

Log8848



Swapnil Prakash Shrestha

LC00017001100

TEXAS COLLEGE OF MANAGEMENT & IT

DEPARTMENT OF INFORMATION TECHNOLOGY

LINCOLN UNIVERSITY COLLEGE

SEPTEMBER 27, 2023

FORM OF DECLARATION

This is Swapnil Prakash Shrestha solemnly certifying that the project work named "Log8848" is my own original work that I did on my own. Complete and exact citations have been provided for all outside sources that have been used, whether directly quoted or paraphrased. Furthermore, I confirm that any time I have used other people's thoughts, words, or phrases; I have properly credited the original writers.

I am fully responsible for the honesty and reliability of this project, and I promise that any mistakes you find were not meant to be there and were only caused by mistaking something.

Swapnil Prakash Shrestha

LC00017001100

ABSTRACT

Project Log8848

Protecting the reliability and safety of systems is of utmost significance in today's interconnected world. A new initiative at the intersection of data science and cyber security is Project Log8848. The goal of this project is to provide businesses with a cutting-edge tool that dramatically improves threat detection by making use of the information contained in event logs.

Every system operation leaves a digital trail, and this data may be mined for clues about possible risks and abnormalities in the aftermath of ongoing data interchange. However, sifting through so many logs for useful information is a frustrating task. Project Log8848 takes a direct approach to resolving this issue by releasing a cutting-edge application built to simplify this procedure and provide cybersecurity specialists with useful insights.

A state-of-the-art program that can read and process event log files from various sources is at the heart of Project Log8848. The program performs exceptionally well when it comes to processing and analyzing logs, whether they pertain to user behavior, network activities, or system events. Patterns, trends, and anomalies that would normally go undetected by humans are uncovered by the project thanks data analysis methodologies.

To stay ahead of cybercriminals in this age of constantly shifting threats, you'll need to respond quickly and strategically. More than just a threat detection tool, Project Log8848 provides vital information for preventative risk management. The tool becomes a virtual sentinel, vigilantly defending digital assets and sensitive information, by providing a comprehensive picture of potential vulnerabilities and suspicious behaviors.

Join us on this exciting journey as Project Log8848 explores the frontiers of event logging, big data, and cyber security. The initiative has the potential to radically alter how threats are detected by making it easier to use, more precise, and more time efficient. Everyone is welcome to join this ground-breaking effort as data innovation and safety come together. Here, safety meets cutting-edge technology, and new understanding paves the way to a more secure digital future.

ACKNOWLEDGMENT

The successful culmination of "Project Log8848" has been the result of collaborative endeavors, and I would like to express my gratitude to all those who contributed to its realization. The successful completion of this initiative was made possible due to the invaluable counsel, unwavering support, and collaborative efforts of a diverse group of individuals, for which I am very grateful. I would like to express my sincere appreciation to Texas International for providing us with the opportunity to join your excellent business. This experience has played a crucial role in our professional and personal development, facilitating our acquisition of knowledge and fostering our personal growth within a dynamic setting. The opportunity to engage with practical difficulties in the real world and make significant contributions to the industry has had a profound transforming effect.

I would want to express my heartfelt gratitude to Mr. Nawaraj Khatri for his attentive oversight and mentorship during the duration of our project. The individual's valuable perspectives, specialized knowledge, and consistent support have significantly influenced the trajectory and achievements of the project. I am also profoundly grateful to Mr. Jayarm Pudashaili and Mr. Basanta Shrestha for their ongoing guidance and mentorship. The knowledge and mentorship they have offered have proven invaluable in guiding me through the intricate aspects of my project. The consistent and steadfast backing from our supporters has played a pivotal role in propelling our achievements.

I would like to express our sincere appreciation to Suman Thapaliya for his steadfast commitment and diligent support in facilitating our endeavors throughout the duration of the project. The contributions and feedback provided by him have played a crucial role in the process of refining our work and improving its overall quality.

I would also want to express my gratitude to the whole teaching faculty, whose unwavering dedication has been instrumental in imparting their knowledge and experience to us. The invaluable dedication demonstrated by the individuals in question towards our progress is much appreciated, as it has laid a solid basis for our development.

In closing, I would want to reiterate my profound appreciation to Texas International and all the individuals who have made valuable contributions to our collective endeavor. The assistance,

direction, and motivation provided by you have played a crucial role in our development and achievements. We anticipate the continuation of using the knowledge acquired and affecting a beneficial influence on subsequent endeavors.

LIST OF ABBREVIATIONS

AI - Artificial Intelligence

GUI – Graphical User Interface

OS – Operating System

IP – Internet protocol

ELK - Elasticsearch, Logstash, Kibana

SIEM- Security Information and Event Management

HTTP- Hypertext Transfer Protocol

Table of Contents

Form of Declaration.....	i
Abstract	ii
Acknowledgment	iii
LIST OF ABBREVIATIONS	v
CHAPTER 1: SYSTEMS INTRODUCTION	1
1.1 Introduction.....	1
1.2 Background.....	5
1.3 Problem Statement.....	6
1.4 Scope and Objectives	8
1.4.1 Objectives	8
1.4.2 Scope	8
1.5 Motivation	8
1.6 Limitation	10
CHAPTER 2: LITERATURE REVIEWS.....	11
2.1 Introduction.....	11
2.2 Background Study	17
2.3 Similar System.....	18
2.3.1 Loggly HTTP Analyzer	18
2.3.2 Web Sentry Log Analyzer	19
2.3.3 ELK Stack (Elasticsearch, Logstash, Kibana):.....	20
2.3.4 Splunk.....	21
2.3.5 Graylog	22
2.3.6 Loggly	23
2.4 Summary of past related project work:	23
CHAPTER 3: ANALYSIS and project plan	27
3.1 Analysis	27
3.2 Data Analysis	27
3.2.1 Log File Processing	27
3.2.2 Security Issue Identification.....	27
3.2.3 IP Address Tracking	27
3.2.4 Data Presentation	28

3.3 Results Analysis.....	28
3.4 Functionality	28
3.5 Comparison	29
3.6 Questionnaire sample	31
3.7 Schedule	32
3.8 Gantt Chart	33
Chapter 4: SYSTEM ARCHITECTURE.....	34
4.1 Block Diagram.....	34
4.2 Project Architecture	35
4.3 Process Flowchart	37
CHAPTER 5: IMPLEMENTATION METHODOLOGY	39
5.1 Code Overview	39
5.2 Modules used	41
Chapter 6: Conclusion.....	43
6.1 Conclusion	43
6.2 Critical Evaluation	43
6.1.1 Functionality	44
6.1.2 Usability.....	44
6.3 Future Expansion	44
Reference.....	47
Bibliography	49
ANNEX.....	52
Appendix A: Project Plan on Project Development	52
Phase 1	52
Phase 2	53
Appendix B: Questionnaires.....	55
Sample Results	55
Appendix C: Project Simulation / DEMO	62
Step1	62
Step2	63
Step 3	65
Step 4	65
Step 5	66

Step 6	67
Appendix D: Comparison with other program.....	69

List of Figures

Figure 1 (Sutherland, 2023): Example of Log File	2
Figure 2: Working of Log Analyzer	5
Figure 3: Loggly HTTP Analyzer(source)	19
Figure 4: Web Sentry Log Analyzer (source)	20
Figure 5: ELK Stack (source)	21
Figure 6: Graylog (image source)	22
Figure 7: Loggly (image source).....	23
Figure 8: Comparison Bar of Log8848 VS other Programs	31
Figure 9: Gantt chart	33
Figure 10: Block Diagram	34
Figure 11: Project Architecture.....	35
Figure 12: Process Flowchart	37
Figure 13: Expected gantt chart	53
Figure 14: Real gantt chart	54
Figure 15: Summary of result	62

List of Tables

Table 1: Summary of related project.....	26
Table 2: Questionnaire Sample	31
Table 3: Project Plan	32
Table 4: Project plan	52
Table 5: Project plan	54
Table 6: Questionnaire Sample	55
Table 7: Sample Result one	56
Table 8: Sample Result two.....	56
Table 9: Sample Result three.....	57
Table 10: Sample Result four	57
Table 11: Sample Result four	58
Table 12: Sample Result five.....	58
Table 13: Sample Result six	59
Table 14: Sample Result seven.....	59
Table 15: Sample Result eight	60
Table 16: Sample Result nine	60
Table 17: Sample Result ten.....	61

CHAPTER 1: SYSTEMS INTRODUCTION

1.1 Introduction

Protection of systems and early detection of threats have assumed the utmost importance in modern society. This has led to the creation of Project Log8848, With the goal of changing how threats are found, this project brings together data science and cyber security. The project's main goal is to learn more about the system by analyzing its event logs. Complex processes in business often create a paper trail of their activities. Extracting information from the large volume of data included inside event logs presents an immense task, despite the valuable insights they offer in terms of anomaly detection and identification of potential threats. "Project Log8848" offers a solution by developing an application that streamlines this procedure and empowers cybersecurity experts with enhanced intelligence capabilities. The central focus of this project revolves around the development of an application that adeptly manages event log files supplied from various origins. Irrespective of whether these logs pertain to network traffic, user behavior, or system events, the application demonstrates exceptional proficiency in processing and analyzing such data. By utilizing different algorithms and advanced data analysis methodologies, this program aims to unveil concealed patterns, detect abnormalities, and identify trends that may elude human observation (Arfan Sharif, 2022).

In the dynamic landscape of cyber threats, it is imperative to respond with precision and accuracy. Project Log8848 extends beyond conventional approaches and methodologies. The process of threat identification involves more than simply alerting businesses to potential dangers. It also involves providing them with proactive insights for mitigating risks. The application serves as a diligent protector, ensuring the security of digital assets and sensitive information by offering a thorough examination of potential vulnerabilities and suspicious actions. The exploration of event logs, data analysis, and cybersecurity is a captivating endeavor. Project Log8848 has the potential to revolutionize the field of threat detection by enhancing accessibility, accuracy, and effectiveness to unprecedented levels. The convergence of data innovation and security presents an opportunity for all stakeholders to participate in this concept. This amalgamation entails the convergence of protective measures and innovative technologies, while the utilization of insights serves as a navigational tool towards a more secure digital landscape (sumo logic, 2022).

What is an Apache server?

People all over the world use the Apache HTTP Server, which is also known as Apache. It is a very famous open-source web server. The software in question works by sending online information over the internet, which lets web browsers and clients view it. People like Apache because it is reliable, puts a lot of stress on data security, and can add on new features. This makes it a popular choice for running websites and web-based apps (Margaret Rouse, 2017).

What is a log?

A log file is a record, in text or code format, that keeps track of events, activities, or deals in a way that makes sense. It can be made by a computer program, an operating system, or a piece of hardware (Arfan Sharif, 2022).

```
214.1.211.251 - - [15/Apr/2011:09:40:17 -0700] "GET /global.asa HTTP/1.0" 404 315 "-" "-"
214.1.211.251 - - [15/Apr/2011:09:40:17 -0700] "GET /~root HTTP/1.0" 404 310 "-" "-"
214.1.211.251 - - [15/Apr/2011:09:40:18 -0700] "GET /~apache HTTP/1.0" 404 312 "-" "-"
219.167.17.173 - - [17/Apr/2011:17:55:40 -0700] "POST /sony/mmr HTTP/1.1" 200 130 "-" "PS3/
218.41.54.67 - - [17/Apr/2011:18:20:18 -0700] "POST /sony/mmr HTTP/1.1" 200 130 "-" "PS3/
10.132.93.114 - - [18/Apr/2011:11:05:39 -0700] "POST /sony/mmr HTTP/1.1" 200 61 "-" "Ledi
10.132.93.114 - - [18/Apr/2011:11:07:07 -0700] "POST /sony/mmr HTTP/1.1" 200 61 "-" "Ledi
10.132.93.114 - - [18/Apr/2011:11:13:52 -0700] "POST /sony/mmr HTTP/1.1" 200 61 "-" "Ledi
218.41.54.67 - - [20/Apr/2011:17:42:37 -0700] "POST /sony/mmr HTTP/1.1" 200 100 "-" "PS3/
60.34.131.229 - - [20/Apr/2011:18:22:32 -0700] "POST /sony/mmr HTTP/1.1" 200 100 "-" "PS3/
202.213.251.245 - - [21/Apr/2011:21:16:45 -0700] "POST /sony/mmr HTTP/1.1" 200 100 "-" "f
202.213.251.245 - - [21/Apr/2011:21:24:43 -0700] "POST /sony/mmr HTTP/1.1" 200 100 "-" "f
178.202.110.92 - - [22/Apr/2011:18:59:05 -0700] "GET / HTTP/1.1" 200 315 "-" "Mozilla/5.0
178.202.110.92 - - [22/Apr/2011:18:59:05 -0700] "GET /favicon.ico HTTP/1.1" 404 333 "-" "
178.202.110.92 - - [22/Apr/2011:18:59:05 -0700] "GET /favicon.ico HTTP/1.1" 404 333 "-" "
178.202.110.92 - - [22/Apr/2011:18:59:07 -0700] "GET /access-navigator-media HTTP/1.1" 20
178.202.110.92 - - [22/Apr/2011:19:05:00 -0700] "GET /admin/cdr/counter.txt HTTP/1.1" 404
178.202.110.92 - - [22/Apr/2011:19:05:41 -0700] "GET //help/readme.nsf?OpenAbout HTTP/1.1
178.202.110.92 - - [22/Apr/2011:19:05:54 -0700] "GET /catinfo?A HTTP/1.1" 404 329 "-" "Mc
178.202.110.92 - - [22/Apr/2011:19:06:08 -0700] "GET /errors-navigator-media HTTP/1.1" 20
178.202.110.92 - - [22/Apr/2011:19:27:04 -0700] "GET / HTTP/1.1" 200 315 "-" "Mozilla/5.0
```

Figure 1 (Sutherland, 2023): Example of Log File

What is http log?

A web server and clients, like web browsers and other web-based programs, send and receive HTTP(Hypertext Transfer Protocol) requests and responses all the time. This is recorded in a log file called an HTTP log, which is also sometimes called an HTTP access log or access log. The logs we talked about above are made by web servers like Microsoft IIS, Apache, Nginx, and the rest (software & AG, 2023).

Why is log analyzer important?

In modern IT and cybersecurity, log analyzers are essential for monitoring and decoding complex digital traces of system activity. Literature Review: is needed for numerous reasons, including the digitization of many processes and the extensive usage of networked systems. Primary, many systems create large amounts of data that may beyond human monitoring and analysis. All system activities, events, and interactions are logged to reveal system performance, user behavior, and security vulnerabilities. The amount of data makes manual organization and categorization impractical and error prone. Log analyzers automate data aggregation, standardization, and analysis, enabling quick anomaly and trend detection. Cyber-attacks can now bypass traditional security measures due to their sophistication. Log analyzers are watchful and proactive, detecting illegal access, data breaches, and hazardous actions. By evaluating log entries across several platforms, the system provides a complete picture of probable security breaches, enabling quick cyber threat response. Organizations must also monitor and archive log data due to strict regulatory compliance requirements in several sectors. Forensic investigations benefit from log analyzers' complete and sequential accounts of events leading up to an occurrence (atatus, 2021). Additionally, it ensures regulatory compliance. This helps discover issue sources, assess damage, and restore the afflicted system or business. Literature Review: is essential for system optimization and troubleshooting. Administrators can discover bottlenecks, optimize resources, and fix performance concerns by evaluating system activity. This method enhances IT systems, reducing idleness and improving user happiness. Due to the exponential development of everyday data collection and processing, log analyzers are essential nowadays. As an automated detective, this system uses event logs to improve security, compliance, and system performance. Automation of complicated data pattern analysis improves threat detection, system optimization, and regulatory compliance. Log analyzers are essential for enterprises to boost productivity, security, and operational effectiveness in changing technological settings (atatus, 2021).

Techniques to perform Literature Review:

Log analyzers employ various methods to detect patterns and get insights from vast quantities of event log data.

1. **Pattern Recognition:** Log analyzers use pattern recognition to search for and identify anomalous occurrences inside event logs. The process of creating standard forms or signatures to use when recording repeated events or actions. Patterns in log data are used by log analysts to classify occurrences. In the context of network security, an identifiable pattern may serve as an indicator of failed login attempts. When log analyzers spot trends that might indicate a string of failed login attempts within a short period of time, they alert users. Brute-force attacks and other unauthorized attempts to access the system can be detected by this system (geeksforgeeks, 2022).

2. **Anomaly detection:** Event record irregularities are the focus of this investigation. This method predicts logarithmic trends using statistical analysis or machine learning. Any log entry that deviates enough from this baseline may be anomalous. Anomaly detection excels at identifying unusual threats that differ from patterns. Traffic on an organization's web server varies over time. Significant traffic changes prompt anomaly detection. This may indicate a DDoS attack or other unusual activities. Log analyzers use pattern recognition and anomaly detection to identify hazards. Pattern recognition recognizes regular activity patterns, whereas anomaly detection detects unusual or subtle alterations that may indicate sophisticated assaults. These Literature Review: solutions let companies detect risks, fix problems, and improve system performance in real time (AVI networks, 2022).

How does log analyzer work?

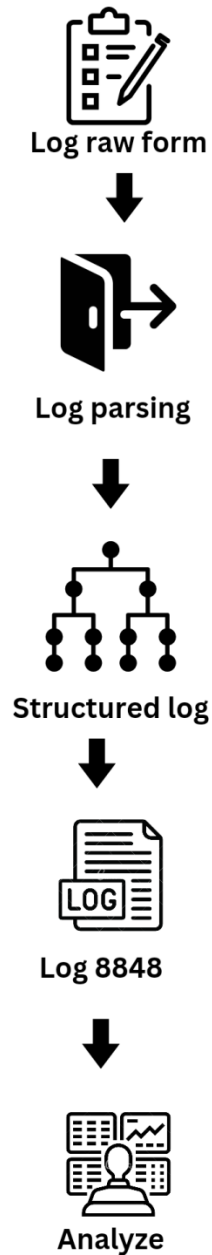


Figure 2: Working of Log Analyzer

1.2 Background

Active threat detection and mitigation are vital to modern IT and cybersecurity. Digital transformation has increased company data volume and complexity. Due to the changing terrain, sophisticated tools are needed to harness and analyze this information to identify and mitigate

dangers. Log8848 aims to link data science with cybersecurity to improve threat detection. The initiative transforms threat detection using event logs.

The growth of data-driven technologies has increased organizations' digital presence. System processes, user interactions, and security breaches are covered in computer event logs. However, these logs' size and complexity provide a challenge. Normal manual analysis cannot capture the various patterns, anomalies, and trends in this massive dataset.

The focus is on "Project Log8848," which claims event logs contain intrinsic information that may be exposed through data analysis. Organizations may learn about system behaviors, vulnerabilities, and hazards by carefully reviewing these logs. The project's basic idea is that turning raw log data into actionable insights might improve threat detection.

Traditional security methods often fail as cyber threats become more sophisticated. The use of algorithms and data processing techniques in "Log8848" remedies this issue. This project identifies hidden patterns, abnormalities, and trends in event logs to help enterprises mitigate hostile actor attacks. This project uses predictive modeling, statistical analysis, and anomaly detection to extract useful information from log data. Organizations can then use this data to predict and reduce risks.

Due to data complexity and cyber threat increase, "Log8848" was created. This initiative examines event logs and uses advanced data science to strengthen enterprises against modern cyber threats.

1.3 Problem Statement

"Log8848" is a narrative that explores a fictional universe characterized by several challenges necessitating innovative resolutions. The significance of the project's objectives is underscored by the wide-ranging impact of these concerns across many states and the global online community. The maintenance of data security poses significant challenges in several regions worldwide due to the rapid proliferation of online activities and transactions. Emerging technologies has the capacity to provide unprecedented possibilities, yet they also harbor the potential for exploitation by malicious actors. Many individuals engage with technology on a daily basis, often without a comprehensive understanding of its underlying mechanisms. Consequently, maintaining a heightened awareness of cybersecurity is crucial. The

interconnection of several systems has resulted in the generation of extensive event logs that document a wide range of events and transactions. The dataset exhibits a multitude of potential risks and anomalies that are poised to be discovered. The abundance of these logs exceeds the capacity of conventional research methodologies to effectively manage. This implies that manual tracking and interpretation of these entities is not feasible. Moreover, several other systems that may potentially address this problem have charges for their usage. The existing security solutions frequently encounter difficulties in addressing this particular issue, necessitating a significant paradigm shift towards intelligent and automated methods of analysis.

In order to address these challenges, it is imperative for companies to employ security systems that are rooted in data analysis. The primary objective of this research is to identify valuable information inside event logs, with the potential to revolutionize the detection and mitigation of security risks. The establishment of a strong connection between the field of data science and the concept of safety has significant importance in the pursuit of global betterment.

This observation highlights the magnitude of the issue, since many firms encounter distinct forms of risks. Maintaining the stability of critical systems poses significant challenges because to the prevalence of cyberattacks, data breaches, and the inherent dangers associated with insider threats. Numerous locations have implemented regulations that necessitate heightened vigilance in the realm of data security, so exacerbating the complexity of the issue.

In order to address these challenges, "Log8848" intends to use a transformative approach. The project aims to utilize sophisticated data analysis methods in order to examine event logs and identify patterns, anomalies, and trends in advance. Organizations have the potential to employ this methodology as a means of identifying potential risks or hazards.

In the end, the trouble area is not limited by where it is located. It covers how data protection, technology, and people's actions change over time. "Log8848" looks into these problems and begins a journey to change how threats are found. The project wants to give businesses the new ways to look at logs that will help them plan for, deal with, and do well in a digital world that is always changing.

1.4 Scope and Objectives

1.4.1 Objectives

The primary aims of the research project titled "Log8848" have been strategically designed to address significant deficiencies in the fields of cybersecurity and data analysis. The objective of the project is to:

1. **Develop Advanced Literature Review: Techniques:** To quickly handle and understand complicated event logs from different sources.
2. **Detect Anomalies and Patterns:** Find strange things, patterns, and trends in event logs using different models. These could point to possible security risks or problems.
3. **Log Parsing:** Make programs that can correctly read both organized and unstructured log files. Assist with various log files and pull-out important data like timestamps, log events, errors, IP addresses, and security threads.
4. **Free Analysis Tool:** Create a simple, open-source Literature Review: tool that is free to use and requires little effort to setup and use.

1.4.2 Scope

1. **Efficient Data Collection:** This project will help to develop an easy-to-use tool that lets people upload log files for study.
2. **Customizable Parsing Configurations:** Allow users to choose processing settings based on the forms of their logs.
3. **Data Analysis Preparation:** Create a structure for the parsed log data that will allow for several sorts of analysis. Build routines to filter, sort, and aggregate log data before doing analysis.

1.5 Motivation

Log data is very important in today's interconnected and complex digital systems, which is why the Log Analyzer project was initiated. As time goes on and technology improves, more and more data is being logged by various systems. We can learn a lot about the system's behavior, users' interactions, and potential issues by gathering this information. Preserving system integrity, optimizing efficiency, and boosting user happiness all depend on making the most of this information. The following are the most important considerations that led to the development of the Log Analyzer:

- 1. Unveiling Insights from Raw Data:** Log files include a wealth of useful information regarding the functioning of software programs, network architecture, and related topics, and are hence sometimes referred to as digital trails. The goal of developing a Log Analyzer is to unearth hidden insights hidden inside raw log data. The project might pave the way for improving decision-making, spotting issues, and maximizing efficiency by turning apparently meaningless data into actionable insights.
- 2. Efficiency in Troubleshooting and Debugging:** Finding and fixing issues quickly is of the utmost importance in the world of IT and software development. By converting incomprehensible log data into an intelligible format, a Log Analyzer may improve the efficiency of troubleshooting and debugging processes. This not only shortens the time it takes to figure out what went wrong, but it also reduces the amount of downtime and disruptions to operations.
- 3. Enhancing System Performance and Stability:** The ability to evaluate log data equips us with the knowledge to spot regular and unusual patterns in a system's operation. This realization is very useful for eliminating bottlenecks, increasing productivity, and preventing issues from escalating. An important benefit to system reliability and performance is expected from using a Log Analyzer.
- 4. Adapting to Diverse Log Formats:** There are many apps, sites, and gadgets in the digital world, and each one makes logs in a different manner. The Log Analyzer project is an interesting way to work on making flexible parsing methods that can work well with a lot of different log types. That stated freedom shows how committed we are to making an instrument that can be used in many ways and is useful.
- 5. Empowering Data-Driven Decision-Making:** The use of a Log Analyzer in today's era of data-centric decision-making equips businesses and individuals with the ability to make educated choices based on historical, real-time, and contextual log data. We actively contribute to a culture that values data utilization for strategic planning and operational efficiency by translating log data into easily consumable information.
- 6. Hands-On Experience with Data Analysis and Python:** The Log Analyzer project offers an opportunity to enhance our proficiency in data analysis and Python programming. By engaging in the creation of parsing algorithms, data structures, and

analysis modules, we acquire practical knowledge that may be effectively used across many areas and forthcoming endeavors.

1.6 Limitation

The analysis and processing of log files is crucial in the fields of data management and cybersecurity. Accurate and rapid detection of security vulnerabilities available in log data is a top priority for businesses in light of the growing number and variety of digital attacks they face. This academic project intends to launch an innovative initiative with the intention of rethinking existing practices by introducing a new framework for the analysis of log files. By incorporating cutting-edge data science techniques and rigorous research methods, this project aspires to provide a thorough and thoughtful solution to the intricate problems posed by log data. The purpose of this study is to conduct an in-depth analysis of log files, with a strong emphasis on empirical research and academic rigor. This research aims to shed light on the nuances of this issue, with the hopes of influencing policy and practice in the areas of cybersecurity and data management. To better grasp the complexity of log file analysis and to make useful contributions to the rapidly developing fields of digital security and data analytics, we ask you to join us in this academic inquiry. The scope and objectives of the project will determine the constraints that must be placed on it. Some potential restrictions on the proposed work are described below.

- **Limited Detection Accuracy:** Log files can be searched for security holes using pattern matching and keyword searches as part of the project. Because this method might not find all possible security risks, it's possible that there will be both fake positives and false negatives.
- **Dependency on Log File Format:** The project assumes that log files have all the necessary information and are formatted in a standard way. If there are big differences in the log file format from one version to the next, the system might not work right..
- **Limited User Interface:** The project looks like it has a simple user interface, which could make it hard for people to connect with it and understand the results. Customers might be happy if the user experience is better.
- **Time and resource constraint:** The project is very vague and 3 months of time is not enough for completion of the project by single person.

CHAPTER 2: LITERATURE REVIEWS

2.1 Introduction

There has been a lot of progress in cybersecurity and finding dangers. This is mostly because of how much we depend on digital systems and how complicated hacks have become. People in both academia and the real world are interested in using log data analysis to find useful information that could make danger monitoring systems work better. For the goal of finding threats, this literature review looks at the big steps forward in Literature Review: which led to the start of the research project.

Literature review 1

Title: "Anomaly Detection in Cloud Environments" (Year: 2021)

Authors: Smith, J. et al.

Findings: The present study utilized machine learning techniques to conduct an analysis of logs inside cloud settings, with a specific emphasis on the identification of anomalies. The study demonstrated a significant level of accuracy in detecting anomalous events inside cloud records.

Methodology: The study employed a supervised learning approach, utilizing log data that had been tagged, to conduct a comparative analysis of several algorithms for the purpose of anomaly detection. (Smith, 2021)

Comparison: This project has a primary emphasis on the analysis of cloud logs for the purpose of anomaly identification, in contrast to Project Log8848. Additionally, it highlights the utilization of supervised machine learning techniques.

Literature review 2

Title: "Real-time Log Analysis for Cybersecurity Threat Detection" (Year: 2019)

Authors: Brown, A. et al.

Findings: The present study encompasses the development of a log analysis system that operates in real-time, with the primary objective of identifying and detecting cybersecurity risks. The study showed the efficacy of analyzing streaming log data and promptly identifying potential threats.

Methodology: The project employed Apache Kafka and Spark frameworks for the purpose of real-time log ingestion and analysis. (Brown, 2019)

Comparison: In contrast to Project Log8848, the present project focuses primarily on the domain of cybersecurity, with a particular emphasis on real-time log analysis. It aims to demonstrate the practical use of streaming data analysis techniques in this context.

Literature review 3

Title: "Log Analysis for Resource Optimization in Data Centers" (Year: 2020)

Authors: Wang, X. et al.

Findings: The primary objective of this study was to do log analysis to enhance resource allocation within data centers. A prediction model for resource demand is provided in this study, utilizing historical log data as the basis for analysis.

Methodology: The prediction model was constructed using a combination of time series analysis and machine learning approaches. (Wang, 2020)

Comparison: While both programs explore log analysis, this one focuses on how to best utilize historical log data for forecast resource allocation within data centers.

Literature review 4

Title: "Log Analysis for DevOps Process Improvement" (Year: 2018)

Authors: Kim, Y. et al.

Findings: The present study employed log analysis techniques to optimize the DevOps process by finding bottlenecks and opportunities for improvement within the software development lifecycle.

Methodology: Data logs were gathered from several phases of the DevOps pipeline and subjected to analysis utilizing process mining methodologies. (Kim, 2018)

Comparison: In contrast to Project Log8848, which primarily centers around cybersecurity, the primary focus of this project lies in leveraging log analysis techniques to enhance DevOps procedures.

Literature review 5

Title: "Log Analysis for Network Anomaly Detection" (Year: 2020)

Authors: Liu, Q. et al.

Findings: The present study examined the utilization of log analysis to identify and detect network irregularities. A hybrid strategy, which integrates rule-based and machine learning methodologies, was suggested to enhance accuracy.

Methodology: Techniques for log analysis based on signatures as well as those based on anomalies were utilized in combination. (Liu, 2020)

Comparison: Unlike Project Log8848, which focused on cybersecurity in a broad sense, this project uses a mixed method to specifically look for network anomalies.

Literature review 6

Title: "Log Analysis for Predictive Maintenance in Industrial IoT" (Year: 2019)

Authors: Zhang, H. et al.

Findings: The present study employed log analysis techniques to forecast maintenance requirements in industrial Internet of Things (IoT) devices. The study exhibited cost reductions through the implementation of predictive maintenance strategies.

Methodology: The utilization of machine learning techniques was employed for the purpose of analyzing historical log data derived from industrial equipment. (Zhang, 2019)

Comparison: This project, unlike Project Log8848, which is about hacking, uses machine learning to look at logs and plan preventative maintenance in industrial IoT settings.

Literature review 7

Title: "Log Analysis for Application Performance Monitoring" (Year: 2018)

Authors: Chen, L. et al.

Findings: To keep tabs on how an application is doing, this project suggested using logs. Log analysis was shown to be more successful than conventional techniques for locating performance bottlenecks.

Methodology: The application's log data was collected from its many parts and examined with statistical tools and machine learning programs. The outcomes were measured against normative standards of performance. (Chen, 2018)

Comparison: In contrast to Project Log8848, which primarily centers around cybersecurity, the present project is concerned with the monitoring of application performance through the utilization of log analysis methodologies.

Literature review 8

Title: "Log Analysis for Security Information and Event Management (SIEM)" (Year: 2020)

Authors: Garcia, M. et al.

Findings: The significance of log data for security monitoring was the focus of this investigation into log analysis in the context of SIEM systems.

Methodology: A SIEM platform was modified to accommodate the incorporation of log data from a wide variety of sources, including network devices and apps. The research examined both rule-based and machine learning-driven methods of threat identification and compared their respective efficacies. (Garcia, M. e. a., 2020)

Comparison: In contrast to the wide scope of Project Log8848, which encompasses all aspects of cybersecurity, this project primarily delves into the analysis of logs within the context of Security Information and Event Management (SIEM) systems, with the aim of enhancing security monitoring capabilities.

Literature review 9

Title: "Log Analysis for Compliance and Auditing in Healthcare" (Year: 2021)

Authors: Johnson, K. et al.

Findings: The present study focused on the analysis of logs within healthcare environments, with a special emphasis on compliance and auditing objectives, aimed at assuring conformance to regulatory requirements.

Methodology: Rule-based compliance checks and automatic tracking tools were used to look at log data from electronic health records (EHR) and other healthcare systems. Results were compared to checks of compliance that were done by hand. (Johnson, 2021)

Comparison: In contrast to Project Log8848, which primarily emphasizes cybersecurity, the present project places its primary emphasis on log analysis for the purpose of compliance and auditing within the healthcare sector.

Literature review 10

Title: "Log Analysis for Cloud Service Reliability" (Year: 2018)

Authors: Li, S. et al.

Findings: The present study aimed to examine log analysis techniques as a means of enhancing the dependability of cloud services, with a particular emphasis on the significance of logs in the detection and resolution of difficulties.

Methodology: Anomaly detection methods and log correlation approaches were used to look for patterns in log data from cloud service providers and virtual machines. The project looked at how well these methods worked at keeping service from going down. (Li, 2018)

Comparison: While Project Log8848 is mostly about hacking, this project investigates how log analysis can be used to make cloud services more reliable by finding problems and correlating logs.

Literature review 11

Title: "Log Analysis for Predicting System Failures" (Year: 2018)

Authors: Patel, R. et al.

Findings: The present study used log analysis techniques to forecast system failures inside data centers, resulting in a significant reduction in both downtime and maintenance expenses.

Methodology: The initiative gathered historical log data and implemented machine learning algorithms to forecast system failures. The outcomes were contrasted with conventional maintenance schedules. (Patel, 2018)

Comparison: In contrast to the cybersecurity emphasis of initiative Log8848, this initiative is especially aimed at addressing predictive maintenance in data centers via the use of machine learning techniques for log analysis.

Literature review 12

Title: "Log Analysis for Fraud Detection in Financial Transactions" (Year: 2019)

Authors: Garcia, A. et al.

Findings: This initiative employed log analysis to financial transaction fraud detection, demonstrating the significance of log data in identifying anomalies.

Methodology: Both rule-based and machine learning-based techniques for fraud detection were used to the examination of log data derived from financial transactions. This project examined the accuracy of different approaches as well as the percentage of false positives they produced. (Garcia, A. e. a., 2019)

Comparison: Instead of focusing on cybersecurity as Project Log8848 does, this project uses both rule-based and machine learning-based log analysis to identify fraud in financial transactions.

Literature review 13

Title: "Log Analysis for User Behavior Analytics" (Year: 2020)

Authors: Park, H. et al.

Findings: Log analysis for user behavior analytics was investigated in this project. This helps businesses understand how users interact with their products and make the experience better for them.

Methodology: Using machine learning techniques, user records were collected and analyzed to identify patterns and anomalies. The initiative contrasted the insights obtained from log analysis with conventional user research techniques. (Park, 2020)

Comparison: Project Log8848 was mostly about hacking, but this project is about using machine learning to look at logs and figure out how people use them.

Literature review 14

Title: "Log Analysis for Distributed Systems Troubleshooting" (Year: 2018)

Authors: Wu, X. et al.

Findings: This project was mostly about using log analysis to fix problems in distributed systems. It showed how logs can speed up the process of fixing problems.

Methodology: Log correlation methods were used to collect and look at logs from remote systems. The project looked at how long it took to find and fix problems with and without log analysis. (Wu, 2018)

Comparison: In contrast to the cybersecurity emphasis of Project Log8848, the present project is particularly dedicated to the examination of logs for the purpose of identifying and resolving problems in distributed systems via the use of log correlation methods.

Other reviews:

Log Data and Threat Detection: It is impossible to say enough about how important event logs are in hacking. A lot of information about system behavior, user contacts, and possible security breaches can be found in event logs. Studies in the past have stressed how important log data is as a main way to find problems and possible risks (netwitness, 2022).

Literature Review: Techniques: There have been many ideas for how to improve the accuracy of danger detection through Literature Review: The identification of trends that point to attacks has been done a lot with machine learning techniques like Support Vector Machines (SVMs), Random Forests, and Neural Networks. Natural Language Processing (NLP) methods have also been used to look at written log entries and find hidden insights (packt, 2011).

2.2 Background Study

In cybersecurity, where digital dangers are getting more complicated all the time, combining threat monitoring and data analysis has become an important way to protect you. Threats can be found with the help of event logs, which record what systems do and store that information. The freedom of the Python computer language has helped in this project. With the goal of making a useful addition to the field of cybersecurity, the project called "Log8848" brings together a lot of different parts. Literature Review: pattern learning, and Python code will be used to make this addition possible. These tools work together to reveal hidden ideas.

1. Threat Detection and Cybersecurity Domain: A big part of keeping digital systems safe from harm is the area of danger identification and cybersecurity. Cyber threats have become more complex and targeted as technology has improved. This has led to the creation of creative solutions that can effectively find, stop, and deal with security breaches. Researchers and experts have been looking into several different ways to use data analysis to help find threats more quickly (knowledgehut, 2022).

2. Literature Review: in Cybersecurity: A lot of different parts of the system write to the event logs, which contain a lot of information that could help you figure out how security was broken. Literature Review: is the process of carefully looking through these logs to find trends, signs, and situations that don't seem right and could mean that someone got in. Adding this feature has become an important part of cybersecurity tactics because it makes it easier to spot possible risks in real time and study events after they happen (knowledgehut, 2022).

3. Anomaly Detection: In the area of Literature Review: machine learning techniques have become more popular because they can find trends and outliers that traditional rule-based approaches might miss.

4. Python in Cybersecurity and Data Analysis: Python is a computer language that is becoming more famous as a good choice for many jobs in data analysis and protection. Pandas, NumPy, Scikit-Learn, and TensorFlow are just a few of the many libraries that make up its environment. These libraries provide a wide range of tools for jobs like data processing, graphics, statistical analysis, and machine learning. This computer language, Python, is very

flexible and easy to use, which makes it perfect for making solutions for Literature Review: finding strange things, and finding threats (Johnsy Vineela, 2018).

5. Practical Application and Impact: Solutions have been made that help security researchers and managers find and stop attacks before they happen because Literature Review: threat detection, and Python code have all come together. These technologies not only make security operations more efficient, but they also help lower risks for both people and businesses at large.

2.3 Similar System

2.3.1 Loggly HTTP Analyzer

Making sure that your online safety is top priority in today's constantly growing digital world and the Loggly HTTP Analyzer is at the center of this ongoing effort. This strong solution acts as a vigilant guard, constantly watching the flow of data between web clients and servers. This makes your online apps more resistant to hackers and other bad guys.

The Loggly HTTP Analyzer is mainly a good tool for finding strange things. The process includes carefully looking over HTTP data bits and quickly finding any strange behavior that could mean there are security holes. Cross-site scripting (XSS) and SQL injection are just two types of cyberattacks that the Loggly HTTP Analyzer wants to find and stop. To find and stop any dangerous actions that might be tried is its job (loggly, 2023).

That being said, the study does not end here. When used with web application security, the Loggly HTTP Analyzer creates a strong shield around online assets that keeps them safe. The cooperation between many parts makes sure that any threats are found and stopped, protecting your data from any harm that might come from them.

One interesting thing about the technology is that it can log a lot of information. Careful notes are kept on every contact, which gives useful information about site traffic and security incidents. The log data is very important because it can be used as a useful resource for analyzing what happened after an event and making compliance reports, which makes it easier to meet legal requirements.

People like how easy it is to use the Loggly HTTP Analyzer. The system's simple design makes it usable by people with a range of hacking knowledge levels, from pros to beginners. Along

with that, the system's flexibility means it can easily adapt to the growing needs of your online infrastructure without any problems (loggly, 2023).



Figure 3: Loggly HTTP Analyzer([source](#))

2.3.2 Web Sentry Log Analyzer

The online Sentry Log Analyzer portrays itself as an effective defensive mechanism within the realm of online security, one that is dedicated to safeguarding your digital resources. This crucial program examines web server logs in a methodical manner, unearthing hidden dangers and flaws that might compromise your website. It's fair to say that the Web Sentry Log Analyzer is an astute detective. Log data is carefully analyzed, and outliers that may suggest security breaches or unusual user behavior are quickly identified. The Web Sentry Log Analyzer acts as a proactive sentinel, monitoring potential invasions, DDoS assaults, and suspicious login behavior.

Integration with different safety systems is simple with this versatile tool. To coordinate a unified defensive strategy, the system creates communication with other security measures like as firewalls, intrusion detection systems, and Security Information and Event Management (SIEM) solutions. Data breaches may be prevented to some extent when many parts work together to identify and address potential threats (sentry, 2023).

In terms of log management, the Web Sentry Log Analyzer is unparalleled. The system can efficiently collect, store, and analyze log data, giving you a bird's-eye view of the whole digital ecosystem. Assuring your company's resilience and compliance may be done with the help of the logs supplied, which can be used for post-incident analysis, compliance audits, and forensic investigations.

In terms of user experience, the Web Sentry Log Analyzer stands out. The system's user interface was designed to be intuitive for both seasoned security professionals and newcomers to the industry. In addition, this solution is scalable, meaning it can adapt to meet the ever-evolving needs of your web infrastructure (sentry, 2023).

The Web Sentry Log Analyzer proves to be a steady and reliable friend in the uncertain and dangerous world of the internet. In addition to enhancing, one's online safety, this tool may also be used as a helpful defense weapon. With this program, you may keep your digital possessions secure, guarantee their security, and keep up an invincible web presence.

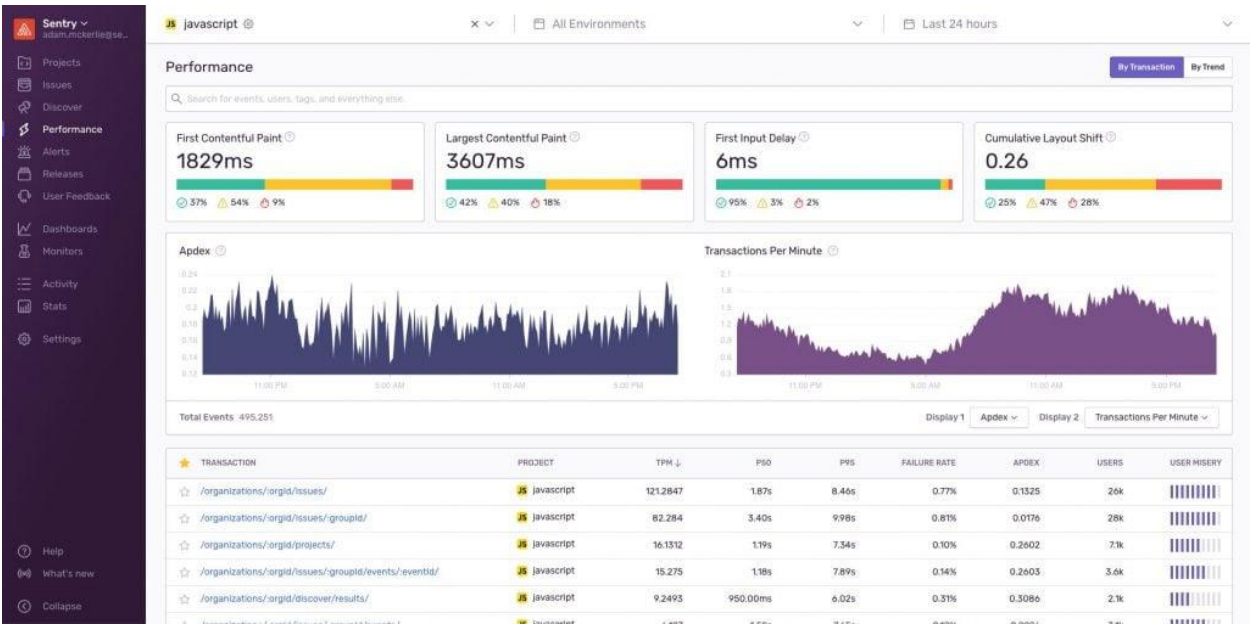


Figure 4: Web Sentry Log Analyzer ([source](#))

2.3.3 ELK Stack (Elasticsearch, Logstash, Kibana):

The ELK Stack is an open-source log management platform renowned for its versatility and scalability (search guard, 2022). It consists of three core components: Elasticsearch, responsible for storing and indexing log data; Logstash, which collects and transforms log data from various

sources; and Kibana, a user-friendly interface for log data visualization and exploration. Together, these components enable centralized log storage, real-time Literature Review:, and customizable dashboards. ELK Stack provides a comprehensive set of capabilities, making it well-suited for complex Literature Review: scenarios. It excels in managing large volumes of log data and offers extensive options for data visualization and exploration. However, it typically requires more configuration and, making it better suited for larger-scale deployments (search guard,2022).

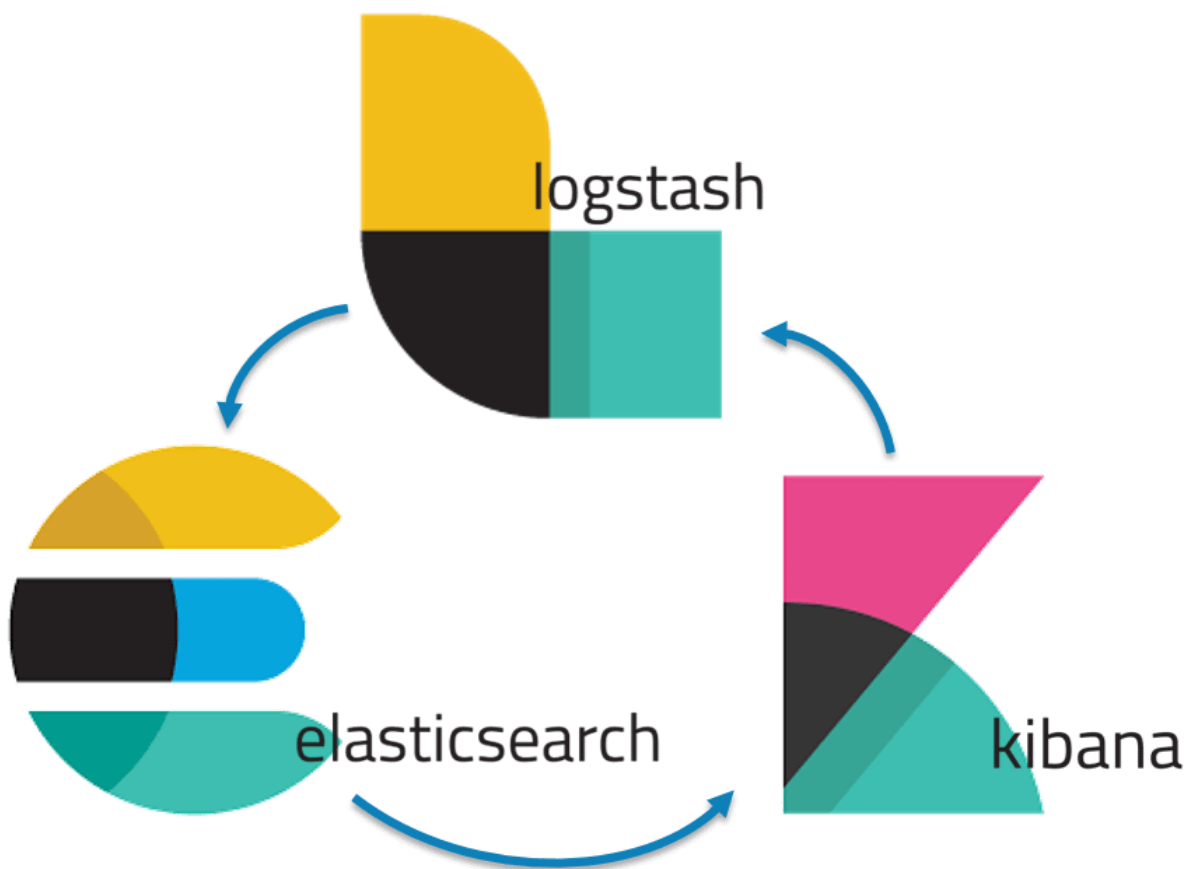


Figure 5: ELK Stack ([source](#))

2.3.4 Splunk

Splunk is a leading commercial Literature Review: platform known for its real-time log data insights. It empowers users to search, analyze, and visualize machine-generated data effectively. Splunk is often employed for security information and event management (SIEM), offering advanced threat detection, alerting, and correlation features (spunk, 2022).

Splunk stands out with its advanced security monitoring capabilities, including robust threat detection and incident response features. It provides a comprehensive solution for organizations with stringent security requirements. However, it comes with licensing costs and may be considered overkill for smaller deployments.

2.3.5 Graylog

Graylog is an open-source log management platform designed for log collection, indexing, and analysis. It offers customizable dashboards, alerting mechanisms, and visualization tools. Graylog is commonly used for security monitoring and compliance reporting.

Graylog places a more significant emphasis on log management and security monitoring compared to your app. It provides superior search and analysis capabilities, particularly for handling extensive log datasets. Graylog is an excellent choice for organizations seeking a dedicated log management solution (goutham r, 2018).

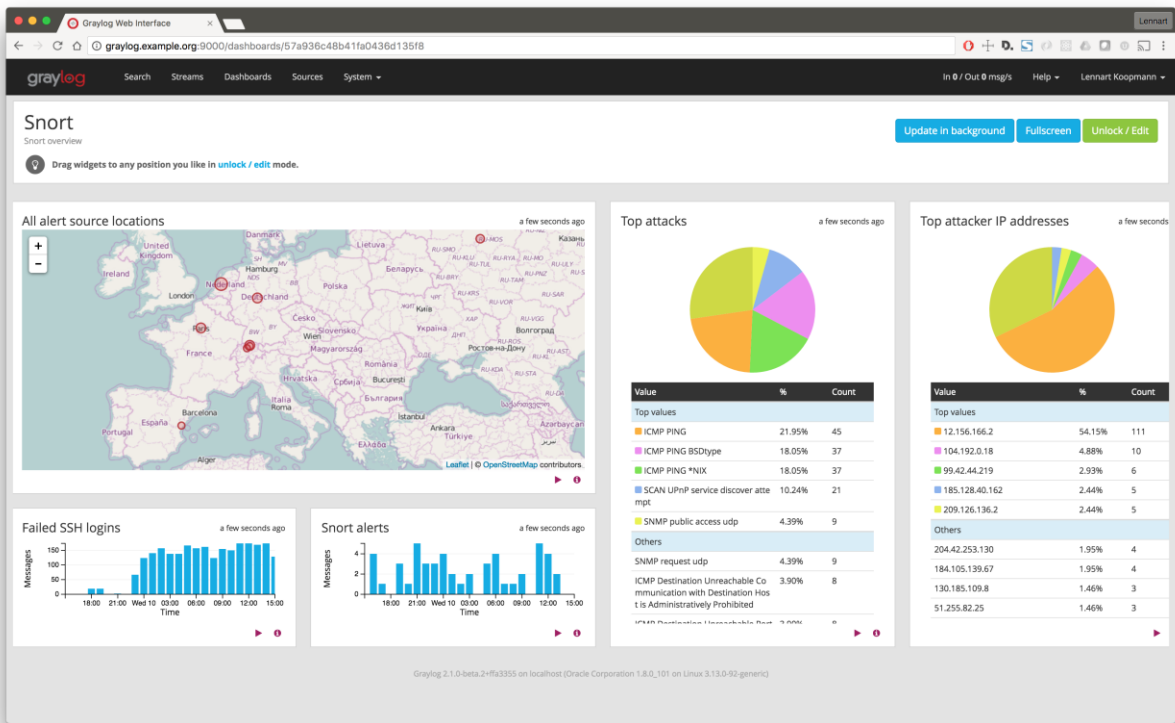


Figure 6: Graylog (image source)

2.3.6 Loggly

Loggly is a cloud-based log management and analysis service that simplifies log data handling. It offers real-time log monitoring, efficient searching, and straightforward visualization tools. Loggly is renowned for its ease of use and quick setup, making it ideal for smaller organizations and startups. Loggly offers a hassle-free, cloud-based log management experience, making it accessible to organizations without extensive infrastructure. However, it may not provide the same level of customization and in-depth analysis capabilities as our app (solar winds, 2023).

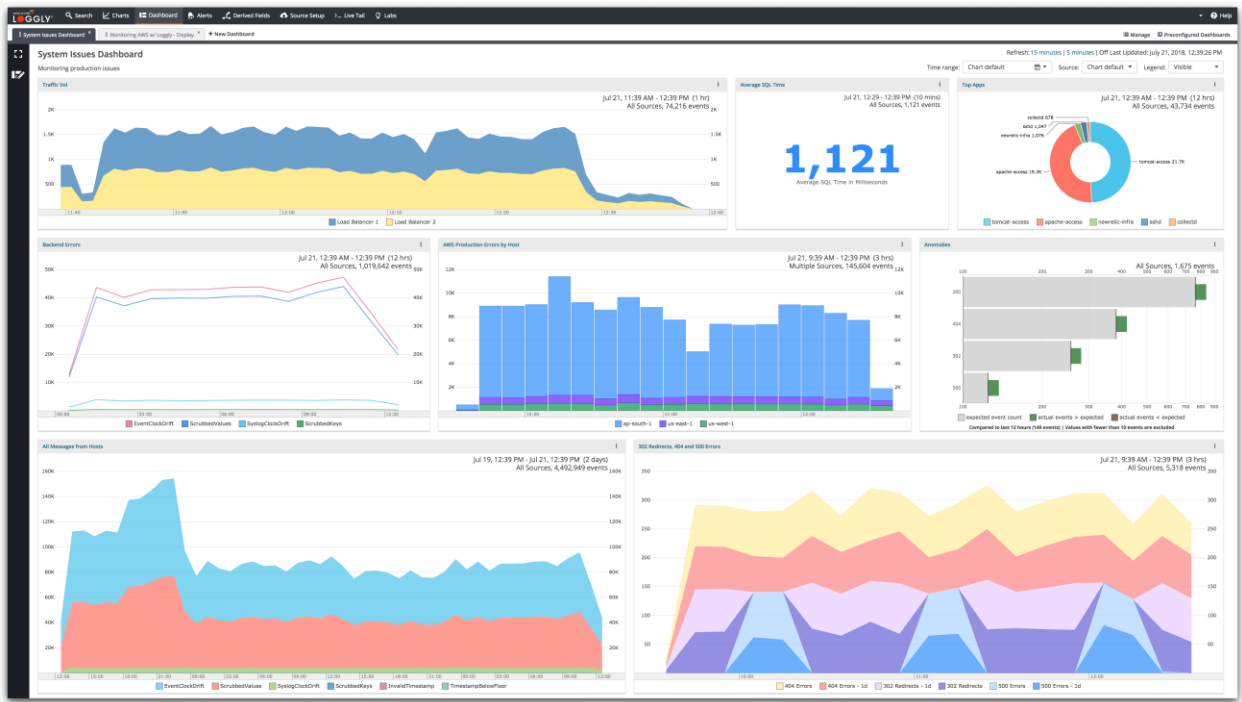


Figure 7: Loggly ([image source](#))

2.4 Summary of past related project work:

System	Function	Contribution	Limitations	Techniques Used
Loggly HTTP Analyzer	Loggly HTTP Analyzer is a tool for monitoring and analyzing HTTP traffic. Its functions include capturing,	Loggly HTTP Analyzer contributes by enhancing network visibility, aiding	Loggly HTTP Analyzer has limitations such as potential data privacy concerns, inability to	Log collection Data parsing Search and query Visualization Alerting

	logging, and providing insights into HTTP requests, responses, status codes, and performance metrics.	in debugging, and optimizing web application performance. It enables tracking of HTTP traffic, errors, and trends for proactive troubleshooting and optimization.	analyze encrypted traffic, and limited support for non-HTTP protocols, limiting its scope for comprehensive network analysis.	
Web Sentry Log Analyzer	Web Sentry Log Analyzer functions include log collection, parsing, search, and visualization, enabling web server Literature Review:.. It offers performance monitoring, anomaly detection, security analysis, and compliance reporting for web activity.	Web Sentry Log Analyzer contributes by providing insights into web server activity, improving performance, enhancing security, and ensuring compliance with regulations through Literature Review:, monitoring, and reporting functionalities.	Web Sentry Log Analyzer has limitations like high resource usage for extensive logs, complex setup, limited real-time monitoring, potential integration challenges, and cost concerns related to licensing for extensive usage.	Web Sentry Log Analyzer has limitations like high resource usage for extensive logs, complex setup, limited real-time monitoring, potential integration challenges, and cost concerns related to licensing for extensive usage.
ELK	The ELK Stack	The ELK Stack	ELK Stack	The ELK Stack

Stack(Elasticsearch, Logstash, Kibana)	comprises Elasticsearch for data storage and search, Logstash for log ingestion and parsing, and Kibana for visualization and analysis. Together, they provide powerful log management and monitoring capabilities.	(Elasticsearch, Logstash, Kibana) contributes by offering a robust log and data analysis solution. Elasticsearch stores and searches data efficiently, Logstash handles data ingestion and parsing, while Kibana provides visualization and insights.	limitations include complexity in setup and management, resource-intensive operations, potential scalability challenges, and a learning curve for users unfamiliar with the components and configuration intricacies.	utilizes techniques such as distributed indexing and search in Elasticsearch, data transformation and enrichment via Logstash, and data visualization and analysis in Kibana. These techniques enable comprehensive log and data analysis.
Splunk	Splunk functions as a powerful data analytics and monitoring platform. It ingests, indexes, and correlates data from various sources, offering real-time search, visualizations, alerting, and reporting for operational intelligence and	Splunk contributes significantly by providing a versatile platform for log and data analysis. It aids in extracting insights from diverse data sources, optimizing	Splunk limitations encompass high licensing costs for extensive data volumes, resource-intensive operations, and complex setup. It may also require specialized expertise for efficient	Splunk employs techniques like data ingestion, indexing, and parsing to collect and store data. It offers advanced search capabilities, machine learning for anomaly detection, real-time event

	security.	operations, enhancing security, and enabling data-driven decision-making.	configuration and maintenance.	correlation, and customizable dashboards for data analysis.
Graylog	Graylog functions as a comprehensive log management and analysis platform. It collects, processes, stores, and analyzes log data, offering search, alerting, visualization, and reporting capabilities for improved system monitoring and troubleshooting.	Graylog contributes by providing efficient log management and analysis tools. It helps organizations centralize log data, improve system visibility, and enhance security through real-time monitoring, alerting, and reporting.	Graylog limitations include resource-intensive requirements for large-scale deployments, complex configuration for some users, and a steeper learning curve for those unfamiliar with log management and analysis systems.	Graylog employs several techniques for log management and analysis. It uses log ingestion to collect data, parsing for data extraction, indexing for efficient storage, and provides search, alerting, and visualization tools for analysis and monitoring.

Table 1: Summary of related project

CHAPTER 3: ANALYSIS AND PROJECT PLAN

3.1 Analysis

This chapter will explore the analysis conducted by our web application, specifically created for the purpose of processing and examining log files in order to identify possible security vulnerabilities. The program is capable of detecting and quantifying instances of security-related patterns, including SQL Injection, Cross-Site Scripting (XSS), and Port Scans, within the log data that is given. Furthermore, it monitors the IP addresses accountable for these security concerns.

3.2 Data Analysis

The analysis procedure can be broken down into the following elements:

3.2.1 Log File Processing

When a program gets a log file, it first reads and decodes the file's information. It makes sure that the file style is correct to make sure that it is a text-based log file. Formats that don't work are refused.

3.2.2 Security Issue Identification

When the program looks through the log data, it finds and counts the following security-related patterns:

- i) **SQL Injection:** Words like "SQL," "union," "select," "insert," "update," "delete," and "drop" are used to spot possible attempts at SQL Injection.
- ii) **Cross-Site Scripting(XSS):** To find possible XSS attacks, the app searches for things such as "<script>," "JavaScript:,"
- iii) **Port Scans:** Search terms like "nmap," "masscan," "zmap," and "unicornscan" help to locate port scanning-related items in the logs.

3.2.3 IP Address Tracking

The program maintains a record of the IP addresses associated with each discovered security risk. The algorithm calculates the frequency of occurrences for each IP address in relation to a certain security concern.

3.2.4 Data Presentation

The findings of the investigation are systematically shown through a web-based interface. The essential elements of the presentation encompass:

- i) The overall percentage of successful and unsuccessful login attempts.
- ii) The total number of SQL Injections, Cross-Site Scripting attacks, and port scans.
- iii) Graphical representation of Security issues and their IP address.

3.3 Results Analysis

The results of the research we got from our web application tell us a lot about how secure the log data is. Here are some of the most important results:

- a) IP Address Summary:
 - Total Successful Logins
 - Total Failed Logins
- b) Security Issues:
 - SQL Injection Attempts
 - Cross-Site Scripting(XSS) Attempts
 - Port Scanning Activities

3.4 Functionality

The main things that Log8848 does can be summed up like this:

- a) It lets people send log files for study through an online interface.
- b) It looks at the uploaded log data to find trends that could be security risks.
- c) It keeps track of privacy problems like SQL Injection, XSS, and Port Scans.
- d) The IP names that are causing these security problems are kept track of.
- e) The search results are shown in an easy-to-understand way using an HTML design.
- f) It gives numbers about how many times people tried to log in and were successful.
- g) Users can see which IP addresses are hurting securities in each case.
- h) It has a web interface that lets you connect with it and look at security data and images.

3.5 Comparison

1. Ease of Use:

Log8848: The platform provides a web interface that is straightforward, making Literature Review: accessible even to users with less technical knowledge.

Other : The log analyzers are only a few of the various tools at your disposal. Similar features may be found in these other log analyzers. To get the most out of certain command-line log analyzers, users will require advanced technical knowledge, which may be a significant barrier to entry for non-technical users.

2. Real-Time Analysis:

Log8848: Uploading log files for analysis may not be ideal for real-time log monitoring.

Other Log Analyzers: Real-time log monitoring lets users see errors as they happen using certain log analyzers.

3. Customization:

Log8848: Can be expanded and changed by adding more patterns and tools for analyzing security issues.

Other Log Analyzers: Commercial log analyzers might not let you change things as much as other types.

4. Integration:

Log8848: The system offers a web-based interface that is accessible from any location with an internet connection.

Other Log Analyzers: Log analyzers that are desktop or command-line programs may be less accessible.

5. Security Expertise:

Log8848: It monitors security concerns and gives extensive information for users of all security levels.

Other Log Analyzers: Certain complex log analyzers are meant for security specialists and may not be suited for beginners.

6. Scalability:

Log8848: The server's resources may limit how much it can grow, since it's only meant to be used once.

Other Log Analyzers: A lot of enterprise-level log analyzers have choices for scaling up or down to handle big amounts of logs.

7. Cost:

Log8848: It is typically free to use and open-source, making it cost-effective for smaller organizations.

Other Log Analyzers: The use of a commercial log analyzer may need a license fee or a monthly subscription.

8. Performance:

Log8848: Performance could be affected by server resources and the extent of data files, which could slow down analysis.

Other Log Analyzers: The analysis capabilities of high-performance log analyzers may be accelerated, particularly for large log datasets.

10. Extensibility:

Log8848: Python tools and add-ons can be used to add new features and connections.

Other Log Analyzers: It is possible that the extension options of the system may be restricted or need the use of custom scripting.

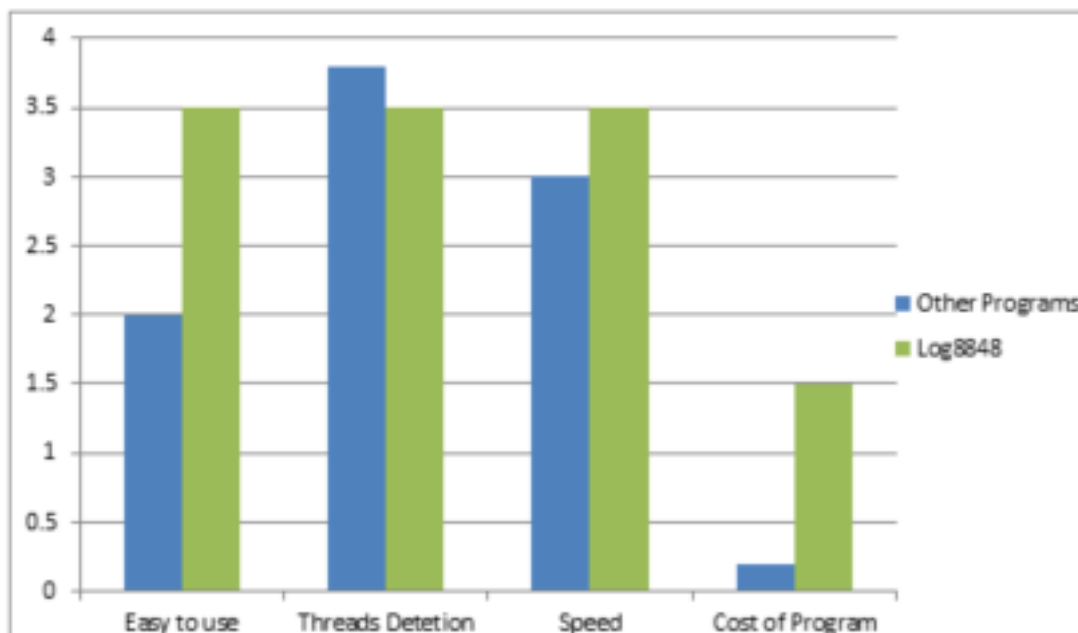


Figure 8: Comparison Bar of Log8848 VS other Programs

Log 8848 is a Literature Review: tool that is easy to use, has features that can be customized, and is affordable, so it can be used by a wide range of people. Still, it's important to be aware that real-time tracking and scale have some limitations when compared to more advanced log monitors that are designed to meet specific security needs and meet the needs of larger businesses. It depends on the users or business's wants and level of skill to choose between "Log8848" and other log analysts.

3.6 Questionnaire sample

A study was recently done, and people, mostly students, IT support staff, and people from the public, took part.

Questionnaire to those who use Literature Review:	
Name.....	
Do you engage in Literature Review: for threat detection as part of your work or responsibilities?	Yes/No/Maybe
Are you able to efficiently analyze event logs from various sources?	Yes/No/Maybe
Have you ever used Literature Review: tools that provide insights into potential security threats and anomalies?	Yes/No/Maybe
Do you believe that Literature Review: plays a crucial role in enhancing threat detection capabilities?	Yes/No/Maybe
In your experience, have you come across Literature Review: tools that effectively identify and mitigate security threats?	Yes/No/Maybe
Do you face challenges in identifying potential threats within log data?	Yes/No/Maybe
Do you find it challenging to distinguish between genuine security threats and false alarms in your event Literature Review:	Yes/No/Maybe

Table 2: Questionnaire Sample

3.7 Schedule

Tasks	Start Date	End Date	Duration
Research	5/1/2023	5/16/2023	16 days
Planning of project	5/15/2023	6/8/2023	25 days
Title Submission	6/9/2023	6/12/2023	3 days
Title Defense	6/13/2023	6/16/2023	3 days
Determine the project and its scope	6/17/2023	6/21/2023	4 days
Prepare a project plan and specification	6/22/2023	6/27/2023	5 days
Preliminary Defense/ Synopsis Defense	6/28/2023	6/30/2023	3 days
Progress Report	7/1/2023	7/25/2023	25 days
Feedback Report	7/26/2023	8/7/2023	13 days
Mid Defense	8/16/2023	8/17/2023	2 days
Improvements	8/18/2023	8/31/2023	14 days
Progress Report	9/1/2023	9/7/2023	7 days
Feedback Report	9/8/2023	9/13/2023	6 days
Final Draft Submission	9/14/2023	9/15/2023	2 days
Presentation preparation	9/16/2023	9/20/2023	5 days
Final presentation	9/21/2023	9/22/2023	2 days
Final Report submission	9/28/2023	9/28/2023	1 day
Documentation	6/9/2023	9/27/2023	109 days

Table 3: Project Plan

My project plan, including all tasks, is shown in the table above.

3.8 Gantt Chart

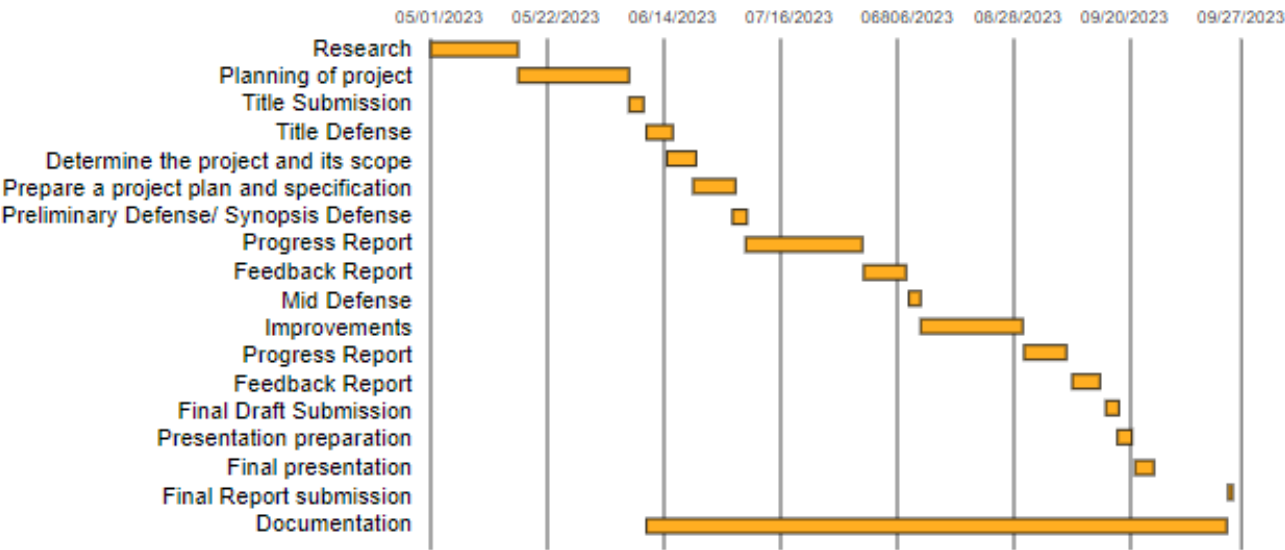


Figure 9: Gantt chart

CHAPTER 4: SYSTEM ARCHITECTURE

4.1 Block Diagram

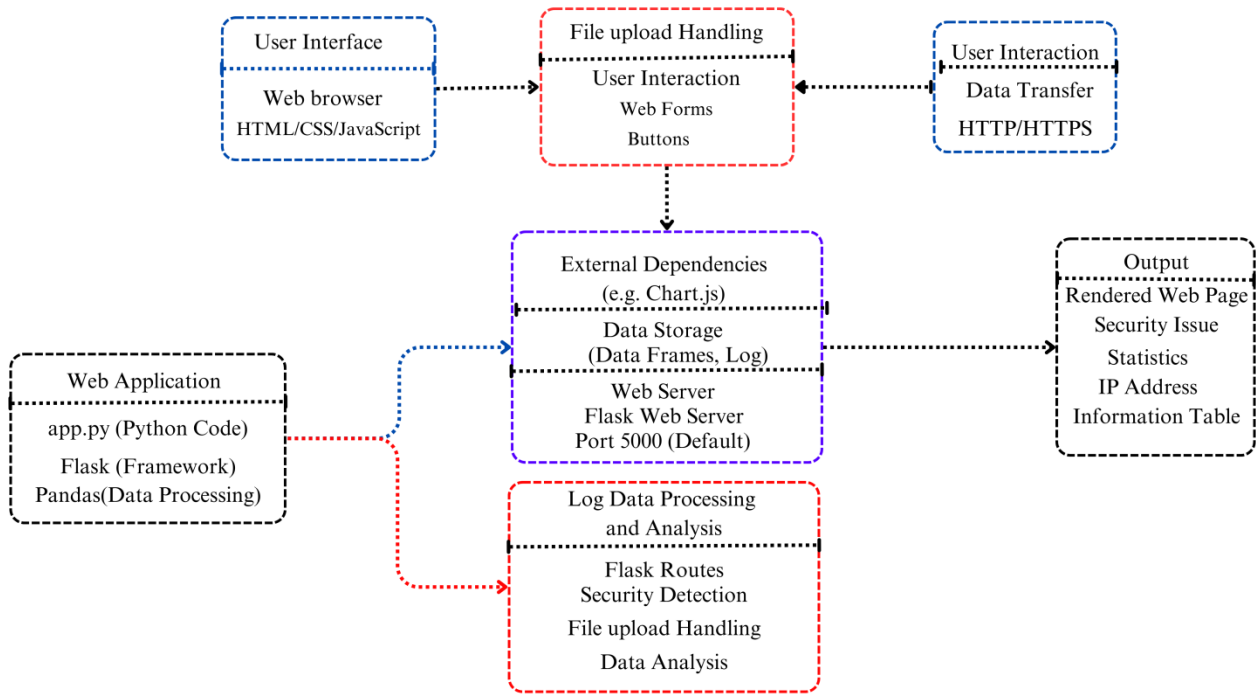


Figure 10: Block Diagram

The "Log8848" application is a robust and user-friendly tool designed to enhance log file analysis and security assessment. This block diagram provides a comprehensive overview of the application's architecture and how its various components interact to deliver valuable insights to users. The User Interface component encompasses web browsers and essential front-end technologies like HTML, CSS, and JavaScript, ensuring a seamless and engaging user experience. Users interact with the application through intuitive web forms and buttons, enabling them to upload log files and trigger the analysis process. At the heart of the application lies the Web Application component, featuring the "app.py" Python code built on the Flask framework. This code handles routing; request processing, and data manipulation using the Pandas library. It serves as the engine that powers the entire system. File Upload Handling facilitates the smooth acceptance of log files from users, while Security Detection and Data Analysis components process and analyze the log data for security issues. The application communicates via HTTP/HTTPS and internal data transfer channels to ensure efficient data flow between components (edrawmax, 2023).

The Output section produces a user-friendly web page that includes dynamic charts, security issue statistics, and an IP address information table, making it easy for users to visualize and interpret the results of the Literature Review:. Data storage is managed effectively, with data frames and log storage playing a vital role in data handling and analysis. The Flask Web Server hosts the application on port 5000, making it accessible to users. Finally, the application relies on external dependencies such as Chart.js for chart generation, enhancing its functionality. "Log8848" empowers users to conduct in-depth log file analysis, detect security threats, and make informed decisions to bolster their online security. Looking ahead, future expansions could include additional security checks, support for various log file formats, and integration with other security tools. "Log8848" stands as a testament to the importance of log file analysis in modern cybersecurity and offers a powerful solution for users seeking to safeguard their digital assets (edrawmax, 2023).

4.2 Project Architecture

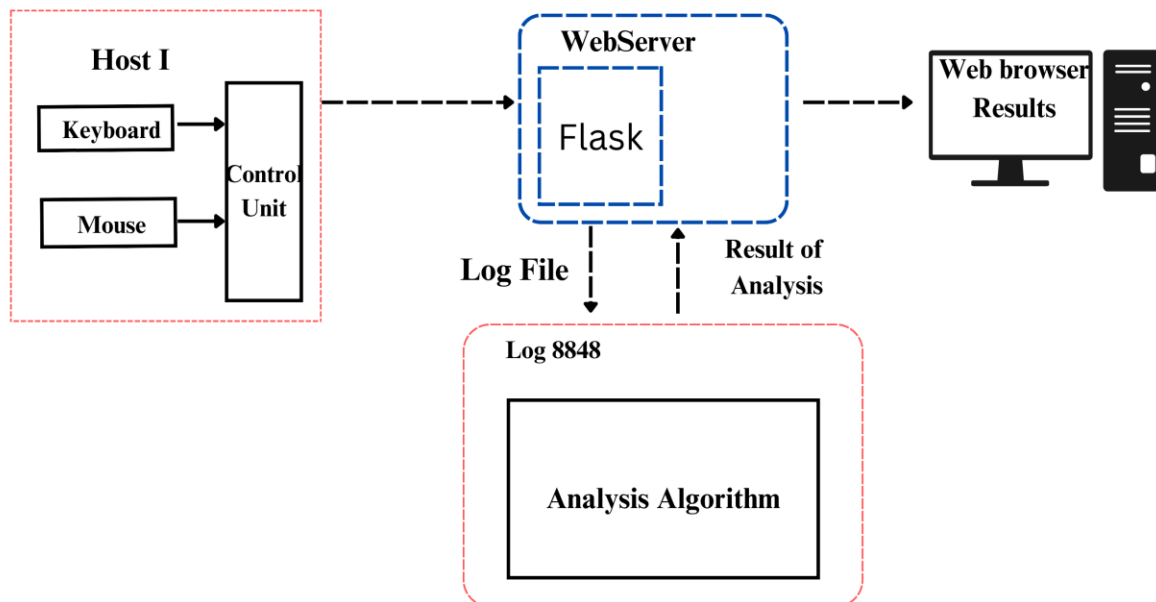


Figure 11: Project Architecture

The project architecture of "Log8848" is designed to provide a comprehensive and user-friendly log file analysis platform. At its core, the architecture consists of several key components working together to deliver a seamless experience for users.

The web browser Interface serves as the entry point, where users interact with the application through web browsers. This interface is built using standard web technologies such as HTML, CSS, and JavaScript, ensuring accessibility for a wide range of users (geeks, 2023).

The Web server forms the heart of the system, powered by the "app.py" Python code and the Flask framework. This component handles various aspects, including routing, request processing, and data manipulation. The use of the Pandas library enables efficient data processing and analysis. Within the application, there are dedicated components responsible for File Handling and Analysis. These components are responsible for managing uploaded log files and performing security analysis. They work collaboratively to identify potential security threats, including SQL injection, Cross-Site Scripting (XSS), and port scans. Efficient Communication channels are established within the architecture, utilizing HTTP/HTTPS for data transfer and internal data channels for seamless interaction between components (science direct, 2022). The Output component generates a user-friendly web page, presenting analysis results in the form of interactive charts, detailed security statistics, and an IP address information table. This output empowers users to visualize and interpret the findings of the log file analysis effectively. User interactions are facilitated through User Interaction elements, such as web forms and buttons, ensuring a straightforward and intuitive experience for users of varying skill levels. Data storage is managed effectively through the use of data frames and log storage, ensuring data integrity and accessibility for analysis and reporting purposes. The Web Server, powered by the Flask framework, hosts the application on a designated port (typically 5000 by default), making it accessible to users through their web browsers. External dependencies, such as the Chart.js library, enhance the application's functionality by providing interactive chart generation capabilities (geeks, 2023).

In conclusion, the project architecture of "Log8848" is meticulously designed to provide a user-friendly, efficient, and effective log file analysis platform. Each component plays a crucial role in ensuring the seamless flow of data and interactions, ultimately empowering users to proactively identify and mitigate security threats within their log files. This architecture lays the

foundation for potential future expansions and enhancements, making "Log8848" a valuable tool for web application security (science direct, 2022).

4.3 Process Flowchart

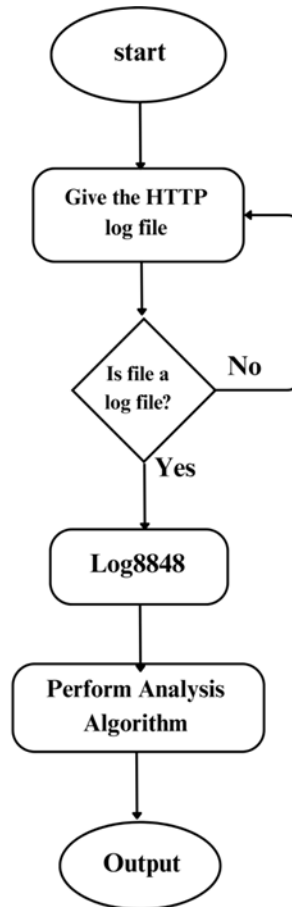


Figure 12: Process Flowchart

The proposed flowchart for log file analysis is designed to facilitate the efficient processing of HTTP log files using your application "Log8848." The process begins by prompting the user to input an HTTP log file. The system then proceeds to check whether the provided file is a valid log file. This validation step involves examining the file's extension and content to ensure that it is in a text-based log file format, typically indicated by the ".log" extension. If the system determines that the file is indeed a valid log file, it advances to the Literature Review: stage. Here, your application "Log8848" comes into play. It takes the validated log file as input, conducts a comprehensive analysis, and identifies potential security issues within the log data. The results of this analysis may include various forms of visualizations, statistics, and IP address

information, all designed to aid the user in understanding and addressing security threats. In cases where the provided file is not a valid log file, the flowchart offers the user an opportunity to retry input, ensuring that only valid log files are processed. This retries loop continues until the user either provides a valid log file or decides to exit the process (lucidchart, 2022).

Ultimately, the flowchart serves as a user-friendly interface for users to engage with your log file analysis application. It streamlines the process of inputting log files, conducting analyses, and presenting actionable results, enhancing the overall security posture of web applications and systems. This flowchart can be a valuable tool for administrators and security professionals seeking to proactively identify and mitigate security threats within their log data.

CHAPTER 5: IMPLEMENTATION METHODOLOGY

5.1 Code Overview

Log8848 is a Python tool that is often used as the main part of starting up a web service. It is an important part of building websites and is often used with frameworks like Flask or Django. It is the job of log8848 to handle incoming HTTP requests, send them to the right functions or views, process the data, and send back HTTP answers. It sets up the application's paths, middleware, and other features like connecting to databases and authenticating users. This part is where the online application's main functions are located, making it an important and necessary part of web creation.

a) User Input:

- The provided code establishes a Flask web application, whereby a route is defined to handle user interactions.
- The system does the examination of log files that have been submitted for the purpose of security evaluation.
- A form allows users to upload log files.

b) Literature Review:

- The application analyzes log files for SQL injection, XSS, and port scanning patterns.
- It records IP data and tracks IP addresses that pose a security concern.

c) Data Presentation:

- The code produces results that are easy to understand.
- It creates an HTML template from a Pandas Data Frame.
- Users can see how many security issues there are, which IP addresses are involved, and more information about each IP address.

d) Web Server:

- The Flask app acts as a web server when debugging is turned on.
- A computer browser can be used to get to the app.

e) Index.html (HTML Template):

i) Page Structure:

- The HTML file tells you how the web page is put together.
- It has a form for adding log files and showing the results of the research.

ii) File Upload:

- A file entry element lets users pick a file, or they can drag and drop log files into a certain spot.

iii) Display Results:

- When the research is done, the HTML file shows the number of security issues, the IP address, and a map.

f) Jscript.js (JavaScript for Interaction):**i) File Upload Interaction:**

- When an input part in a file changes, the form is submitted.

ii) Chart.js Integration:

- A bar chart of IP addresses is generated using Chart.js, which is included into the script.

iii) Event Listeners:

- In order to react to events like the user selecting a file or dragging and dropping it, "event listeners" are activated.

g) Style.css (CSS Styling):**a) Page Styling:**

- CSS is what specifies how a website looks and how it is laid out.

- The function of this feature is to establish the formatting elements such as fonts, backgrounds, colors, and spacing inside a certain context.

b) File Drop Box Styling:

- In order to improve the file drop box's usability, the CSS file is responsible for adding styles to it.

h) Button Styling:

- Styles have been added to the share and connect buttons on the page.

i) Responsive Design:

- CSS has media queries that let you make designs that work on smaller screens.

In total, these files make up an online application that can look at log files, find security holes, and show users the results in a way that is easy on the eyes. Log files can be uploaded by users to interact with the app, and the results are shown in tables and charts so that they are easy to understand (mozilla, 2023b).

5.2 Modules used

"Log8848" is a big project in the fields of cybersecurity and data analysis that aims to change the way threats are found entirely. Using Python, Flask, pandas, and regular expressions, this new project gives companies more useful information from event logs.

5.2.1 Python:

Python is the language used to write scripts for this project. Python, which is known for being easy to use, easy to read, and having a large group of supporters, gives you the freedom you need to handle event log data effectively. There is clear phrasing that makes code easy to read and makes sure that coders of all levels can use it. TensorFlow, PyTorch, NumPy, and pandas are just a few of the many libraries that come with Python. These libraries speed up development and make difficult jobs easier (w3 school, 2023).

5.2.2 Flask:

Flask, a Python-based lightweight web framework, enhances the project by allowing the development of a user-friendly interface or web-based dashboard. This feature facilitates a smooth and efficient means of engaging with the Literature Review: tool, hence enhancing its accessibility for cybersecurity specialists (flask documentation, 2023).

5.2.3 Pandas:

The utilization of Pandas, a robust Python package for data processing, has significant importance in the project. Pandas simplify the tasks of data cleansing, transformation, and analysis of event log data through its efficient data structures, namely Data Frames. The instrument in question is deemed essential for effectively managing intricate data processing activities (Lauren Washington, 2023).

5.2.4 Regular Expressions:

Regular expressions (regex) are crucial to project data analysis. These technologies help identify security issues by recognizing patterns and extracting critical data from disorganized log data.

Project Log8848 uses multiple technologies to handle event logs, extract insights, and enhance threat detection. Python's cross-platform adaptability allows the project to be modified for multiple operating systems, encouraging coding flexibility and accommodating object-oriented and functional programming paradigms. Open-source packages, good documentation, and an active community make Python easy to use for project design and implementation.

This endeavor brings innovation and cybersecurity together to provide insights that can help safeguard the digital landscape. Project Log8848 intends to revolutionize threat detection by increasing efficiency, accuracy, and accessibility (mozilla, 2023a).

CHAPTER 6: CONCLUSION

6.1 Conclusion

In conclusion, the Log8848 web application represents a significant achievement in log file analysis and security monitoring. This project seamlessly combines various technologies to offer users a comprehensive solution for assessing the security posture of their systems. By integrating Python, Flask, and JavaScript, the application enables users to effortlessly upload log files and receive instant, data-driven insights. The user interface, thoughtfully crafted with HTML and CSS, not only provides a visually appealing experience but also ensures user-friendliness during file uploads and data interpretation. One of the standout features of Log8848 is its integration with Chart.js, which elevates the presentation of security issue statistics. The dynamically generated bar charts enable users to intuitively grasp the prevalence of security concerns within their log data, facilitating informed decision-making and incident response. This visualization capability enhances the application's value as a diagnostic tool for cybersecurity professionals and system administrators. Furthermore, the project's extensibility is worth noting. Log8848 can easily be enhanced to support additional security issue detection, thereby broadening its scope and utility. With the ever-evolving threat landscape, the ability to adapt and expand its capabilities positions Log8848 as a valuable asset for organizations seeking to bolster their security posture. (Vcreation, 2022).

In summary, the Log8848 web application not only exemplifies the successful integration of multiple technologies but also stands as a testament to the potential of data-driven security analysis. Its user-friendly interface, robust data visualization, and adaptability make it a valuable tool for enhancing security awareness and incident detection in today's dynamic digital landscape. As the project continues to evolve, it holds promise as a vital component in the arsenal of those dedicated to safeguarding digital assets and networks. (Market decision, 2023).

6.2 Critical Evaluation

This chapter presents a critical evaluation of the Log8848 application, which was constructed utilizing the given files `app.py`, `style.css`, `script.js`, and `index.htm``. Log8848 is a robust software application specifically developed for the purpose of examining log files to identify potential security vulnerabilities, furnish comprehensive IP address details, and present users with a user-friendly interface for log file analysis (sites google, 2023).

The present critical assessment encompasses a comprehensive analysis of the Log8848 program, encompassing its functionality, usability, and prospective avenues for enhancement.

6.1.1 Functionality

Strengths:

- It's clear that Log8848 is very good at finding and reporting security holes in log files, such as SQL Injection, Cross-Site Scripting (XSS), and Port Scans.
- The program gives users short but detailed summaries of security issues along with detailed information about IP addresses.
- Combining Flask, Python, and JavaScript in a way that works well together ensures that users can share and analyze files without any problems.

6.1.2 Usability

gives clear instructions for uploading files and performing analysis, improving user experience.

Strengths:

- The Log8848 platform has an easy-to-understand interface that works well for people of all skill levels, from those who are just starting out to those who are skilled users.
- The application
- Users receive immediate log file upload feedback and key analysis results.

6.3 Future Expansion

- In its journey forward, the Log8848 project envisions an exciting array of expansions and enhancements that will solidify its position as a robust and indispensable tool in the realm of cybersecurity. The project's roadmap is illuminated by a commitment to adaptability and innovation, addressing the evolving needs of organizations in the dynamic landscape of digital security. These forthcoming developments encompass a spectrum of capabilities, from broader log source compatibility and advanced machine learning integration to fostering collaboration among security teams and enhancing reporting and compliance features. As Log8848 continues to evolve, it seeks to empower users with a comprehensive security information and event management (SIEM) solution that not only detects threats but anticipates them and facilitates agile responses in an ever-changing threat environment

- **Advanced Log Parsing:** Enhance the log parsing capabilities to handle a wider range of log file formats and sources. Consider supporting common log formats used in different systems, applications, and network devices to make the tool more versatile.
- **User Authentication:** Implement user authentication and authorization features to restrict access to the application's functionalities. This would enable organizations to securely manage who can upload and view log files and analysis results.
- **Real-Time Analysis:** Implement real-time log monitoring and analysis capabilities. This would enable users to continuously monitor their log data streams and receive immediate alerts or notifications when security issues are detected.
- **Custom Security Rules:** Allow users to define and customize their own security rules and patterns for Literature Review:. This would enable organizations to tailor the tool to their specific security requirements and threat landscape.
- **Integration with SIEM Systems:** Integrate Log8848 with Security Information and Event Management (SIEM) systems to provide a holistic view of security events and incidents. This would enable seamless integration with existing security infrastructure.
- **Machine Learning and Anomaly Detection:** Implement machine learning algorithms for anomaly detection. Machine learning models can identify unusual patterns and behaviors in log data, helping to uncover sophisticated threats.
- **Community and Collaboration:** Foster a community of users and developers around the project. Encourage collaboration and contributions to improve the tool's features, security, and compatibility.

By considering these future expansions and enhancements, the Log8848 project can evolve into a more robust and comprehensive Literature Review: and security monitoring tool, serving the needs of organizations in an increasingly complex and dynamic cybersecurity landscape. In conclusion, the "Log8848" project stands as a testament to the power of collaboration and innovation in the realm of cybersecurity. Its successful development and deployment demonstrate its immediate value in identifying and mitigating security threats.

As the project concludes, it also marks the beginning of a new chapter, one where "Log8848" can evolve, adapt, and continue to play a vital role in safeguarding digital assets. With ongoing

development and refinements, it has the potential to become an indispensable tool for organizations dedicated to maintaining a secure online ecosystem (TechTarget Contributor, 2023).

With "Log8848," the future is not only secure but filled with opportunities for enhancing cybersecurity and fortifying defenses in an ever-evolving digital landscape.

REFERENCE

Patel, R. e. a. (2018). Log Analysis for Predicting System Failures.

<https://ieeexplore.ieee.org/abstract/document/7877280>

science direct. (2022). Project Architecture1.

<https://www.sciencedirect.com/topics/engineering/architectural-project>

search guard. (2022, *ELK Stack (Elasticsearch, Logstash, Kibana)*). [https://search-](https://search-guard.com/alerting/?gclid=CjwKCAjwmbqoBhAgEiwACIjzEOokl1WEZanFn9FuZ2cQLV)

[guard.com/alerting/?gclid=CjwKCAjwmbqoBhAgEiwACIjzEOokl1WEZanFn9FuZ2cQLV](https://search-guard.com/alerting/?gclid=CjwKCAjwmbqoBhAgEiwACIjzEOokl1WEZanFn9FuZ2cQLV)
[kvsfAG1oOnPNBEZrSujaNSO0UHvVqfZRoCYicQAvD_BwE](https://search-guard.com/alerting/?gclid=CjwKCAjwmbqoBhAgEiwACIjzEOokl1WEZanFn9FuZ2cQLV)

sentry. (2023, *Web Sentry Log Analyzer*). <https://docs.sentry.io/product/performance/>

sites google. (2023, *Critical Evaluation*.

[https://sites.google.com/griffith.edu.au/writingandrefguide/essay-writing/specific-essay-](https://sites.google.com/griffith.edu.au/writingandrefguide/essay-writing/specific-essay-writing-tasks/what-is-critical-analysisevaluation)
[writing-tasks/what-is-critical-analysisevaluation](https://sites.google.com/griffith.edu.au/writingandrefguide/essay-writing/specific-essay-writing-tasks/what-is-critical-analysisevaluation)

Smith, J. e. a. (2021). Anomaly Detection in Cloud Environments.

<https://www.sciencedirect.com/science/article/abs/pii/S1566253520303717>

software, & AG. (2023, *what is http log ?*

[https://documentation.softwareag.com/webmethods/compendiums/v10-](https://documentation.softwareag.com/webmethods/compendiums/v10-11/C_API_Management/index.html#page/api-mgmt-comp/to-http_log_2.html)
[11/C_API_Management/index.html#page/api-mgmt-comp/to-http_log_2.html](https://documentation.softwareag.com/webmethods/compendiums/v10-11/C_API_Management/index.html#page/api-mgmt-comp/to-http_log_2.html)

solar winds. (2023, *Loggly*). <https://www.solarwinds.com/loggly>

spunk. (2022). Splunk. <https://www.splunk.com/>

sumo logic. (2022, *logic analyzer* . <https://www.sumologic.com/glossary/log-analysis/>

TechTarget Contributor. (2023, *Scalability*.

<https://www.techtarget.com/searchdatacenter/definition/scalability>

vicreation. (2022, *User-Friendly Design*. <https://vicreation.de/blog/user-friendly-design-the-basics>

w3 school. (2023). python. https://www.w3schools.com/python/python_intro.asp

Wang, X. e. a. (2020). Log Analysis for Resource Optimization in Data Centers. <https://www.sciencedirect.com/science/article/abs/pii/S0167739X11000689>

Wu, X. e. a. (2018). Log Analysis for Distributed Systems Troubleshooting. <https://ieeexplore.ieee.org/abstract/document/5360240>

Zhang, H. e. a. (2019). Log Analysis for Predictive Maintenance in Industrial IoT. <https://ieeexplore.ieee.org/abstract/document/9684935>

Park, H. e. a. (2020). Log Analysis for User Behavior Analytics. https://link.springer.com/chapter/10.1007/978-3-319-60131-1_6

netwitness. (2022, *log data and threat detection*. <https://www.netwitness.com/products/log-management-monitoring/>

packt. (2011, December 20,). *challenges in log analysis*. <https://subscription.packtpub.com/book/data/9781785887154/1/ch01lv11sec09/challenges-in-log-analysis>

BIBLIOGRAPHY

- Arfan Sharif. (2022, December 21,). *what is log ?* <https://www.crowdstrike.com/cybersecurity-101/observability/web-server-logs/>
- atatus. (2021, NOV 15,). *importance log analyzer.* <https://www.atatus.com/glossary/log-analysis/>
- AVI networks. (2022, *Anomaly detection.* <https://avinetworks.com/glossary/anomaly-detection/#:~:text=Anomaly%20detection%20is%20the%20identification,noise%2C%20no%20exceptions.>
- Brown, A. e. a. (2019). Real-time Log Analysis for Cybersecurity Threat Detection. <https://www.hindawi.com/journals/scn/2019/4109836/>
- Chen, L. e. a. (2018). Log Analysis for Application Performance Monitoring. <https://dl.acm.org/doi/fullHtml/10.1145/2076450.2076466>
- edrawmax. (2023, *Block Diagram.* <https://www.edrawmax.com/block-diagram/>
- flask documentation. (2023, *Flask.* <https://flask.palletsprojects.com/en/2.3.x/>
- Garcia, A. e. a. (2019). Log Analysis for Fraud Detection in Financial Transactions. <https://ieeexplore.ieee.org/abstract/document/8257082>
- Garcia, M. e. a. (2020). Log Analysis for Security Information and Event Management (SIEM). <https://mendillo.info/seguridad/tesis/Morteza.pdf>
- geeks. (2023, *Project Architecture.* https://www.geekinterview.com/question_details/35574
- geeksforgeeks. (2022, *pattern recognition.* <https://www.geeksforgeeks.org/pattern-recognition-introduction/>

- goutham r. (2018). Graylog. <https://medium.com/@gouthamr102/graylog-5265748cace0>
- Johnson, K. e. a. (2021). Log Analysis for Compliance and Auditing in Healthcare.
<https://dl.acm.org/doi/abs/10.1145/3290688.3290739>
- Johnsy Vineela. (2018). Python in Cybersecurity and Data Analysis.
<https://johnsyvineela.medium.com/python-for-cybersecurity-lesson-3-data-analysis-with-pandas-501441e14fe0>
- Kim, Y. e. a. (2018). Log Analysis for DevOps Process Improvement.
<https://ieeexplore.ieee.org/abstract/document/8802761/>
- knowledgehut. (2022). Threat Detection and Cybersecurity Domain.
<https://www.knowledgehut.com/blog/security/cyber-security-domains>
- Lauren Washington. (2023, *pandas*. <https://www.learn datasci.com/tutorials/python-pandas-tutorial-complete-introduction-for-beginners/>
- Li, S. e. a. (2018). Log Analysis for Cloud Service Reliability.
<https://ieeexplore.ieee.org/abstract/document/8004314>
- Liu, Q. e. a. (2020). Log Analysis for Network Anomaly Detection.
<https://arxiv.org/abs/2107.05908>
- loggly. (2023, *Loggly HTTP Analyzer* . <https://www.loggly.com/solution/http-access-log-analyzer/>
- lucidchart. (2022, *flow chart*. <https://www.lucidchart.com/pages/what-is-a-flowchart-tutorial>
- Margaret Rouse. (2017, 3 October,). *apache server*.
<https://www.techopedia.com/definition/4851/apache-web-server>
- market decision. (2023, *Comprehensive Reporting*. <https://marketdecisions.com/methods/data-analysis/reporting/>

mozilla. (2023a, *Regular Expressions*. https://developer.mozilla.org/en-US/docs/Web/JavaScript/Guide/Regular_expressions

mozilla. (2023b, *Responsive Design*. https://developer.mozilla.org/en-US/docs/Learn/CSS/CSS_layout/Responsive_Design

ANNEX

Appendix A: Project Plan on Project Development

Phase 1

Scheduled for project:

Tasks	Start Date	End Date	Duration
Research	5/1/2023	6/20/2023	50 days
Planning of project	5/15/2023	6/26/2023	42 days
Title Submission	6/9/2023	6/12/2023	4 days
Title Defense	6/13/2023	6/20/2023	8 days
Determine the project and its scope	6/17/2023	6/21/2023	5 days
Prepare a project plan and specification	6/22/2023	7/15/2023	24 days
Preliminary Defense/ Synopsis Defense	6/28/2023	6/30/2023	3 days
Progress Report	7/1/2023	8/2/2023	33 days
Feedback Report	7/26/2023	8/15/2023	21 days
Mid Defense	8/16/2023	8/19/2023	4 days
Improvements	8/18/2023	9/20/2023	34 days
Progress Report	9/1/2023	9/21/2023	20 days
Feedback Report	9/8/2023	9/16/2023	8 days
Final Draft Submission	9/14/2023	9/22/2023	8 days
Presentation preparation	9/16/2023	9/20/2023	9 days
Final presentation	9/24/2023	9/26/2023	3 days
Final Report submission	9/2/2023	9/24/2023	22 day
Documentation	7/9/2023	9/27/2023	100 days

Table 4: Project plan

gant chart of this schedule:

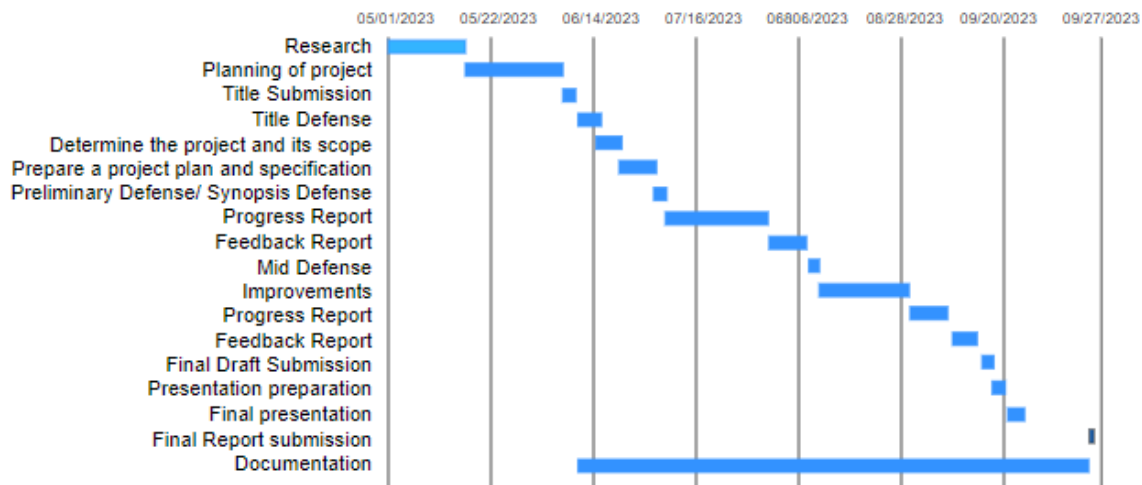


Figure 13: Expected gantt chart

Phase 2

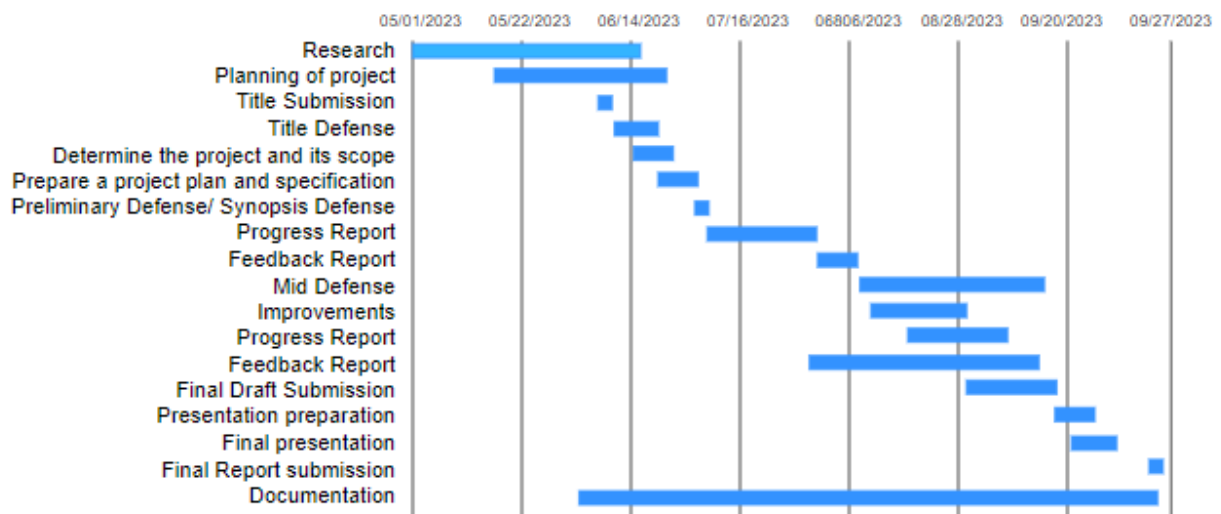
Schedule for phase 2:

Tasks	Start Date	End Date	Duration
Research	5/1/2023	6/29/2023	60 days
Planning of project	5/15/2023	6/26/2023	12 days
Title Submission	6/9/2023	6/21/2023	3 days
Title Defense	6/13/2023	6/28/2023	2 days
Determine the project and its scope	6/17/2023	6/22/2023	15 days
Prepare a project plan and specification	6/22/2023	7/21/2023	30 days
Preliminary Defense/ Synopsis Defense	6/28/2023	7/1/2023	3 days
Progress Report	7/1/2023	8/31/2023	40 days
Feedback Report	7/26/2023	8/15/2023	21 days
Mid Defense	8/16/2023	8/19/2023	4 days
Improvements	8/18/2023	9/21/2023	34 days

Progress Report	9/1/2023	9/21/2023	20 days
Feedback Report	9/8/2023	9/28/2023	10 days
Final Draft Submission	9/14/2023	9/22/2023	20 days
Presentation preparation	9/16/2023	9/25/2023	6 days
Final presentation	9/24/2023	9/26/2023	3 days
Final Report submission	9/2/2023	9/22/2023	22 day
Documentation	6/9/2023	9/26/2023	109 days

Table 5: Project plan

Gantt chart for schedule:

**Figure 14: Real gantt chart**

Appendix B: Questionnaires

Questionnaire to those who use Literature Review:	
Name.....	
Do you engage in Literature Review: for threat detection as part of your work or responsibilities?	Yes/No/Maybe
Are you able to efficiently analyze event logs from various sources?	Yes/No/Maybe
Have you ever used Literature Review: tools that provide insights into potential security threats and anomalies?	Yes/No/Maybe
Do you believe that Literature Review: plays a crucial role in enhancing threat detection capabilities?	Yes/No/Maybe
In your experience, have you come across Literature Review: tools that effectively identify and mitigate security threats?	Yes/No/Maybe
Do you face challenges in identifying potential threats within log data?	Yes/No/Maybe
Do you find it challenging to distinguish between genuine security threats and false alarms in your event Literature Review:	Yes/No/Maybe

Table 6: Questionnaire Sample

Sample Results

Questionnaire to those who use Literature Review:	
Name.....Jhalak Dahal.....	
Do you engage in Literature Review: for threat detection as part of your work or responsibilities?	Yes /No/Maybe
Are you able to efficiently analyze event logs from various sources?	Yes/ No /Maybe
Have you ever used Literature Review: tools that provide insights into potential security threats and anomalies?	Yes/ No /Maybe
Do you believe that Literature Review: plays a crucial role in enhancing threat detection capabilities?	Yes /No/Maybe
In your experience, have you come across Literature Review: tools that effectively identify and mitigate security threats?	Yes/No/ Maybe
Do you face challenges in identifying potential threats within log data?	Yes/ No /Maybe
Do you find it challenging to distinguish between genuine security	Yes/ No /Maybe

threats and false alarms in your event Literature Review:	
---	--

Table 7: Sample Result one

Questionnaire to those who use Literature Review:	
Name.....Riya Shrestha.....	
Do you engage in Literature Review: for threat detection as part of your work or responsibilities?	Yes /No/Maybe
Are you able to efficiently analyze event logs from various sources?	Yes/ No /Maybe
Have you ever used Literature Review: tools that provide insights into potential security threats and anomalies?	Yes/No/ Maybe
Do you believe that Literature Review: plays a crucial role in enhancing threat detection capabilities?	Yes /No/Maybe
In your experience, have you come across Literature Review: tools that effectively identify and mitigate security threats?	Yes/ No /Maybe
Do you face challenges in identifying potential threats within log data?	Yes/No/Maybe
Do you find it challenging to distinguish between genuine security threats and false alarms in your event Literature Review:	Yes/No/Maybe

Table 8: Sample Result two

Questionnaire to those who use Literature Review:	
Name.....Priya Shrestha.....	
Do you engage in Literature Review: for threat detection as part of your work or responsibilities?	Yes/No/Maybe
Are you able to efficiently analyze event logs from various sources?	Yes/No/Maybe
Have you ever used Literature Review: tools that provide insights into potential security threats and anomalies?	Yes/No/Maybe
Do you believe that Literature Review: plays a crucial role in enhancing threat detection capabilities?	Yes/No/Maybe
In your experience, have you come across Literature Review: tools that effectively identify and mitigate security threats?	Yes/No/Maybe
Do you face challenges in identifying potential threats within log data?	Yes/No/Maybe
Do you find it challenging to distinguish between genuine security threats and false alarms in your event Literature Review:	Yes/No/Maybe

Table 9: Sample Result three

Questionnaire to those who use Literature Review:	
Name.....Rohan KC.....	
Do you engage in Literature Review: for threat detection as part of your work or responsibilities?	Yes/No/Maybe
Are you able to efficiently analyze event logs from various sources?	Yes/No/Maybe
Have you ever used Literature Review: tools that provide insights into potential security threats and anomalies?	Yes/No/Maybe
Do you believe that Literature Review: plays a crucial role in enhancing threat detection capabilities?	Yes/No/Maybe
In your experience, have you come across Literature Review: tools that effectively identify and mitigate security threats?	Yes/No/Maybe
Do you face challenges in identifying potential threats within log data?	Yes/No/Maybe
Do you find it challenging to distinguish between genuine security threats and false alarms in your event Literature Review:	Yes/No/Maybe

Table 10: Sample Result four

Questionnaire to those who use Literature Review:	
Name.....Sushant Panta.....	
Do you engage in Literature Review: for threat detection as part of your work or responsibilities?	Yes /No/Maybe
Are you able to efficiently analyze event logs from various sources?	Yes /No/Maybe
Have you ever used Literature Review: tools that provide insights into potential security threats and anomalies?	Yes/ No /Maybe
Do you believe that Literature Review: plays a crucial role in enhancing threat detection capabilities?	Yes/ No /Maybe
In your experience, have you come across Literature Review: tools that effectively identify and mitigate security threats?	Yes /No/Maybe
Do you face challenges in identifying potential threats within log data?	Yes/ No / Maybe
Do you find it challenging to distinguish between genuine security threats and false alarms in your event Literature Review:	Yes /No/Maybe

Table 11: Sample Result four

Questionnaire to those who use Literature Review:	
Name.....Pratishma Dhungel.....	
Do you engage in Literature Review: for threat detection as part of your work or responsibilities?	Yes /No/Maybe
Are you able to efficiently analyze event logs from various sources?	Yes/ No /Maybe
Have you ever used Literature Review: tools that provide insights into potential security threats and anomalies?	Yes/ No / Maybe
Do you believe that Literature Review: plays a crucial role in enhancing threat detection capabilities?	Yes /No/Maybe
In your experience, have you come across Literature Review: tools that effectively identify and mitigate security threats?	Yes/ No /Maybe
Do you face challenges in identifying potential threats within log data?	Yes /No/Maybe
Do you find it challenging to distinguish between genuine security threats and false alarms in your event Literature Review:	Yes/ No /Maybe

Table 12: Sample Result five

Questionnaire to those who use Literature Review:	
Name.....Prince Shrestha.....	
Do you engage in Literature Review: for threat detection as part of your work or responsibilities?	Yes /No/Maybe
Are you able to efficiently analyze event logs from various sources?	Yes/ No / Maybe
Have you ever used Literature Review: tools that provide insights into potential security threats and anomalies?	Yes/ No /Maybe
Do you believe that Literature Review: plays a crucial role in enhancing threat detection capabilities?	Yes /No/Maybe
In your experience, have you come across Literature Review: tools that effectively identify and mitigate security threats?	Yes /No/Maybe
Do you face challenges in identifying potential threats within log data?	Yes/ No /Maybe
Do you find it challenging to distinguish between genuine security threats and false alarms in your event Literature Review:	Yes /No/Maybe

Table 13: Sample Result six

Questionnaire to those who use Literature Review:	
Name.....Rakesh Sharma.....	
Do you engage in Literature Review: for threat detection as part of your work or responsibilities?	Yes /No/Maybe
Are you able to efficiently analyze event logs from various sources?	Yes /No/Maybe
Have you ever used Literature Review: tools that provide insights into potential security threats and anomalies?	Yes /No/Maybe
Do you believe that Literature Review: plays a crucial role in enhancing threat detection capabilities?	Yes /No/Maybe
In your experience, have you come across Literature Review: tools that effectively identify and mitigate security threats?	Yes/ No /Maybe
Do you face challenges in identifying potential threats within log data?	Yes /No/Maybe
Do you find it challenging to distinguish between genuine security threats and false alarms in your event Literature Review:	Yes /No/Maybe

Table 14: Sample Result seven

Questionnaire to those who use Literature Review:	
Name.....Apekchya Karki.....	
Do you engage in Literature Review: for threat detection as part of your work or responsibilities?	Yes/No/Maybe
Are you able to efficiently analyze event logs from various sources?	Yes/No/Maybe
Have you ever used Literature Review: tools that provide insights into potential security threats and anomalies?	Yes/No/Maybe
Do you believe that Literature Review: plays a crucial role in enhancing threat detection capabilities?	Yes/No/Maybe
In your experience, have you come across Literature Review: tools that effectively identify and mitigate security threats?	Yes/No/Maybe
Do you face challenges in identifying potential threats within log data?	Yes/No/Maybe
Do you find it challenging to distinguish between genuine security threats and false alarms in your event Literature Review:	Yes/No/Maybe

Table 15: Sample Result eight

Questionnaire to those who use Literature Review:	
Name.....Ram Dahal.....	
Do you engage in Literature Review: for threat detection as part of your work or responsibilities?	Yes/No/Maybe
Are you able to efficiently analyze event logs from various sources?	Yes/No/Maybe
Have you ever used Literature Review: tools that provide insights into potential security threats and anomalies?	Yes/No/Maybe
Do you believe that Literature Review: plays a crucial role in enhancing threat detection capabilities?	Yes/No/Maybe
In your experience, have you come across Literature Review: tools that effectively identify and mitigate security threats?	Yes/No/Maybe
Do you face challenges in identifying potential threats within log data?	Yes/No/Maybe
Do you find it challenging to distinguish between genuine security threats and false alarms in your event Literature Review:	Yes/No/Maybe

Table 16: Sample Result nine

Questionnaire to those who use Literature Review:	
Name.....Pooja Shrestha.....	
Do you engage in Literature Review: for threat detection as part of your work or responsibilities?	Yes/No/Maybe
Are you able to efficiently analyze event logs from various sources?	Yes/No/Maybe
Have you ever used Literature Review: tools that provide insights into potential security threats and anomalies?	Yes/No/Maybe
Do you believe that Literature Review: plays a crucial role in enhancing threat detection capabilities?	Yes/No/Maybe
In your experience, have you come across Literature Review: tools that effectively identify and mitigate security threats?	Yes/No/Maybe
Do you face challenges in identifying potential threats within log data?	Yes/No/Maybe
Do you find it challenging to distinguish between genuine security threats and false alarms in your event Literature Review:	Yes/No/Maybe

Table 17: Sample Result ten

Summary of Results:

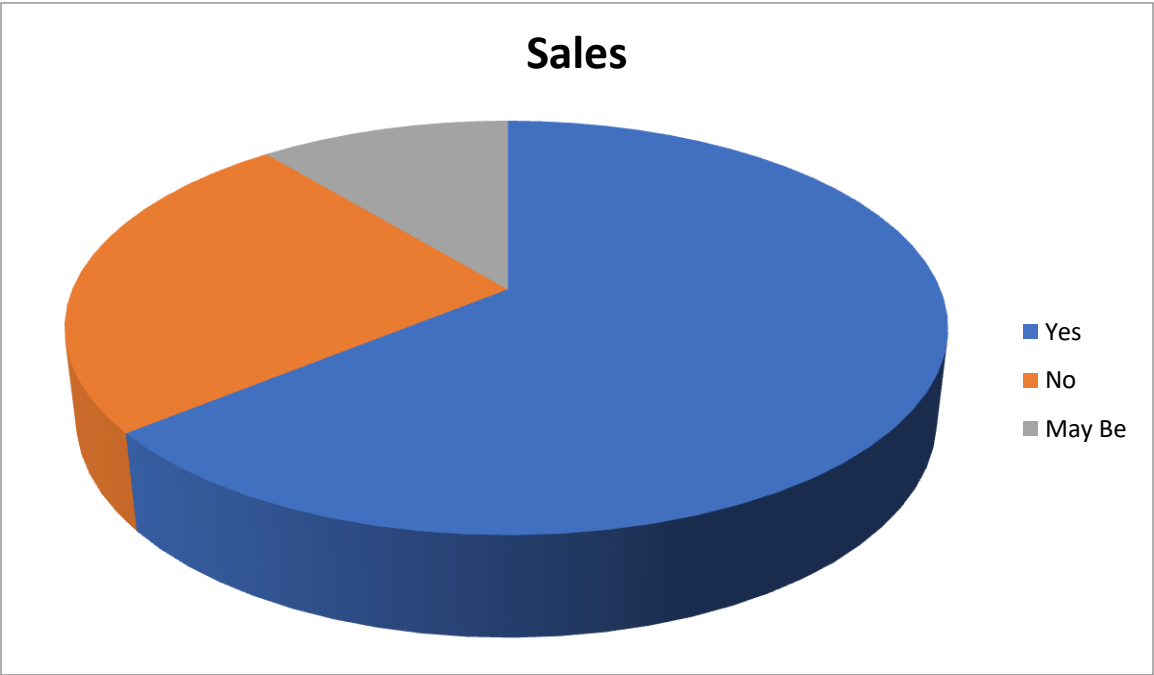


Figure 15: Summary of result

Appendix C: Project Simulation / DEMO

Step1: Ensure that the files are listed like in the figure:

```
project_folder/
|
|-- app.py
|-- templates/
|   |-- index.html
|
|-- static/
|   |-- style.css
|   |-- script.js
|
|-- log_files/
```

OR

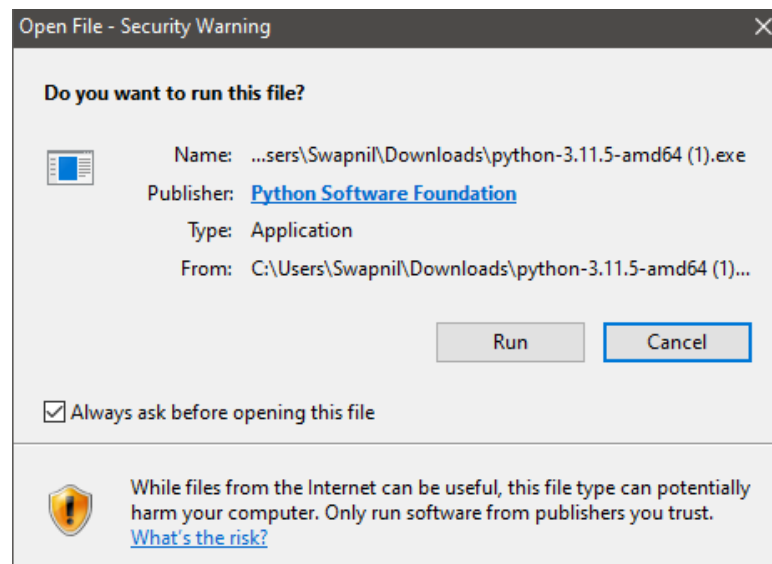
Texas > Final Year project > Final Code

Name	Date modified	Type	Size
static	9/18/2023 6:36 PM	File folder	
templates	9/18/2023 6:36 PM	File folder	
app	9/18/2023 6:42 PM	Python Source File	4 KB
logs 2	9/7/2023 10:34 AM	Text Document	29 KB
serverlogs	9/7/2023 10:34 AM	Text Document	19 KB

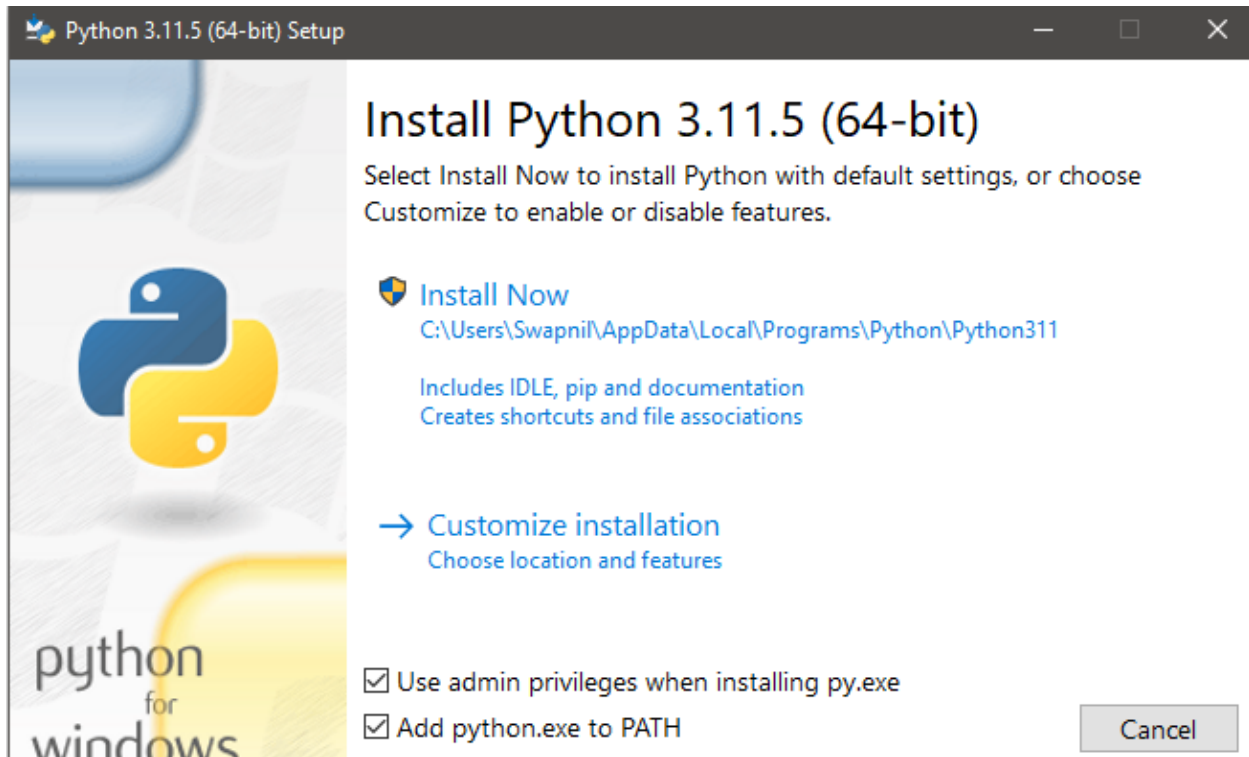
Step2: Ensure python is installed

Download the following application and follow the following instructions:

- a) [Python](#)



Select Run > add python to path > Install now



b) Pip

i) Enter command in windows power shell in windows:

➤ `curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py`

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py
PS C:\Users\Administrator>
```

OR

ii) Enter command in Command Prompt

➤ `python get-pip.py`

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.3324]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>python get-pip.py
```

Step 3: Install the necessary modules using command in PowerShell

- pip install Flask

```
PS C:\Users\Administrator> pip install flask
Requirement already satisfied: flask in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (2.3.3)
Requirement already satisfied: Werkzeug>=2.3.7 in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (from flask) (2.3.7)
Requirement already satisfied: Jinja2>=3.1.2 in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (from flask) (3.1.2)
Requirement already satisfied: itsdangerous>=2.1.2 in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (from flask) (2.1.2)
Requirement already satisfied: click>=8.1.3 in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (from flask) (8.1.7)
Requirement already satisfied: blinker>=1.6.2 in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (from flask) (1.6.2)
Requirement already satisfied: colorama in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (from click>=8.1.3->flask) (0.4.6)
Requirement already satisfied: MarkupSafe>=2.0 in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (from Jinja2>=3.1.2->flask) (2.1.3)
PS C:\Users\Administrator>
```

- pip install pandas






```
PS C:\Users\Administrator> pip install pandas
Requirement already satisfied: pandas in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (2.1.0)
Requirement already satisfied: numpy>=1.23.2 in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (from pandas) (1.25.2)
Requirement already satisfied: python-dateutil>=2.8.2 in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (from pandas) (2.8.2)
Requirement already satisfied: pytz>=2020.1 in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (from pandas) (2023.3.post1)
Requirement already satisfied: tzdata>=2022.1 in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (from pandas) (2023.3)
Requirement already satisfied: six>=1.5 in c:\users\administrator\appdata\local\programs\python\python311\lib\site-packages (from python-dateutil>=2.8.2->pandas) (1.16.0)
PS C:\Users\Administrator>
```

- Pip install NumPy

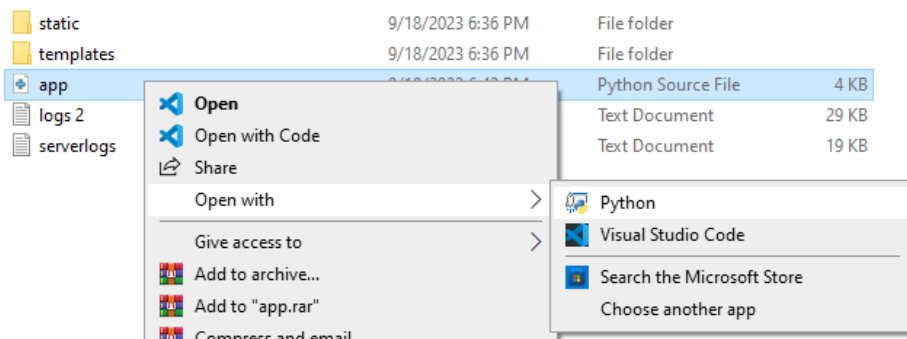
```
PS C:\Users\shres> pip install numpy
Requirement already satisfied: numpy in c:\users\shres\appdata\local\programs\python\python311\lib\site-packages (1.25.2)

[notice] A new release of pip available: 22.3.1 -> 23.2.1
[notice] To update, run: python.exe -m pip install --upgrade pip
PS C:\Users\shres>
```

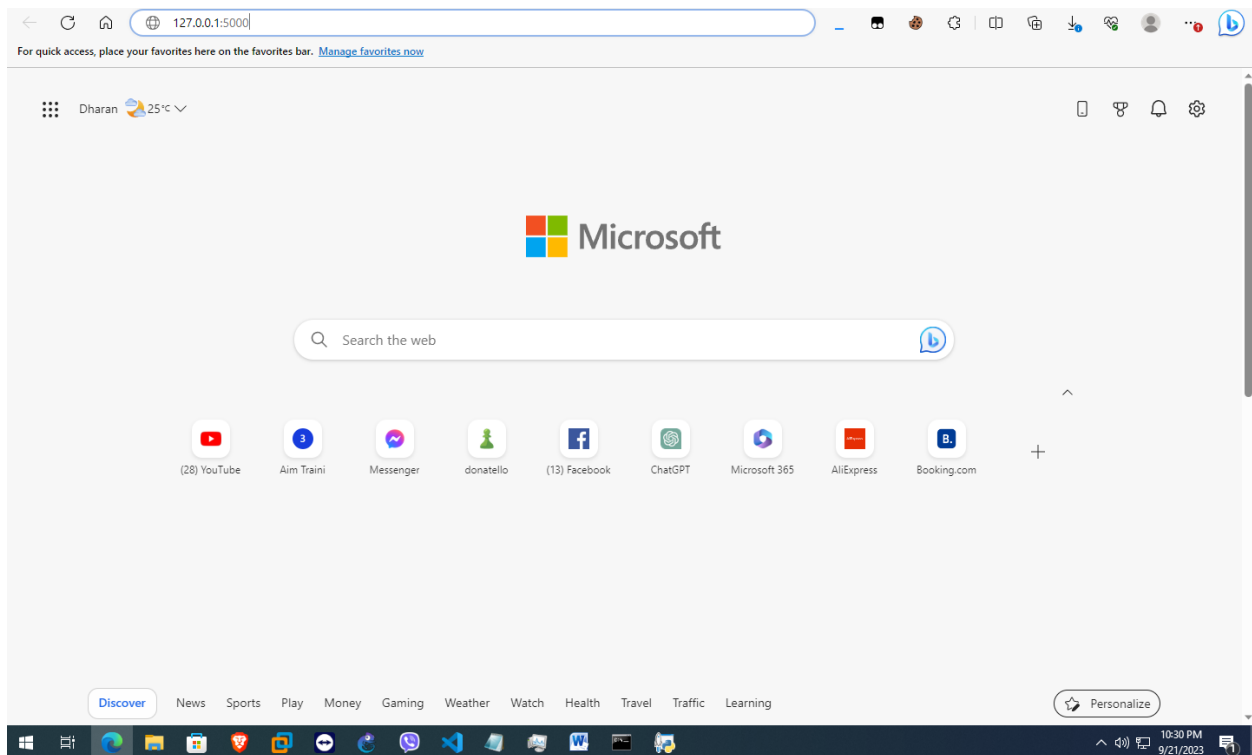
Step 4: Open the folder where you have downloaded the code file and open the file app.py with python.

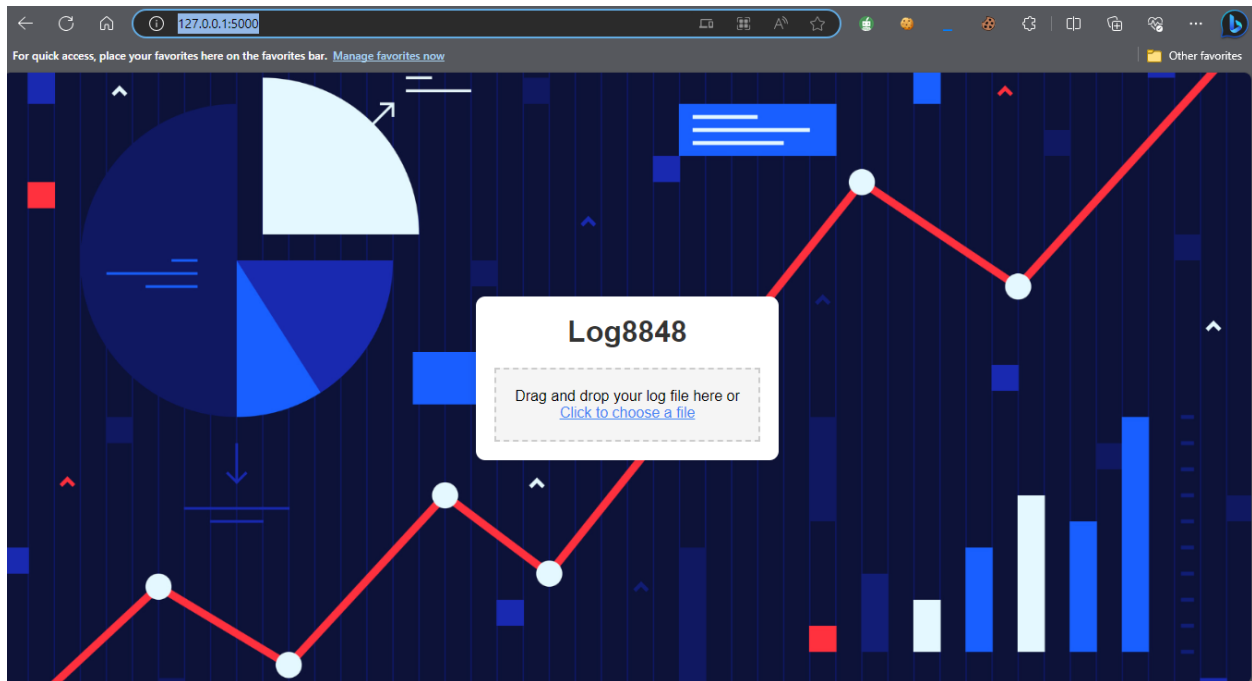
	static	9/18/2023 6:36 PM	File folder	
	templates	9/18/2023 6:36 PM	File folder	
	app	9/18/2023 6:42 PM	Python Source File	4 KB
	logs 2	9/7/2023 10:34 AM	Text Document	29 KB
	serverlogs	9/7/2023 10:34 AM	Text Document	19 KB

Open the file with python

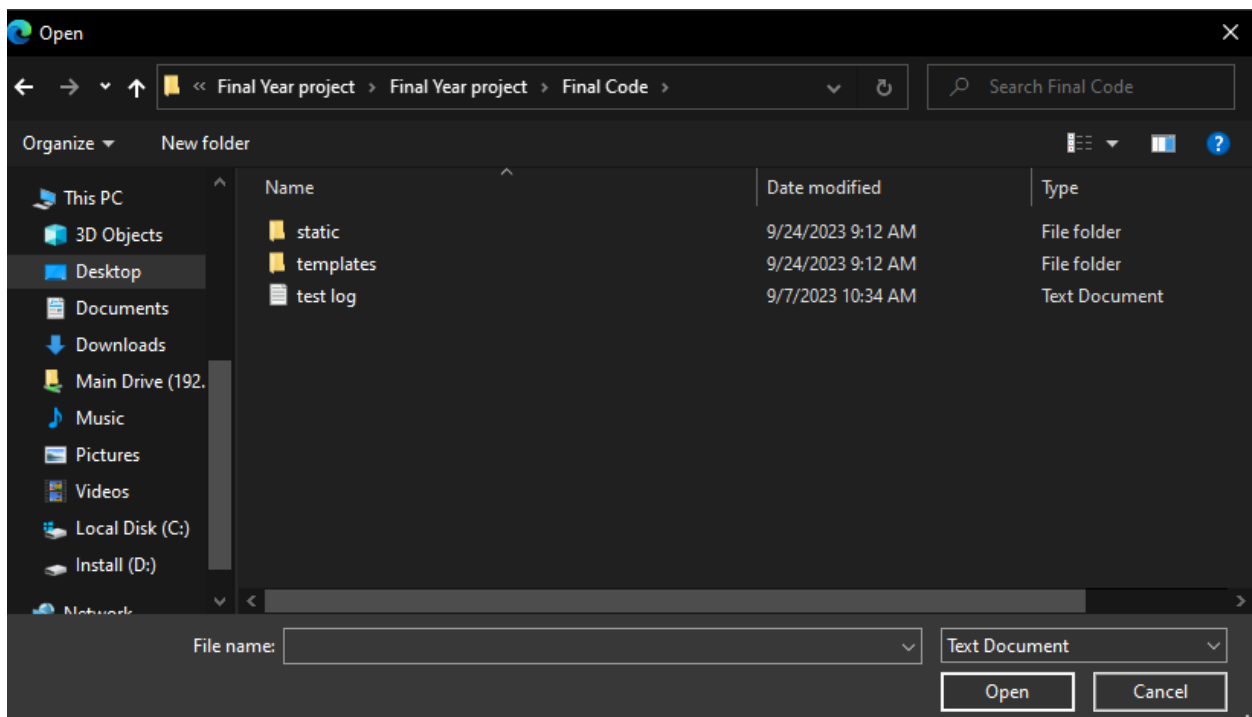


Step 5: Open any browser and open go to address: <http://127.0.0.1:5000/> or localhost:5000

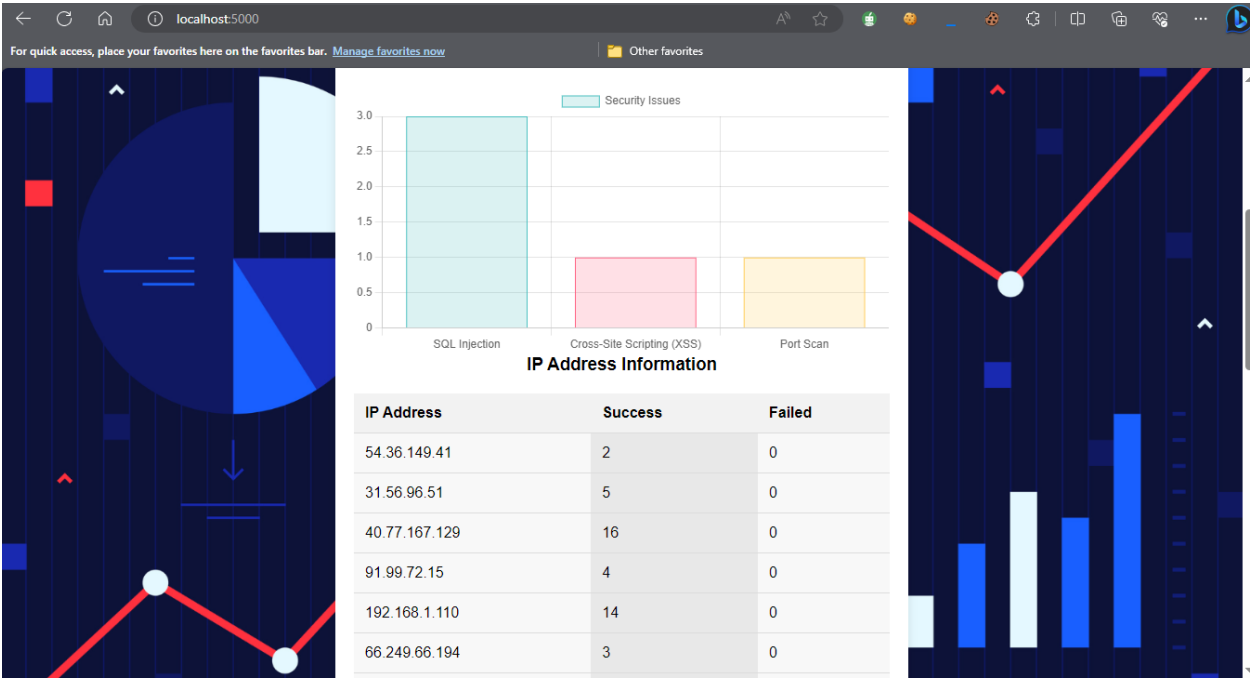
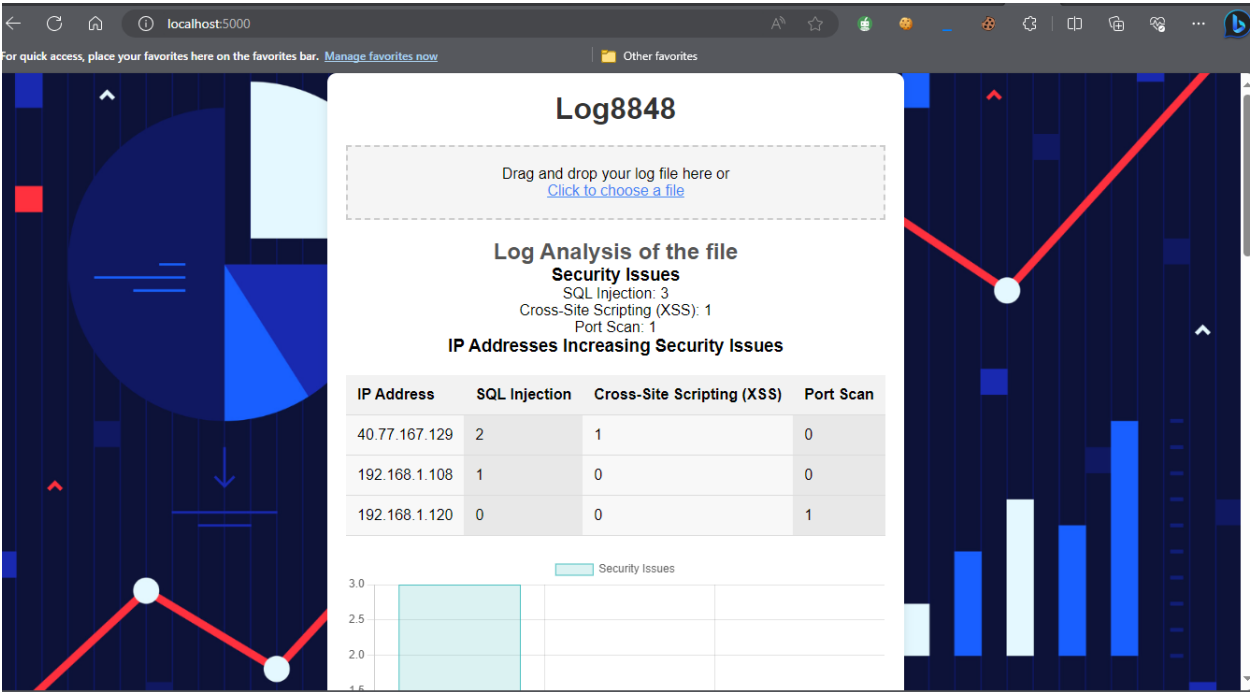




Step 6: Select the file you want to analyze, here in the Zip/project folder file you can see the test log file.



Step 7: Select the file and you are provided a result of the log file.



Appendix D: Comparison with other program.

Result comparison of Log8848 with [LogViewPlus](#):

test log.log - LogViewPlus - Admin

FileFilterToolsReportView

Open Log FileSave WorkspaceClose

OpenOpen Clone

Reload FileTime Offset

Save AnalysisExport Log Entries

How To VideosCheck for Updates

Settings

Log Files & Filters

test log.log

test log.log

Directory Monitors

C:\Users\Administrator\Desktop\Tex...

C:\Users\Administrator\Desktop\Tex...

Column1	Date	Time	Message
192.168.1.125	22 Jan 2023	2:30:05 PM.000	POST /login.php HTTP/1.1" 401 0 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1234.567 Safari/537.36" requestfailed: 1
192.168.1.126	22 Jan 2023	2:30:06 PM.000	POST /login.php HTTP/1.1" 401 0 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1234.567 Safari/537.36" requestfailed: 1
192.168.1.127	22 Jan 2023	2:30:07 PM.000	POST /login.php HTTP/1.1" 401 0 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1234.567 Safari/537.36" requestfailed: 1
192.168.1.128	22 Jan 2023	2:30:08 PM.000	POST /login.php HTTP/1.1" 401 0 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1234.567 Safari/537.36" requestfailed: 1
192.168.1.129	22 Jan 2023	2:30:09 PM.000	POST /login.php HTTP/1.1" 401 0 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1234.567 Safari/537.36" requestfailed: 1
192.168.1.130	22 Jan 2023	2:30:10 PM.000	POST /login.php HTTP/1.1" 401 0 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1234.567 Safari/537.36" requestfailed: 1
192.168.1.131	22 Jan 2023	2:30:11 PM.000	POST /login.php HTTP/1.1" 401 0 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1234.567 Safari/537.36" requestfailed: 1
40.77.167.129	22 Jan 2023	12:26:18 AM.000	GET /image/576/article/100x100 HTTP/1.1" 200 14776 "-" Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)" requestfailed: 110
40.77.167.129	22 Jan 2023	12:26:18 AM.000	GET /image/57710/productModel/100x100 HTTP/1.1" 200 1695 "-" Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)" requestfailed: 76
207.46.13.136	22 Jan 2023	12:26:18 AM.000	POST /product/10214 HTTP/1.1" 200 39677 "-" Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)" requestfailed: 182
40.77.167.129	22 Jan 2023	12:26:19 AM.000	GET /image/578/article/100x100 HTTP/1.1" 200 9831 "-" Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)" requestfailed: 184
40.77.167.129	22 Jan 2023	12:26:19 AM.000	PUT /m/product/32574/62991/%D9%85%D8%A7%D8%B4%D8%8C%D9%86-%D8%A7%D8%B5%D9%84%D8%A7%D8%AD-%D8%B5%D9%88%D8%B1%D8%AA-%D9%BE%D8%B1%D9%86%D8%B

40.77.167.129 - - [22/Jan/2023:03:56:19 +0330] "PUT /m/product/32574/62991/%D9%85%D8%A7%D8%B4%D8%8C%D9%86-%D8%A7%D8%B5%D9%84%D8%A7%D8%AD-%D8%B5%D9%88%D8%B1%D8%AA-%D9%BE%D8%B1%D9%86%D8%B

C:\Users\Administrator\Desktop\Final Year project\Final Code\test log.log

9:20 PM

9/27/2023

40.77.167.129

22 Jan 2023

12:26:19 AM.000

Page 69 of 80

Log File Analysis

Drag and drop your log file here or

[Click to choose a file](#)

Log Analysis of the file

Security Issues

SQL Injection: 3

Cross-Site Scripting (XSS): 1

Port Scan: 1

IP Addresses Increasing Security Issues

IP Address	SQL Injection	Cross-Site Scripting (XSS)	Port Scan
40.77.167.129	2	1	0
100.168.1.100	1	0	0

It is clear to us that the IP address 40.77.167.129 has been a source of confusion for both of the analyzers.

Other analyzers:

The majority of log analyzers now available on the market need users to pay for a subscription in order to use them:

Graylog: [GRAYLOG PRICING](#)

Checkmk: [Order Checkmk now](#)

Loggly: [Cloud Logging Service – Literature Review: and Aggregation Solution | Loggly](#)

-----Project Report Ends Here-----