like password reset, charts, or email notifications. These changes can make the system even better in the future.

Overall, **Cyber Threat Tracker** is a good step toward making cyber threat sharing and response faster, easier, and more organized.

Limitations

- No password reset feature.
- No analytics or charts.
- No email verification.

Future Work

- We will add graphs and data dashboards.
- Allow email notifications also.
- Add mobile support.
- In future we also provide solutions for these attacks through our web.

---

8. Deliverables

- Full PHP source code.
- SQL file with all tables.
- This documentation.
- Screenshots and ERD.

9. Github Link

https://github.com/AmmarKalim/DataBase-Project-cyberthreat_Tracker