GEETHANJALI COLLEGE OF ENGINEERING AND TECHNOLOGY
(Autonomous)

Cheeryal (V), Keesara (M), Medchal Dist., Telangana - 501 301

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MAJOR PROJECT ABSTRACT
IV B.Tech. I SEM CSE - C Section

BATCH NUMBER: C7	Major Project	Academic Year: 2024-2025

PROJETC TITLE: API Logging and Monitoring for Security Events

TEAM MEMBERS:

S.No.	Roll Number	Student Name	Mail Id	Contact Number
1.	21R11A05A5	Abburi Bhavya Sri	21r11a05a5@gcet.edu.in	9515351352
2.	21R11A05B5	Busholla Srinath	21r11a05b5@gcet.edu.in	9550457871
3.	21R11A05C8	Kosuru Bharath Kumar	21r11a05c8@gcet.edu.in	9010018199

GUIDE DETAILS:

Name of the Guide	Dr. S. Radha
Designation	Associate Professor
Department	CSE
Mail ID	radhacse@gcet.edu.in
Contact Number	9849166200

Signature of the Project In-charge ***Signature of the Guide with Date*** ***Signature of the Project Coordinator***

ABSTRACT

In today's digital landscape, Application Programming Interfaces (APIs) serve as critical components in enabling communication between systems, applications, and services. However, the widespread use of APIs also brings about significant security challenges, as APIs are increasingly targeted by attackers aiming to exploit vulnerabilities. This project focuses on designing and implementing a robust logging and monitoring system tailored specifically for API security. The system aims to track, record, and analyze security-related events within APIs to ensure the detection and quick response to potential threats. By leveraging real-time logging, integration with monitoring tools like Prometheus and Grafana, and setting up automated alerts for suspicious activities, this project aims to create a secure and resilient environment that allows API developers and administrators to proactively manage and respond to security incidents. The goal is to provide a comprehensive solution that not only secures API interactions but also aligns with modern Security Information and Event Management (SIEM) practices.

Objective:

1. Real-Time Security Tracking: Log critical security events to detect threats proactively.
2. Integrated Monitoring: Use Prometheus and Grafana for visualizing API security metrics.
3. Automated Alerts: Trigger alerts for high-risk activities to ensure swift response.
4. SIEM Compliance: Align logging practices with SIEM standards for robust security.

Commercializable: Yes

References:

1. https://ieeexplore.ieee.org/document/9645216
2. https://www.getknit.dev/blog/api-monitoring-and-logging
3. https://blog.shiftleft.io/api-security-101-insufficient-logging-and-monitoring-87a8e5996e36
4. https://www.pynt.io/blog/owasp-top-ten-blogs/the-matrix-chronicles-api-security-and-the-battle-for-sufficient-logging-and-monitoring

Date of Submission: 30-10-2024

Signature of the Guide with Date

Signature of the Project In-charge