Tunisian Republic
Ministry of Higher Education and Scientific Research
University of Tunis El Manar
National Engineering School of Tunis

Information and Communication Technologies Department
Communication

Engineering Internship Report

Elaborated by :

Seifeddine Ben Amor

Supervised by :

Ms. Gammoudi Mouna

Ms. Mahjoub Mariem

Hosting company :
NACS National Agency for Computer Security

Academic year: 2023/2024

Contents

List of Figures

Acronymes

GSI: Générale de service informatique
BDB: Bahrain Development Bank
ECA: Export Credit Agency
MVC: Model–view–controller
DAO: Data Access Object
SGBD: Systeme de gestion de base de données
IDE: Integrated development environment
POM: Modèle d'objet de projet
WYSIWYG: What You See Is What You Get
JEE: Java Enterprise Edition
XML: Extensible Markup Language

Acknowledgment

I would like to extend my sincere gratitude to Ms. Mariem MAHJOUB and Ms. Mouna GAMMOUDI, my esteemed supervisors at the National Agency for Computer Security (NASC). Their unwavering guidance, expertise, and encouragement have been invaluable throughout my internship journey. Their commitment to fostering my growth and learning has enriched my experience and broadened my horizons.

These past two months have been a whirlwind of energy and creativity. The challenges I encountered and the skills I acquired under their mentorship have been instrumental in my professional development. Their dedication to my progress has been a driving force, inspiring me to surpass my own expectations.

I would also like to express my heartfelt appreciation to the National Engineering School of Tunis for affording me this incredible opportunity. The partnership between my institution and the National Agency for Computer Security has provided me with an environment to apply my theoretical knowledge in a real-world setting. This experience has been truly transformative, allowing me to bridge the gap between academia and the professional world.

In conclusion, I acknowledge the immense impact of Ms. Mariem MAHJOUB, Ms. Mouna GAMMOUDI, and the entire National Agency for Computer Security team on my growth and learning. My gratitude also extends to the National Engineering School of Tunis for facilitating this internship program. The lessons I've learned and the experiences I've gained will undoubtedly shape my future endeavors in the field of computer security.

Introduction

In an era where the digital landscape forms the backbone of critical infrastructures and organizational functions, my summer internship project takes on heightened significance. My primary focus revolves around conceiving and developing an innovative web application tailored for the meticulous supervision of a national cyberspace.

This endeavor is driven by the integration of a multitude of APIs, enabling the acquisition of essential information from diverse organizations operating within this cyberspace. This wealth of data will undergo comprehensive analysis, serving as the foundation for a dynamic dashboard creation. This dashboard, meticulously designed, will serve as an intuitive masterpiece, distilling intricate data into easily understandable insights.

My journey throughout this project embarks on various phases, initiating with the exposition of the rationale and profound importance of a supervised national cyberspace. Subsequently, I delve into the intricate technical intricacies, shedding light on the pivotal role of APIs in data retrieval, subsequent analysis, and the seamless orchestration of a user-friendly dashboard. The pragmatic aspects of server deployment, system configuration, and the eventual implementation phase collectively form the tapestry of my expedition.

By crafting this exceptional web application, my aspiration is to fortify national cyber resilience while exemplifying the transformative prowess of cutting-edge technology in rendering cyberspace supervision effortlessly accessible and profoundly enlightening.

My forthcoming report will be meticulously organized into five distinct chapters, each contributing to a comprehensive understanding of my project's journey. The inaugural chapter is dedicated to establishing the broader context of my endeavor, shedding light on the overarching objectives and the significance of my project within its domain. Subsequently, I delve into the intricate technical intricacies and the specific needs and requirements in the second chapter, "Requirements Analysis and Specification" The third chapter, "Analysis and Design" sheds light on the pivotal role of APIs in data retrieval, subsequent analysis, and the seamless orchestration of a user-friendly dashboard. The pragmatic aspects of server deployment, system configuration, and the eventual implementation phase collectively form the tapestry of my expedition, detailed in the final chapter, "Realization and Validation".By crafting this exceptional web application, my aspiration is to fortify national cyber resilience while exemplifying the transformative prowess of cutting-edge technology in rendering cyberspace supervision effortlessly accessible and profoundly enlightening.

My forthcoming report will be meticulously organized into these four distinct chapters, each contributing to a comprehensive understanding of my project's journey. These chapters will offer a comprehensive perspective on the various facets of my project's evolution.

Chapter 1

General context of the project

1.1 Introduction

In this opening chapter, we embark on a journey of introduction. We'll acquaint ourselves with the hosting company's activities, partnerships, and delve into an overview of our project's essence. Additionally, we'll unveil the methodology that will guide our path forward. This chapter serves as the foundation upon which we build a deeper understanding of our project's context and aspirations.

1.2 Overview of the Hosting Company

1.2.1 Presentation:

Created in 2004, the National Agency for Computer Security, as national coordinator, works to develop a climate of trust in information technologies to reassure users, the state and investors and to protect citizens and public or private property against any cyber threat.
The strategy of the National Agency for IT Security is based on these axes:

- Strengthen the security of the national cyber space against cyber risks.
- Strengthen the protection of national information systems.
- PPromote the development of an adequate legal and regulatory framework.
- Establishing a partnership with academic research structures.

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Figure 1.1: Logo NASC
[**wakawakka**]

History

- 1999: Launch of a management unit by objective for the realization of the development of computer security within the State Secretariat of Information Technology.
- 2002:Modification of the role and structure of the unit.
- 2003: Restricted ministerial council dedicated to IT and information systems security which decided:
  The creation of a national agency specializing in the security of information systems.
  The introduction of a mandatory and periodic audit in the field of computer security.
  The creation of a body of certain auditors in information systems security.
- 2004: Creation of the National Computer Security Agency following Law No. 2004-5.

ANSI's organization chart

In accordance with Decree No. 635 of April 5, 2010 establishing the organization chart of the National Agency for Computer Security, here is the diagram representing the administrative organization of ANSI: From Figure 1.2, ANSI consists of 6 units and directorates managed by the CEO. The main units and directorates can be summarized as follows:

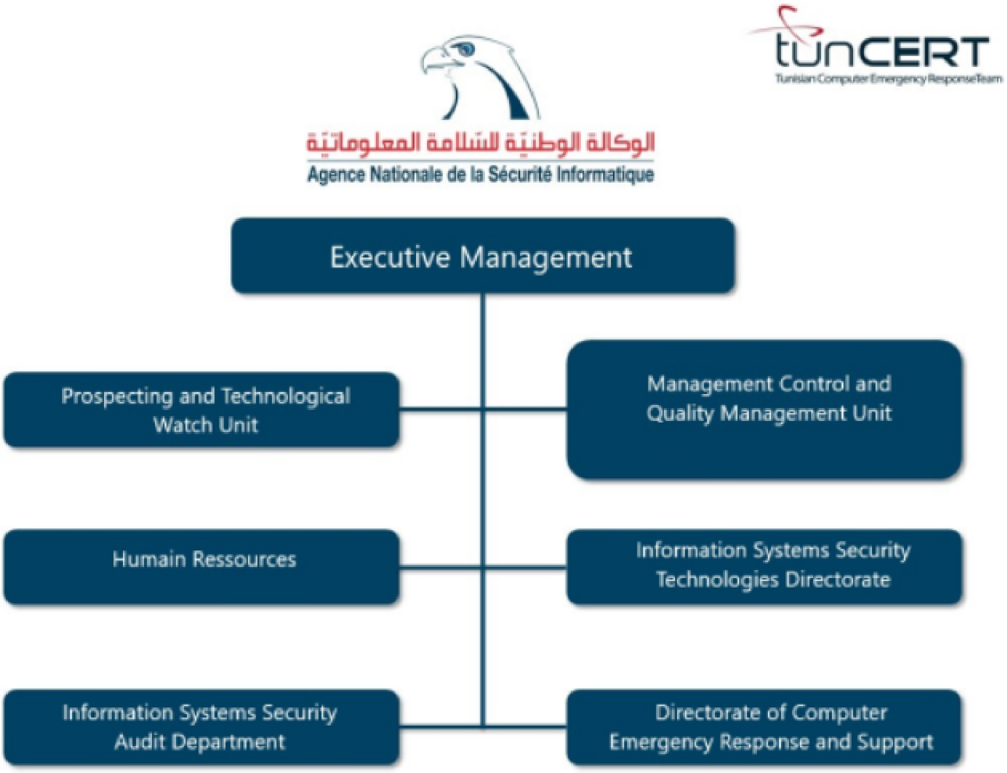

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique
tunCERT
Tunisian Computer Emergency Response Team
Executive Management
Prospecting and Technological Watch Unit
Management Control and Quality Management Unit
Humain Ressources
Information Systems Security Technologies Directorate
Information Systems Security Audit Department
Directorate of Computer Emergency Response and Support

Figure 1.2: NASC's organization chart

- Prospecting and technology watch unit: whose function is to follow scientific developments in the field of computer security and to provide technical tools to attract research and development projects.

- Management Control and Quality Management Unit: which prepares management and quality guides, monitors the preparation of statistics and monitors implementation.

- Information Systems Security Technologies Directorate: which intervenes during an incident or an attack on Tunisian networks and websites to carry out the processing and provide the necessary technical assistance. In addition, it assesses the level and effectiveness of the security mechanisms established at the national network level, by carrying out technical audit missions and white operations for the security of information systems of vital interest.

- Information Systems Security Audit Department: This department analyzes the security status of information systems and networks subject to the obligation to audit the security of their information systems by encouraging companies to adhere to the audit process and putting evaluation indicators.

- Directorate of Computer Emergencies Response and Support: which puts out guides and awareness programs for the public and specialists in the field and detects dangers and assesses them by directly announcing attacks that target the national cyber space. It also ensures coordination with similar international centers (CERTs) in order to identify and combat cybernetic risks and to exchange information on international developments in the field.

1.2.2 ANSI missions:

As part of the implementation of the national strategic choice in the field of computer security, and to meet the requirements of constant development assisted by the use of modern technologies and the integration of services and public and private institutions, the ANSI was created to ensure IT security and implement a specific national plan. Its main missions are:

- Ensure the execution of the national orientations and the general strategy in security systems of computer systems and networks.
- Monitor the execution of plans and programs relating to computer security in the public sector, with the exception of applications specific to defense and national security, and ensure coordination between stakeholders in this area.
- Ensure technology watch in the field of IT security.
- Establish specific IT security standards and develop technical guides on the subject and publish them.
- Work to encourage the development of national solutions in the field of computer security and to promote them in accordance with the priorities and programs to be set by the agency.
- Participate in the consolidation of training and retraining in the field of computer security.
- Ensure the implementation of the regulations relating to the obligation of the periodic audit of the security of computer systems and networks.

1.2.3 ANSI's services

The agency works to ensure a climate of trust in information technology for users, the state and investors. Also, it encourages citizens and public and private property to strengthen their security against any cyber threat. To achieve these objectives, the agency relies on 5 main areas that can be detailed as:
TunCERT: Tunisian Computer Emergency Response Team / Computer emergency response team:

- Provide online technical assistance (call-center, e-mail) to IT users, 12 hours a day, 7 days a week.
- Inform Internet users in “real time” about vulnerabilities and malicious activities observed nationally and internationally.

- Operate as an awareness-raising engine by setting up and executing the annual awareness program which sets up simple actions aimed at users of new technologies in order to raise their awareness to improve their online security.
- Observation and supervision of alerts in Tunisian cyberspace.
  DASSI: Information Systems Security Audit Department:
- Ensure the follow-up of Tunisian companies subject to the obligation of auditing the security of their information systems.
- Encourage companies to adhere to the process of auditing the security of their information systems.
- Evaluate the quality of audit reports and propose appropriate recommendations.
- Take charge of requests for certification and renewal of expert auditors in the field of information systems security and monitor the activity of expert auditors.
- Ensure the recognition of training in the field of information systems security.
  ISAC: Observation and Warning Center:
- Measure the national cyberspace alert level, by extracting global indicators informing about potential threats.
- Provide a platform for monitoring cyber-attacks and providing investigation support for computer security incidents.
- Install and develop solutions for detecting and tracing cyber-attacks using advanced technologies.
- Monitor critical nodes to detect anomalies and intrusions that can cause cyber- attacks.
- Detect attacks targeting websites hosted in national cyberspace.
  CSIRT: The computer incident response and handling team performs the following activities:
- Field intervention following an incident and handling IT security incidents.
- Collection and analysis of evidence to define the cause of the claim.
- National and international coordination following an information security incident.
- Receive incident notifications and take charge of them.
  DEAT: Study and technical assistance for national systems and projects:

- Assistance to the government and companies in the study of their needs in terms of information system security and the realization of the technical terms of reference for the acquisition of solutions or studies in information system security.

- Evaluation of the security of national systems within the framework of the implementation of national projects and national information processing platforms.

- Study and advice on information system security as part of the implementation of national projects.

1.3 Context of the Project:

In an era where the digital landscape forms the backbone of critical infrastructures and organizational functions, safeguarding and efficiently managing national cyberspaces have become paramount. Our solution was inspired by the wealth of data and resources available to us, motivating us to address the security of our national cyberspace. The relentless surge in cyber threats underscores the need for unwavering commitment to maintaining the resilience and security of these intricate digital ecosystems.

Our project, a pivotal component of the summer internship program within the second year of our Engineering degree in Telecommunication at the National Engineering School of Tunis, confronts the pressing challenge of ensuring the security and supervision of our national cyberspace. This undertaking is proposed by the National Agency for Computer Security, a cornerstone institution in the execution of its mission, including the encouragement and promotion of national cybersecurity solutions.

Our specific task was to conceptualize, construct, and develop a web application that would revolutionize the meticulous supervision of the national cyberspace. This endeavor not only provided us with a unique opportunity to apply the knowledge gained during our educational journey but also facilitated our transition into the professional sphere. Over the course of two months, we became immersed in the intricacies of the project and embraced the challenges it posed.

1.3.1 Preliminary Study:

Security assessment and risk management are essential components of cybersecurity aimed at identifying, analyzing, and mitigating security risks and vulnerabilities within an organization's information technology (IT) environment.

Security assessment:

Security assessment is a systematic process used to evaluate an organization's IT infrastructure, which includes systems, applications, and processes. Its main purpose is to identify vulnerabilities, weaknesses, and potential threats that could compromise the confidentiality, integrity, or availability of data and systems. Common types of security assessments include vulnerability assessments, penetration testing, security audits, and risk assessments. These assessments are essential for organizations to proactively manage and strengthen their cybersecurity defenses

Risk Management:

Risk management is a vital process for organizations aimed at protecting their assets and aligning with business objectives. It encompasses various key steps, beginning with the identification of potential security risks, both internal and external. These risks, spanning technology, personnel, processes, and third-party relationships, are then assessed to gauge their impact and likelihood, often involving risk scoring for prioritization. Mitigation strategies are developed and executed to reduce or eliminate these risks, incorporating security measures, policies, and employee training. Continuous risk monitoring ensures adaptability to emerging threats, while incident response and recovery plans are established to address security breaches. Lastly, compliance and reporting efforts ensure alignment with industry regulations and facilitate auditing and regulatory compliance.

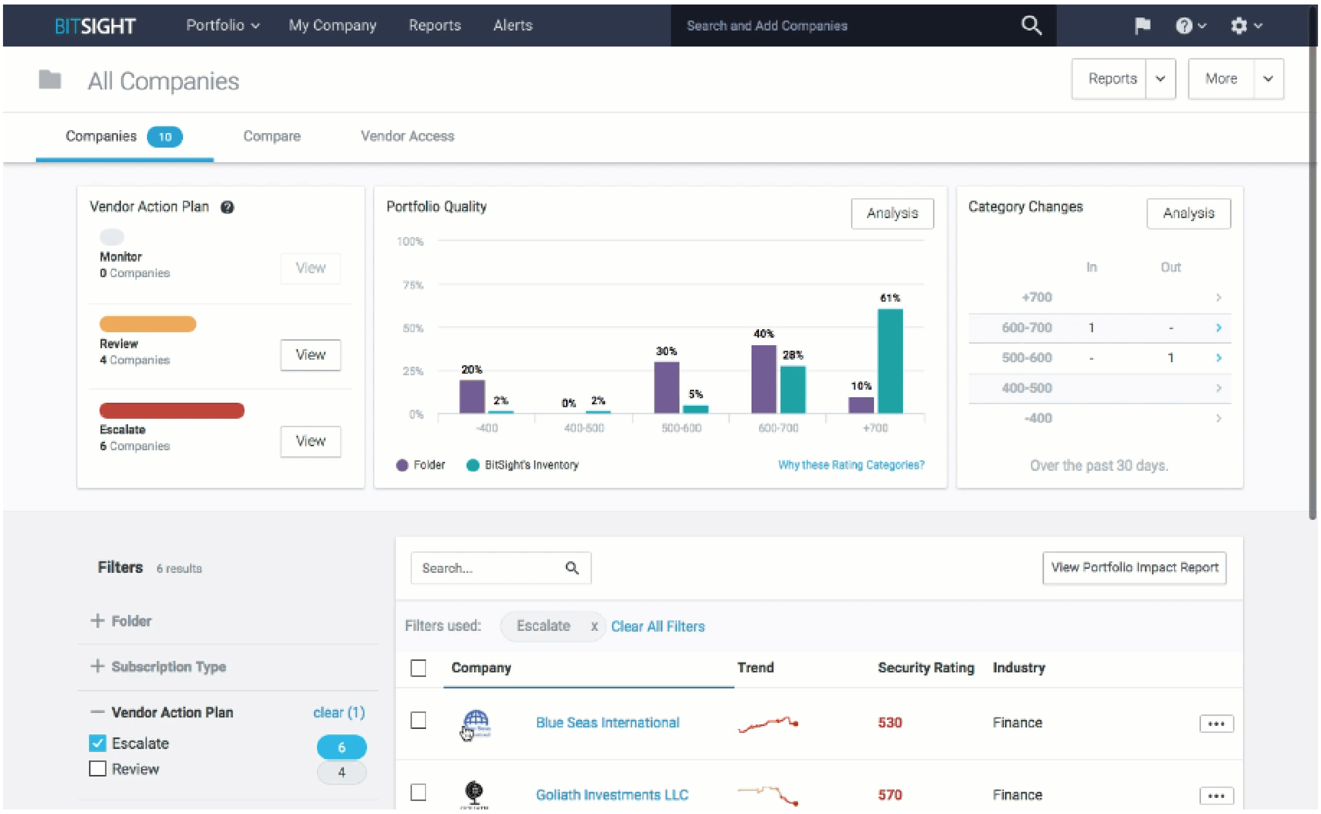
The importance of the project in security assessment and risk management:

In today's rapidly evolving digital landscape, where cyber threats continue to grow in complexity and sophistication, security assessment and risk management have become paramount for organizations of all sizes and sectors.
The interconnected nature of modern business operations, reliance on technology, and the constant exchange of data necessitate a proactive approach to safeguarding valuable assets and sensitive information.
Organizations face a multitude of risks, including data breaches, malware attacks, and vulnerabilities in their supply chains. Consequently, the need for robust security assessment tools,- such as a dashboard designed for the NASC (National Association of Security Companies) to access information on national organizations that contains their assets, contacts, and an analysis of whether their IP addresses and websites are malicious, harmful, or safe ...- has never been more acute. These tools empower NASC to comprehensively evaluate the security posture of the assets of the different organizations, enabling informed decision-making, risk mitigation, and the preservation of trust in an increasingly interconnected business environment. This project's contribution lies in its provision of a practical solution to aid organizations, especially those within the NASC, in navigating the complex terrain of cybersecurity, enhancing their resilience in the face of ever-evolving digital threats.

1.3.2 Existing Security Services:

Several cybersecurity rating services exist in the market, each with its own methodologies, data sources, and areas of expertise. Some of the well-known cybersecurity rating services are:

- BitSight: BitSight is a cybersecurity company that specializes in providing security ratings and risk assessment services. They offer a platform that assesses and monitors the cybersecurity posture of organizations and their third-party vendors. BitSight's core offering involves assigning security ratings to entities based on various data sources and analysis. These ratings help organizations evaluate the security risk associated with their own operations and those of their business partners, suppliers, or vendors.



	In	Out
+700		
600-700	1	-
500-600	-	1
400-500		
-400		

Over the past 30 days.

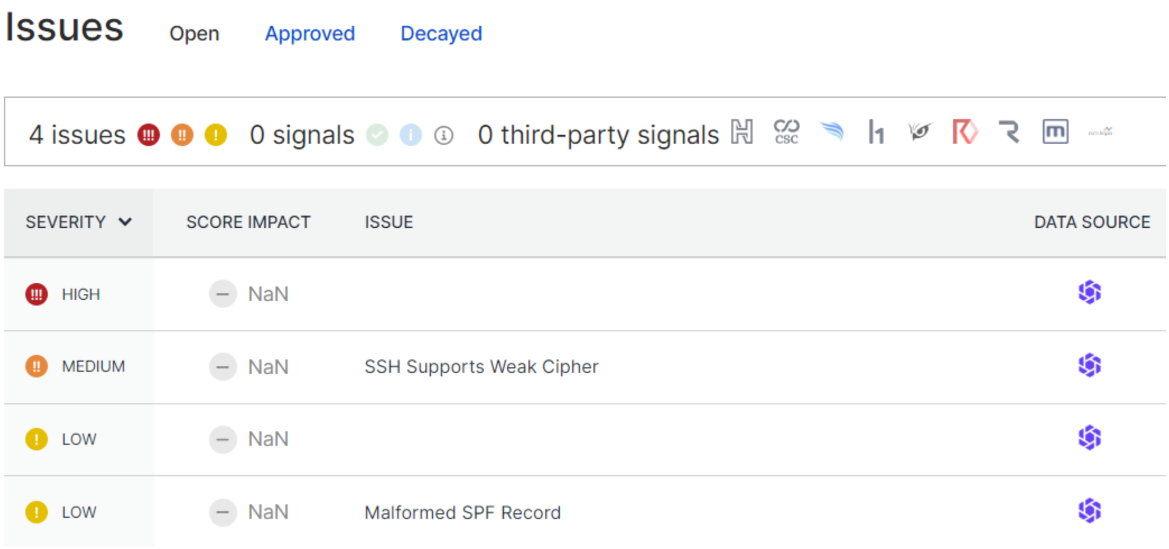
☑ Escalate 6
□ Review 4

Filters used: Escalate x Clear All Filters

□	Company	Trend	Security Rating	Industry	
□	Blue Seas International		530	Finance	•••
□	Goliath Investments LLC		570	Finance	•••

Figure 1.3: Bitsight's Dashboard

- SecurityScorecard: SecurityScorecard offers security ratings and risk assessments. They collect data from various sources, including web traffic, network traffic, and third-party data providers. Their rating system assesses factors such as DNS health, endpoint security, IP reputation, and patching cadence.



Issues Open Approved Decayed

4 issues 0 signals 0 third-party signals

SEVERITY	SCORE IMPACT	ISSUE	DATA SOURCE
HIGH	NaN		
MEDIUM	NaN	SSH Supports Weak Cipher	
LOW	NaN		
LOW	NaN	Malformed SPF Record	

Figure 1.4: SecurityScorecard

1.3.3 Critical analysis of the existing security services:

While BitSight and SecurityScorecard offer valuable insights into cybersecurity ratings and risk assessments, it's essential to recognize that even established players in this field have their limitations. These platforms provide organizations with high-level security ratings and risk assessments, enabling them to make informed decisions about their cybersecurity strategies. However, as with any tool, they have constraints that may affect their suitability for specific cybersecurity needs. Now, let's delve into some of the limitations of these platforms and introduce how our project addresses these challenges, offering a unique and innovative approach to cybersecurity assessment and monitoring.

- Frequency of Assessment: BitSight and SecurityScorecard typically provide periodic assessments, which may not capture rapidly evolving security threats.

- Limited Data Sources: BitSight and SecurityScorecard rely on specific data sources and standardized assessments, which may not capture certain nuances or unique security aspects of an organization.

- Port Scanning: BitSight and SecurityScorecard may not conduct port scanning, potentially missing vulnerabilities that could be detected through this method.

- Lack of Tailoring: These platforms typically do not allow organizations to customize the assessment process to focus on their particular areas of concern. Instead, they provide a standardized view of security, which may not align precisely with an organization's unique security needs and priorities.

In conclusion, this project takes inspiration from existing security services and aims to advance cybersecurity assessment and monitoring.
It introduces crucial features such as real-time monitoring, granular analysis,

customization, and port scanning.
Real-time monitoring provides timely responses in today's rapidly changing threat landscape, Granular analysis offers in-depth insights into assets aiding in pinpointing security weaknesses, Customization tailors assessments to meet unique security requirements, and port scanning adds an extra layer of vulnerability detection. This innovative approach, with a user-friendly dashboard, sets a new standard in security assessment, helping NASC to take action towards cyber-attacks.

1.3.4 The proposed solution:

The primary objective of our project was to develop a comprehensive web application designed to redefine the way organizations safeguard their digital assets and manage security risks within the national cyberspace. Our solution was envisioned as an innovative approach to security assessment and monitoring, introducing a multitude of crucial features to empower organizations in their cybersecurity endeavors.

Solution Overview:

The heart of our solution lies in a dynamic web application that seamlessly integrates data from various APIs, including sources like CriminalIP, AbuseIPDB, Virus Total, and more. These APIs provide invaluable information on IP addresses and domains, including data related to their potential malicious or harmful nature. The extracted features are processed and analyzed to determine the security posture of the entities in question.

Key Features:

- Real-Time Monitoring: The application offers real-time monitoring capabilities, providing organizations with up-to-the-minute updates. This feature is essential to address the dynamic and ever-evolving nature of cybersecurity threats, ensuring that organizations can respond promptly.

- Granular Analysis: Our solution provides in-depth insights into the security stance of IP addresses and domains. This granular analysis enables organizations to pinpoint specific vulnerabilities, weaknesses, and threats, allowing for precise remediation efforts.

- Customization: One of the core strengths of our solution is its customization options. Organizations can tailor security assessments to their unique needs and priorities. This flexibility ensures that assessments align precisely with the specific security requirements of each organization.

- Port Scanning: Our application incorporates port scanning capabilities to enhance the assessment process. This feature helps uncover open ports and potential weaknesses that may not be evident through other means.

- Dashboard: At the heart of the application, a user-friendly and flexible dashboard serves as the central hub for accessing security insights. The dashboard displays organizations and their contact information, along with the extracted features and assessments related to their IP addresses and domains.

Impact and Significance: The project's significance in the realm of cybersecurity assessment and risk management cannot be overstated. In a rapidly evolving digital landscape where cyber threats continue to grow in complexity, the need for advanced security solutions has never been more acute. Our solution empowers organizations, including the National Association of Security Companies (NASC), with the capabilities to proactively address cyber threats and enhance their security preparedness.

By providing real-time monitoring, granular analysis, customization, and port scanning, our project sets a new industry standard for advanced security insights and tailored risk management. It equips organizations with a powerful tool to navigate the complex cybersecurity landscape effectively and respond to cyber threats with agility and precision.

1.4 The modeling language:

In the development of our cybersecurity assessment and monitoring project, we employed Unified Modeling Language (UML) as a powerful modeling language to create a range of essential diagrams. UML served as a vital tool in visualizing and conceptualizing the various aspects of our project's architecture and design. Through UML, we crafted diagrams that encompassed system architecture, data flow, user interactions, and more. These UML diagrams not only facilitated a clear understanding of our project's structure but also played a pivotal role in guiding our development process. By utilizing UML, we ensured that our project was designed and implemented in a structured and well-organized manner, ultimately contributing to its effectiveness and efficiency in delivering advanced cybersecurity assessment capabilities

1.5 Conclusion:

In this chapter, we have laid the foundation for our project, offering a comprehensive overview of its environment, context, and challenges. We introduced the proposed solution, highlighting its innovative features and how it seeks to address existing cybersecurity assessment needs. Additionally, we conducted a comparative analysis with similar existing solutions to underscore the project's potential for advancement. In the forthcoming chapter, we delve deeper into the project's intricacies, presenting a preliminary study that elucidates its core concepts and embarks on a thorough requirements analysis. This critical phase of the project development process will further refine our understanding of the project's scope and the essential prerequisites for its successful implementation.

Chapter 2

Requirements Analysis And Specification

2.1 Introduction:

In the preceding chapter, we offered a comprehensive introduction to the project's context and unveiled the innovative solution we are proposing. Building upon this foundation, the focus now shifts to the heart of the project as we embark on an in-depth exploration of its requirements and functionality. This chapter is dedicated to articulating precisely what the product must accomplish and how it should perform its vital functions. Through a meticulous extraction of both functional and non-functional requirements, we aim to crystallize the project's specifications, providing a clear blueprint for its development.

2.2 Requirements Analysis

2.2.1 Functional Requirements

Functional requirements define the specific functions and features that a software system or project must possess to meet its objectives and provide value to users. In the context of your cybersecurity assessment and monitoring project, here are some functional requirements that you may consider:
User Authentication and Authorization:

- Implement a secure user authentication system to verify user identities.
- Define user roles and permissions to ensure appropriate access control.

User Dashboard:

- Create a user-friendly dashboard that displays security ratings, assessment results, and relevant insights.
- Provide a search and filter functionality for organizations and assets.

Real-Time Monitoring:

- Continuously collect and analyze data from various sources to provide real-time security updates.
- Send alerts and notifications to users in case of critical security events.

Granular Analysis:

- Conduct comprehensive assessments of organizations, assets, IP addresses, and websites.
- Generate detailed reports on security weaknesses and vulnerabilities.

Customization:

- Allow users to customize their security assessments by selecting specific data sources and criteria.
- Provide the ability to configure assessment frequency and depth.

Port Scanning:

- Implement port scanning functionality to identify open ports on assessed systems.
- Integrate the results of port scans into security assessments.

Integration with External APIs:

- Connect and retrieve data from external sources like TotalVirus, Shodan, AbuseIPDB, and Censys.
- Ensure seamless data synchronization and updates.

Reporting and Analytics:

- Generate comprehensive reports with visualizations to summarize security assessments.
- Offer historical data and trend analysis for security improvements.

User Management:

- Allow admins to manage user accounts, including adding, modifying, and deactivating accounts.
- Support password management and account recovery options.

These functional requirements form the basis for the capabilities and features of your cybersecurity assessment and monitoring project. They guide the development process to ensure that the final product meets the needs of organizations seeking advanced security insights and tailored risk management solutions.

2.2.2 Non-functional requirements:

Non-functional requirements define the qualities, characteristics, and constraints that your cybersecurity assessment and monitoring project must adhere to, rather than specific features or functions. Here are some non-functional requirements to consider for your project:

Performance: The system should respond promptly to user interactions, with minimal latency. It should support a large number of concurrent users and assessments without degradation in performance.

Scalability: The system should be scalable, allowing for easy expansion to accommodate increasing data volumes and user loads.

Availability: The system should aim for high availability, with minimal downtime for maintenance and updates. Define acceptable uptime percentages (e.g., 99.%) in service level agreements (SLAs).

Reliability: Ensure that the system operates reliably and consistently, with minimal errors or crashes. Implement robust error handling and recovery mechanisms.

Security: Data security is paramount. Encrypt sensitive data during transmission and storage. Comply with industry standards and regulations for data privacy and protection.

Data Integrity: Guarantee the accuracy and consistency of data across the system. Implement data validation and verification mechanisms.

Usability: The user interface should be intuitive and user-friendly, requiring minimal training for users. Conduct usability testing to gather user feedback for improvements.

Interoperability: Ensure that the system can integrate with external APIs and data sources seamlessly. Use industry-standard protocols for data exchange and communication.

Maintainability: Develop the system with modular and well-documented code to facilitate maintenance and updates. Implement version control and change management processes.

Monitoring and Logging: Implement comprehensive monitoring and logging to track system performance, security events, and user activities. Use log analysis tools to identify issues proactively.

Disaster Recovery: Establish a disaster recovery plan that includes regular data backups, off-site storage, and procedures for system restoration in case of failures or data loss.

Resource Utilization: Optimize the use of system resources, such as memory and processing power, to minimize resource consumption.

Load Testing: Conduct load testing to evaluate the system's performance under various loads, ensuring it meets defined performance requirements. These non-functional requirements are essential to ensure that your cybersecurity assessment and monitoring project not only delivers valuable functionality but also meets the essential performance, security, and compliance standards expected in today's complex cybersecurity landscape.

2.3 Requirements and Specification:

2.3.1 Actors Identification

Employee

Employees are individuals or entities that utilize the system to assess and monitor their cybersecurity posture.
They are responsible for:

- Initiating assessments: Creating and managing security assessments for organizations.
- Viewing reports: Accessing assessment reports and insights.
- Customization: Tailoring assessments based on specific criteria and needs.

Permissions: Users have access to the system's assessment and reporting features based on their organizational role.

Admin

Admins are responsible for managing and overseeing the cybersecurity assessment and monitoring system. They are responsible for:

- User management: Creating, modifying, and deactivating user accounts.
- Configuration: Setting system parameters and customization options.
- Data management: Ensuring data accuracy, privacy, and compliance.
- Incident response: Addressing security incidents and critical alerts.

Permissions: Admins have full access to all system features and data.

General Use Case:

Customize Assessment Criteria:

Actor: The admin
Description: The admins have the option to customize assessment criteria based on their organization's specific security needs. They can select data sources, assessment frequency, and depth of analysis.

View Assessment Reports:

Actor: Normal User
Description: After initiating an assessment, users can access and view detailed assessment reports. These reports provide insights into the organization's security posture and vulnerabilities.

User Management:

Actor: admin
Description: admins have the authority to manage user accounts within the system. They can create, modify, or deactivate user accounts, ensuring that access control

is maintained.
Configuration and Settings:
Actor: admin
Description: Admins can configure system parameters and settings. This includes defining assessment criteria, data sources, and customization options for users.
Monitoring and Reporting:
Actor: admin
Description: admins monitor the overall system performance, security events, and user activities. They can generate comprehensive reports and analytics to track security improvements and trends.
Customization Oversight:
Actor: admin
Description: Admins oversee the customization options available to normal users. They may provide guidance and support in tailoring security assessments to meet specific organizational needs.
The following figure presents the general functionalities that the system offers:

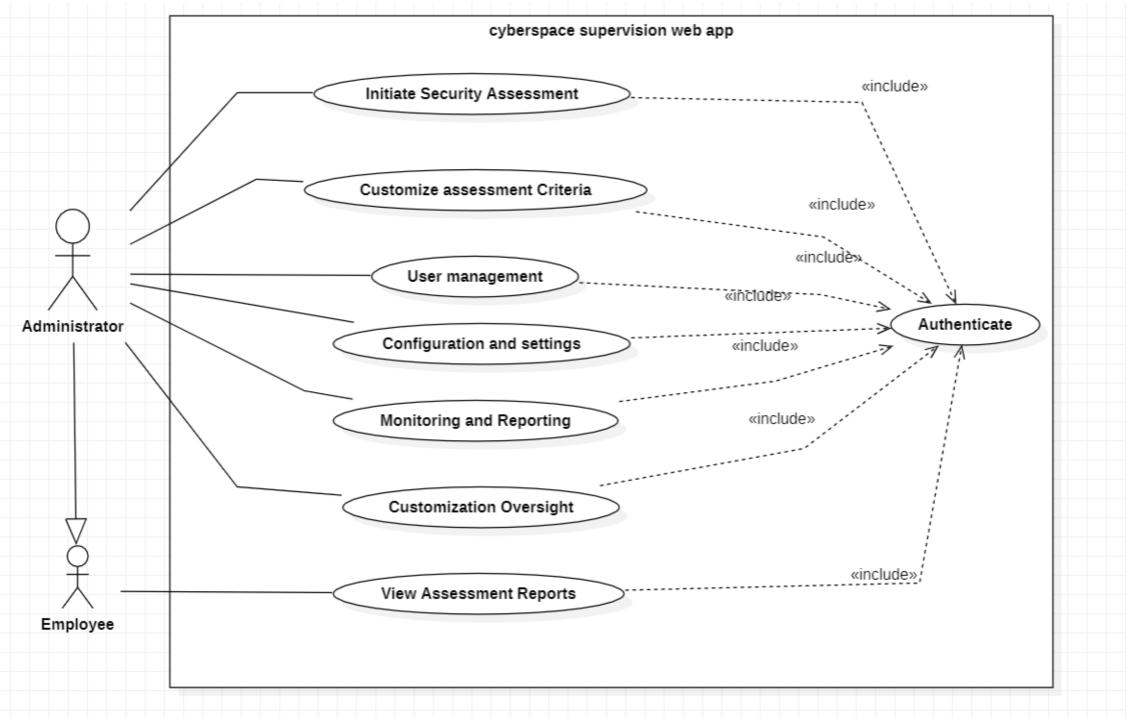


Figure 2.1: Use Case diagram

The use case diagram contains the actions by each actor and the depends on each one.

The Detailed Use Cases:

In this section, we will detail the most important use cases:
Initiate Security assessment:

The admin is able to manage, add, delete and update the security assessment. The following Figure represents the detailed use case diagram of “Initiate security assessment ":

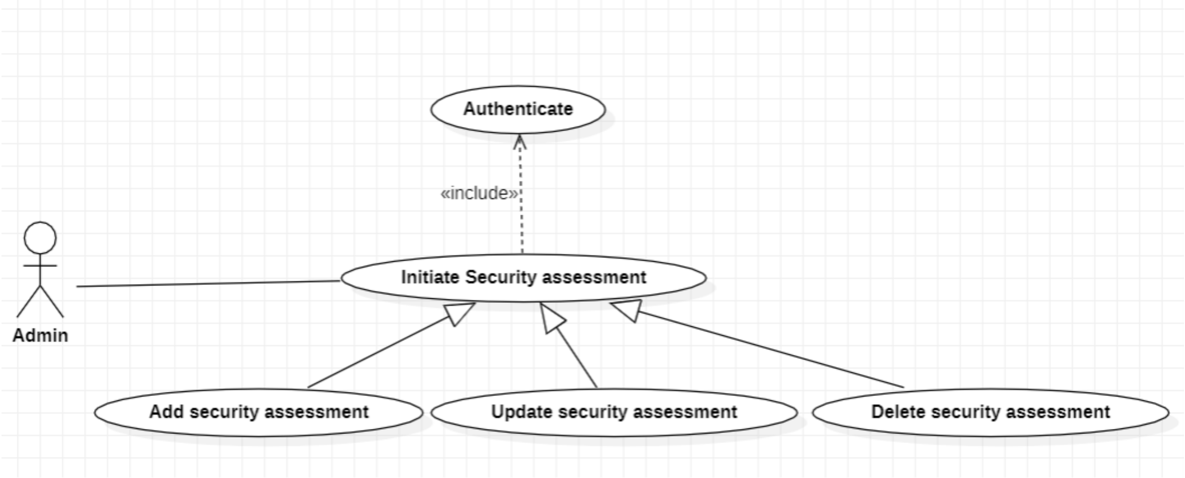

Authenticate
«include»
Admin
Initiate Security assessment
Add security assessment
Update security assessment
Delete security assessment

Figure 2.2: Manage the security assessment

User Management

The admins is able to manage, to add, delete and update the user’s information. The following Figure represents the detailed use case diagram of “User Management":

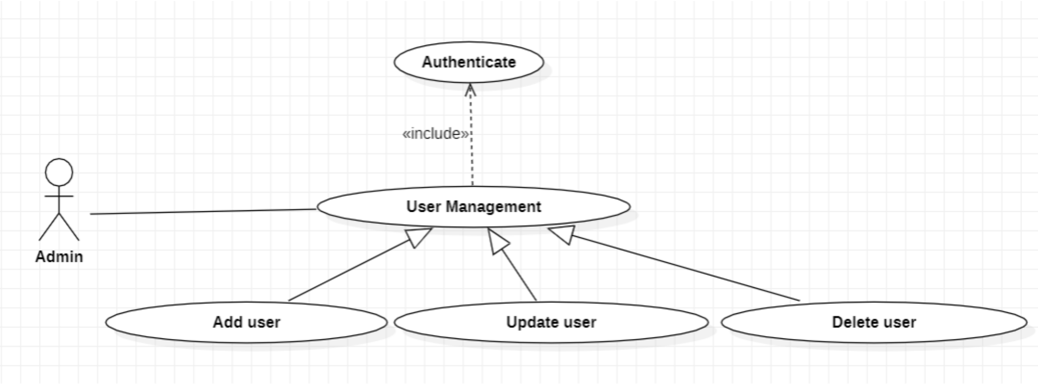


Figure 2.3: User Management

Configuration and settings:

The admin can manage, add, delete, and update organization information. The following Figure represents the detailed use case diagram of “Configuration and settings ":

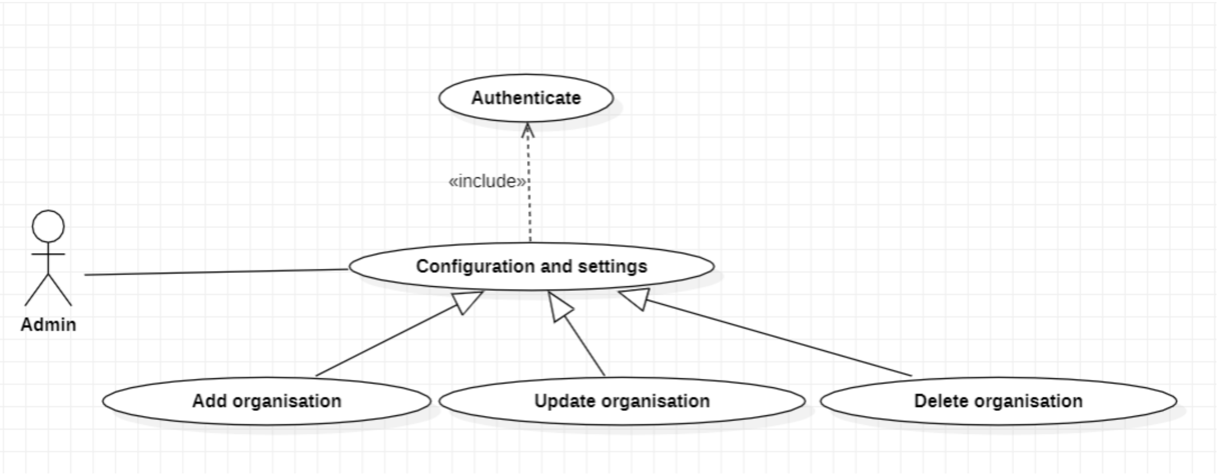


Figure 2.4: Configuration and settings

2.4 Conslusion:

Throughout the requirements analysis and the requirements specification presented in this chapter, we have clearly identified the system actors and the functionality that the product should offer. Indeed, the next chapter displays the global and detailed design of the solution permitting to perform these requirements.

Chapter 3

Analysis and Design

3.1 Introduction

In this pivotal third chapter of my internship project report, we embark on a journey into the intricate realms of web application analysis and design. Building upon the solid foundation laid in the preceding chapters, where I meticulously elucidated the project's requirements and specifications, this chapter delves deeper into the project's core. Here, I meticulously craft a vivid depiction of the project's anatomy through the presentation of a comprehensive class diagram. Furthermore, we shine a spotlight on the development environment, unraveling the intricate architectural patterns that have been ingeniously woven into the fabric of our application. In doing so, we pave the way for a thorough understanding of the underlying framework that breathes life into our web application, setting the stage for a captivating exploration of its development journey.

3.2 Development Environment

3.2.1 UML Diagram:

Class Diagram:

The class diagram holds a significant position in the world of object-oriented modeling, playing a pivotal role within the structural diagrams of the Unified Modeling Language (UML). Known for its expressive syntax, the class diagram stands out as one of the most commonly used UML diagrams. It serves as a central tool in illustrating the core structure of an object-oriented application, revealing the intricate relationships among classes. Much like the architectural blueprint of a grand building, the class diagram provides a comprehensive visual representation of the foundational elements that shape an entire software system. This ensures that the development process adheres to a clear and well-structured design. Within our project's context, the class diagram acts as a crucial roadmap, guiding the development of our supervisory app for the national cyberspace using

Flask. It promotes effective communication and enhances project stakeholders' understanding of the system's architecture.
In order to illustrate the class diagram defined above, we present the following figure displays the different classes and relationships between them :

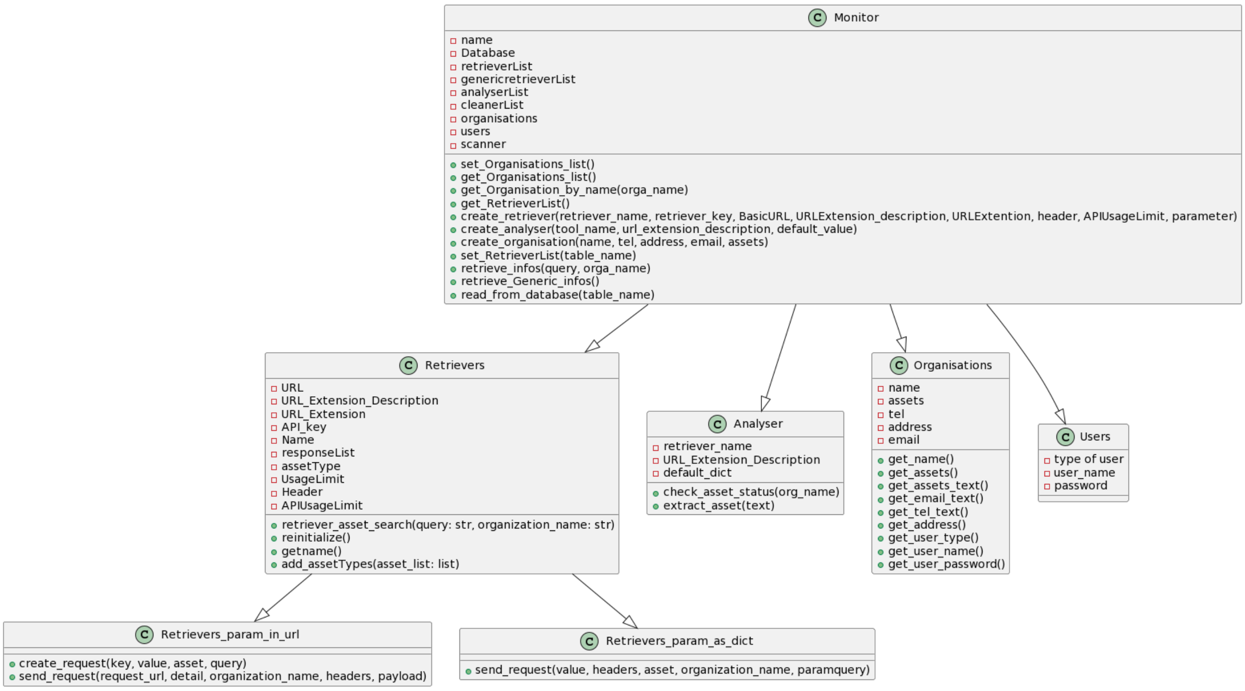

Monitor
name
Database
retrieverList
genericretrieverList
analyserList
cleanerList
organisations
users
scanner
set_Organisations_list()
get_Organisations_list()
get_Organisation_by_name(orga_name)
get_RetrieverList()
create_retriever(retriever_name, retriever_key, BasicURL, URLExtension_description, URLExtention, header, APIUsageLimit, parameter)
create_analyser(tool_name, url_extension_description, default_value)
create_organisation(name, tel, address, email, assets)
set_RetrieverList(table_name)
retrieve_infos(query, orga_name)
retrieve_Generic_infos()
read_from_database(table_name)
Retrievers
URL
URL_Extension_Description
URL_Extension
API_key
Name
responseList
assetType
UsageLimit
Header
APIUsageLimit
retriever_asset_search(query: str, organization_name: str)
reinitialize()
getname()
add_assetTypes(asset_list: list)
Analyser
retriever_name
URL_Extension_Description
default_dict
check_asset_status(org_name)
extract_asset(text)
Organisations
name
assets
tel
address
email
get_name()
get_assets()
get_assets_text()
get_email_text()
get_tel_text()
get_address()
get_user_type()
get_user_name()
get_user_password()
Users
type of user
user_name
password
Retrievers_param_in_url
create_request(key, value, asset, query)
send_request(request_url, detail, organization_name, headers, payload)
Retrievers_param_as_dict
send_request(value, headers, asset, organization_name, paramquery)

Figure 3.1: Class Diagram

Retrievers		
Description	**Attributes**	**Methods**
Collects data from various sources.	• URL • URL_Extension • API_key • Name • responseList • assetType • UsageLimit • Header • APIUsageLimit	• retriever_asset_search(self, query, organization_name: str): Searches for assets based on a query and organization name. • reinitialize(self): Resets the retriever's state. • getname(self): Retrieves the retriever's name. • add_assetTypes(self, assetlist: list): Adds asset types to the retriever.

Table 3.1: Class Retrievers

<table>
<tr><th colspan="3">Retrievers_param_in_url</th></tr>
<tr><th>Description</th><th>Attributes</th><th>Methods</th></tr>
<tr><td>Inherits from Retrievers and adds URL parameters.</td><td>• URL</td><td>• retriever_asset_search(self, query, organization_name): Searches for assets based on a query and organization name.
• create_request(self, key, value, asset, query): Creates a request with specified parameters.
• send_request(self, request_url, detail, organization_name, headers, payload): Sends a request to the specified URL.</td></tr>
</table>

Table 3.2: Retrievers_param_in_url

Retrievers_param_as_dict		
Description	**Attributes**	**Methods**
Description: Inherits from Retrievers and adds parameters as a dictionary.	• parameter	• retriever_asset_search(self, query, organization_name): Searches for assets based on a query and organization name. • send_request(self, value, headers, asset, organization_name, paramquery): Sends a request with specified parameters.

Table 3.3: Class Retrievers_param_as_dict

Analyser		
Description	**Attributes**	**Methods**
Description: Analyzes data received from Retrievers.	• retriever_name • URL_Extension_Description • default_dict	• check_asset_status(self, org_name): Checks the status of an asset for a specific organization. • extract_asset(text): Extracts asset information from text data.

Table 3.4: Class Analyser

Organization		
Description	**Attributes**	**Methods**
Stores information about organizations.	• name • assets • tel • address • email	• get_name(self): Retrieves the organization's name. • get_assets(self): Retrieves the organization's assets. • get_assets_text(self): Retrieves the textual representation of the organization's assets. • get_email_text(self): Retrieves the textual representation of the organization's email. • get_tel_text(self): Retrieves the textual representation of the organization's telephone number. • get_address(self): Retrieves the organization's address. • get_user_type(self): Retrieves the type of user. • get_user_name(self): Retrieves the user's name. • get_user_password(self): Retrieves the user's password.

Table 3.5: Class Organisations

Monitor		
Monitor	**Attributes**	**Methods**
Manages Retrievers, Analysers, and Organizations.	• name • Database • retrieverList • genericretrieverList • analyserList • cleanerList • organisations • users • scanner	• set_Organisations_list(self): Sets the list of organizations. • get_RetrieverList(self): Retrieves the list of retrievers. • create_analyser(tool_name, url_extension_description, default_value): Creates an analyser. • create_organisation(name, tel, address, email, assets): Creates an organization. • retrieve_infos(self, query, orga_name): Retrieves information based on a query and organization name. • read_from_database(self, table_name): Reads data from the database. • add_retriever(self, new_data): Adds a retriever. • update_retriever_by_id(self, retriever_id, updated_data): Updates a retriever by ID. • set_analyserList(self): Sets the list of analysers. • analyse_organisation(self, orga_name): Analyzes an organization. • add_organisation(self, new_data): Adds an organization. • update_organisation_by_id(self, organisation_id, updated_data): Updates an organization by ID. • add_analyser(self, new_data): Adds an analyser.

Table 3.6: Class Monitor

<table>
<tr><th colspan="3">Users</th></tr>
<tr><th>Description</th><th>Attributes</th><th>Methods</th></tr>
<tr><td>Manages user information and access control.</td><td>• type of user
• user_name
• password</td><td></td></tr>
</table>

Table 3.7: Class Users

Sequence Diagram:

The sequence diagram is a graphical representation of the interactions between the actors and the system in chronological order in the Unified Modeling Language formulation. It is part of behavioral diagrams (dynamic) and more precisely interaction diagrams. It shows the order of message exchanges and the passage of time. It is called temporal diagram. It allows you to show object interactions as part of a scenario of a Use Case Diagram.The goal is to describe how the actions take place between the actors or objects It includes a group of objects, represented by lifelines, and the messages that these objects exchange during the interaction.The main information contained in a sequence diagram are the messages exchanged between the lifelines This section details the most important object interactions: visualizing information on the dashboard.
In order to illustrate the sequence diagram defined above, here is its sequence diagram :

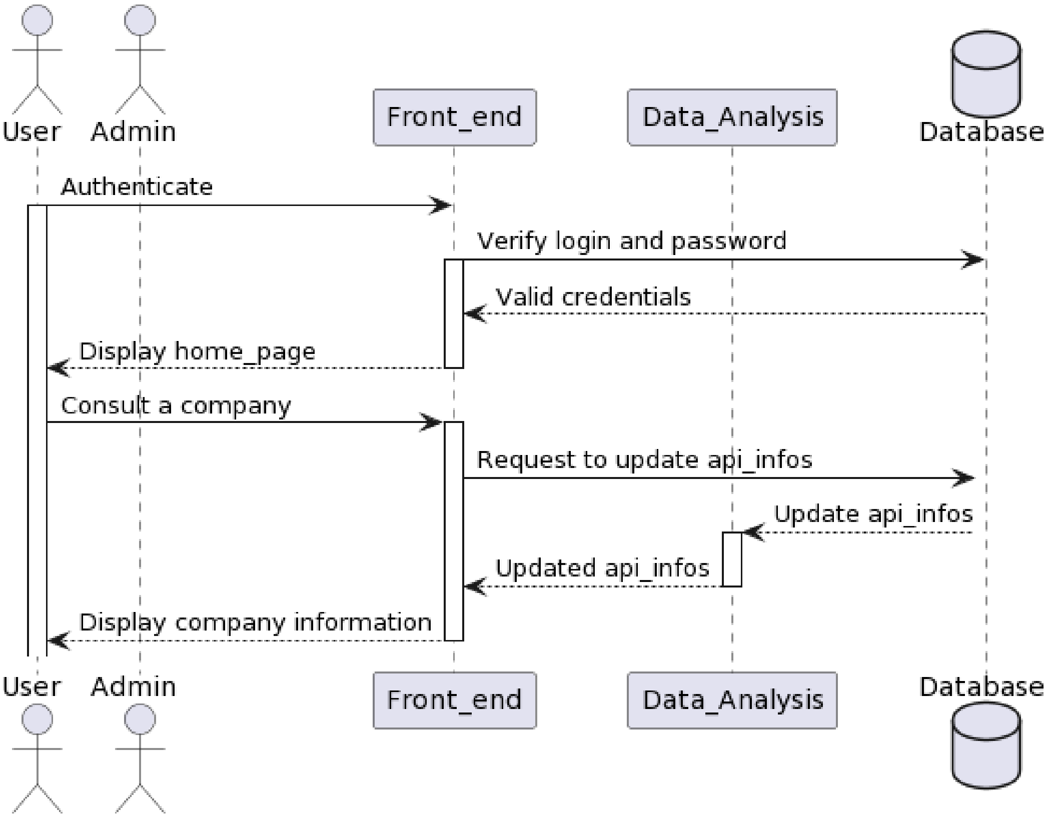


Figure 3.2: Sequence Diagram of visualizing information on the dashboard

Title: visualizing information on the dashboard.
Main Actor: Employee
Goal:visualize the retrieved and analyzed data on the dashboard.
Summary: the central action revolves around our employees who are empowered to access and harness critical data insights. To initiate this process, employees begin by authenticating themselves securely, ensuring that access is only granted to authorized personnel. Once authenticated, employees have the capability to submit requests for data retrieval from a variety of APIs, each serving as a valuable source of information. These requests trigger a seamless process where the data is meticulously gathered, filtered, and analyzed for relevance and accuracy.

Subsequently, the analyzed data is skillfully visualized, employing a dynamic dashboard interface that offers an intuitive and real-time view of key metrics and trends. This visualization process, driven by a sophisticated backend system, culminates in a user-friendly frontend interface where employees can readily interpret and act upon the insights gained. The synergy of authentication, data retrieval, analysis, and visualization provides our employees with a powerful toolset to make informed decisions and drive actionable outcomes
Preconditions: Authentication with valid employee credentials.

The following sequence diagram illustrates the steps involved in the user authentication process, depicting the interactions between the user, the user interface, the authentication system, and the database.

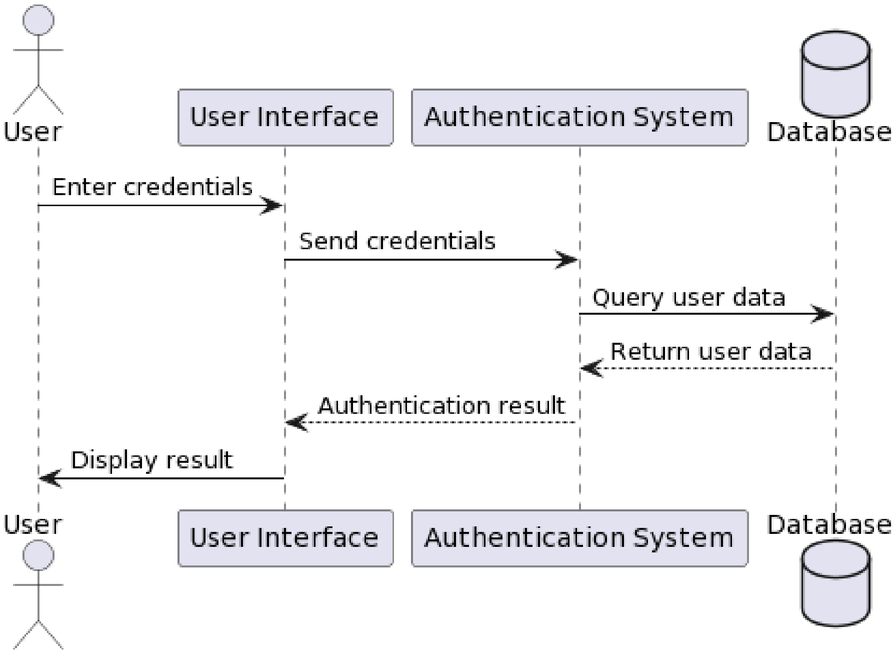


Figure 3.3: User Authentication Sequence Diagram

Title: User Authentication Sequence.
Main Actor: Employee
Goal: Securely authenticate users for system access.
Summary: The central action involves employees who need to securely authenticate themselves before gaining access to the system. Authentication is a critical step to ensure that access is granted only to authorized personnel. Employees provide their credentials, typically a username and password, to the system.
Preconditions: Authentication with valid employee credentials.

3.3 Framework Selection and Data Source

In the following section, I will delve into two pivotal aspects that underpin the foundation of my project: the choice of the web application framework and the array of data sources I have harnessed to enrich our platform. The careful selection of a suitable framework lays the groundwork for efficient development and scalability, while the integration of diverse APIs forms the lifeblood of our system, providing invaluable insights into the security posture of organizations. In this part of the report, I will unveil the rationale behind our adoption of Flask as the framework of choice and shed light on the key data sources will empower our application to offer comprehensive cybersecurity assessments.

3.3.1 Framework Selection

Empowering Our Vision with Flask When embarking on the journey to develop a sophisticated web application tailored to analyze organizations' IP addresses and domain names for potential security threats, the choice of a robust and adaptable framework was paramount. After careful consideration, I opted for Flask as the cornerstone of my project.

Flask: The Power of Simplicity Flask's minimalist yet highly extensible design philosophy resonated with me as the sole developer of this project. This micro-framework offered the flexibility I needed to accommodate the intricacies of data retrieval, analysis, and presentation seamlessly. Its simplicity, often characterized as its strength, allowed me to focus on crafting custom solutions tailored to the specific requirements of the project without unnecessary complexity.

Agility and Speed of Development One of the defining factors in selecting Flask was its rapid development cycle. Flask's lightweight nature, coupled with its modular structure, facilitated swift progress in the implementation of our project. This efficiency was critical in meeting our project timeline and delivering a feature-rich application to our users.

Scalability for Future Growth Flask's innate scalability was another key factor in its favor. As the user base expands and the volume of data to be analyzed increases, Flask's robust support for handling heightened demands ensures that the application can adapt and evolve seamlessly. This scalability was essential to my long-term vision for the platform, allowing it to accommodate growing data requirements and user traffic as the project continues to develop.

Figure 3.4: Flask logo

In summary, Flask emerged as the natural choice for this web application framework due to its agility, simplicity, and scalability. It empowers me to efficiently harness data from diverse sources, process it with precision, and present real-time insights to enhance organizations' cybersecurity postures. In the following sections, we will explore in depth the data sources that complement Flask's capabilities, providing the lifeblood of our security analysis platform.

3.3.2 Data Sources

In order to empower the web application with comprehensive cybersecurity insights, I harnessed a diverse range of data sources, including CriminalIP, AbuseIPDB, TotalVirus, and Censys. These APIs played a pivotal role in providing the application with crucial information concerning the security posture of IP addresses and domains. Through these sources, I obtained real-time intelligence that allowed me to determine whether an IP address or domain should be classified as harmful, malicious, suspicious, or blacklisted. This multifaceted approach to data acquisition enabled the platform to offer users a holistic view of potential security threats, facilitating informed decision-making and proactive risk mitigation.

CriminalIP: Unveiling Malicious Intent

One of my key data sources, CriminalIP, played a pivotal role in uncovering malicious intent behind certain IP addresses and domains. By querying this source, I was able to identify IP addresses and domains that have been associated with criminal activities, such as cyberattacks, malware distribution, and fraudulent schemes. The insights provided by CriminalIP enabled me to flag these entities as high-risk, ensuring that our users could proactively safeguard their systems against potential threats.

Figure 3.5: CriminalIP logo

AbuseIPDB: Unearthing Suspicions

AbuseIPDB served as an invaluable data source in my development toolkit. This API allowed me to identify IP addresses and domains that had been reported for abusive behavior, suspicious activities, or spamming. By leveraging the collective intelligence of AbuseIPDB's user community, I could quickly pinpoint potentially harmful entities and classify them accordingly. This proactive approach to threat detection helped bolster the security posture of our users by highlighting sources of suspicion that might otherwise go unnoticed.

Figure 3.6: AbuseIPDB logo

TotalVirus: Assessing Malware Risks TotalVirus played a critical role in my development efforts by assisting in the assessment of malware risks associated with IP addresses and domains. With this data source, I could scrutinize whether an IP or domain had been flagged as a host for malware distribution. TotalVirus's malware database provided me with up-to-date information on known threats, enabling me to issue timely alerts and mitigate potential malware-related risks effectively. This insight into malware associations was paramount in enhancing our users' cybersecurity defenses.

Figure 3.7: TotalVirus logo

Censys: Uncovering Internet-wide Trends Censys, my final data source, offered a broader perspective by allowing me to uncover internet-wide trends and vulnerabilities. This API provided me with comprehensive data on IP addresses and domains, including information on their certificates, open ports, and services. By analyzing this data, I could identify security weaknesses and trends that could potentially affect a wide range of organizations. Censys empowered our users with a more holistic view of their digital footprint, helping them proactively address vulnerabilities and enhance their overall cybersecurity posture.

Figure 3.8: Censys logo

Through the integration of these four diverse data sources into our platform, I ensured that our users had access to a comprehensive and multifaceted security analysis tool. This tool was capable of detecting threats, suspicious behavior, malware risks, and broader internet-wide trends. This approach empowered organizations to make well-informed decisions and implement proactive security measures, effectively safeguarding their digital assets.

3.4 Conclusion:

In this chapter, I've laid the groundwork for our project. UML diagrams provided clarity on the project's architecture. The Flask framework was chosen for its simplicity and adaptability, and data sources like CriminalIP, AbuseIPDB, TotalVirus, and Censys enriched our platform's threat intelligence. This foundation sets the stage for the implementation phase, enabling us to enhance cybersecurity and facilitate informed decision-making.

Chapter 4

Realization and Validation

4.1 Introduction

In this final chapter, I take the opportunity to provide a comprehensive overview of the work I've accomplished during the internship. It represents the culmination of my efforts and offers a detailed look at the tangible outcomes of this experience. To begin, I'll walk you through the software environments that have played a pivotal role in shaping my internship journey. Afterward, I'll delve into a meticulous presentation of the work I've achieved, showcasing the various interfaces, solutions, and innovations that I've personally crafted and refined throughout the course of this internship.

4.2 Realization Environment

4.2.1 Used Programming language

Python serves as the core programming language within our Flask-based web application, and it plays a pivotal role in analyzing information retrieved from various APIs. Flask, which is based on Python, provides the structural foundation and essential tools needed to seamlessly integrate this analysis into our platform. Leveraging the versatility and power of Python, I've crafted custom data processing logic that fits seamlessly within Flask's framework. This combination enables me to efficiently handle and analyze the diverse data obtained from sources like CriminalIP, AbuseIPDB, TotalVirus, and Censys. Python's rich ecosystem of libraries and its ease of use have been instrumental in my ability to extract actionable insights from these APIs, empowering our platform to deliver comprehensive cybersecurity assessments to our users.

Figure 4.1: Python Logo

4.2.2 Used Tools

As we delve deeper into the mechanics of the project, it's essential to acknowledge the pivotal role that a range of carefully selected tools played in its development. These tools, each offering unique capabilities and functionalities, were instrumental in ensuring the seamless progress and success of the project. They not only enhanced efficiency but also facilitated collaboration, making it possible to bring the vision to fruition. In the subsequent sections, we will explore each of these tools in detail, shedding light on their respective contributions to the project's development. **PyCharm:** PyCharm became my go-to development environment throughout the project's lifecycle. This robust integrated development environment (IDE) tailored for Python offered a plethora of features that significantly streamlined my development process. PyCharm's intelligent code editor, real-time code analysis, and seamless integration with Flask allowed for efficient coding, debugging, and testing. Its built-in version control system with Git simplified collaboration and ensured that our codebase remained organized and manageable. The user-friendly interface and the array of built-in tools enhanced my productivity, allowing me to focus on crafting the core functionality of our application. PyCharm played a pivotal role in ensuring that my development was efficient, error-free, and aligned with best practices, ultimately contributing to the project's success.

Figure 4.2: PyCharm Logo

PlantText: PlantText, a tool I relied on extensively, played a pivotal role in visualizing our project's architecture. Its remarkable ability to transform UML code into comprehensive diagrams was a game-changer in our documentation and design process. By providing the UML code representation of our system, PlantText effortlessly translated it into clear and visually informative diagrams. This streamlined our communication and collaboration efforts, making it easy to convey intricate architectural details and system structures. PlantText became an invaluable asset, enhancing our project's documentation and ensuring that both my development efforts and our stakeholders shared a unified understanding of our system's design.

Figure 4.3: PlaintText Logo

XAMPP: XAMPP played a pivotal role in shaping the infrastructure of this project. It provided a comprehensive development environment that was indispensable in the creation of my web application. With XAMPP, I had the convenience of running a local server that seamlessly integrated Apache, MySQL, PHP, and PhpMyAdmin. This powerful stack allowed me to develop and test the web application effectively on my local machine, mirroring the production environment closely. The user-friendly interface of PhpMyAdmin simplified database management, enabling me to configure and interact with the database efficiently, ensuring data integrity and reliability. XAMPP's flexibility and cross-platform compatibility made it a trusted and indispensable tool throughout the development and testing phases of our project, providing a solid foundation upon which I could confidently build and refine our web application.

Figure 4.4: XAMPP Logo

MySQL: MySQL played a pivotal role in the data management strategy, serving as the core database system that seamlessly integrated with our web application code. This relational database management system (RDBMS) allowed me to efficiently store, organize, and retrieve data, ensuring the reliability and scalability of our application. The compatibility of MySQL with the Python programming language, which we used extensively in our web application, facilitated smooth interactions between the database and our code. Through Python scripts, I could effortlessly establish connections, execute queries, and process database results, enabling our application to dynamically fetch and present data to users. MySQL's robust features, including support for complex queries and transactions, gave me the tools needed to create a robust and responsive application that met our project's data management requirements with precision.

Figure 4.5: MySQL Logo

4.3 The Global Architecture

The global architecture of this project, as I've meticulously designed it, is geared towards ensuring a seamless flow of data and requests. It all initiates at the front-endthis, where user actions trigger requests. These requests are then dispatched to the back-end, which serves as the essential intermediary responsible for processing and managing them. Within the back-end, these requests often find their way to our MySQL database, where data is securely stored and swiftly retrieved. The database carries out the necessary operations to fetch the pertinent information, which is subsequently relayed back to the back-end for further processing. Finally, the back-end returns the response to the front-end, where the requested data seamlessly populates the user interface. This architecture reflects a deliberate approach to ensure user-friendly interactions, data integrity, and the overall efficiency of our application, all in line with our project's objectives.

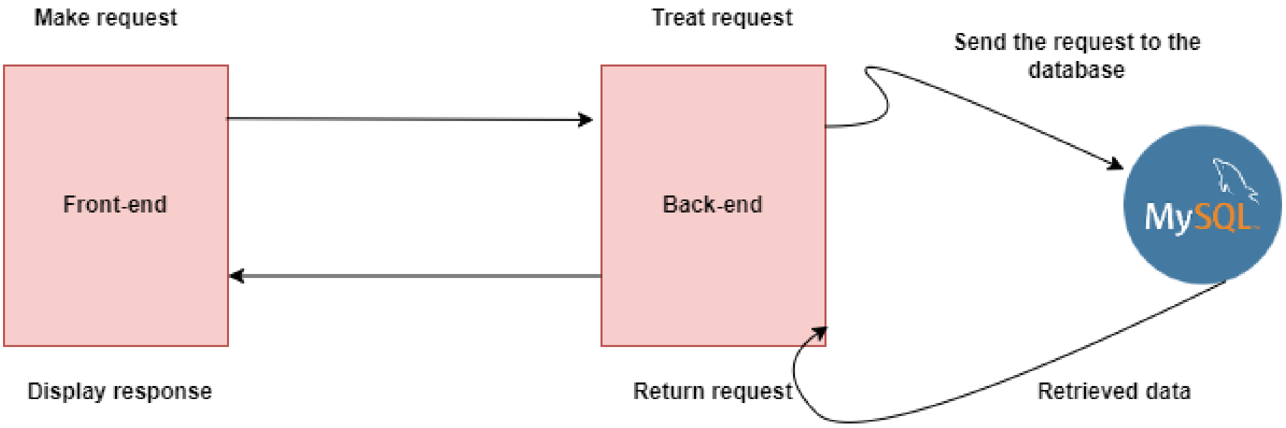


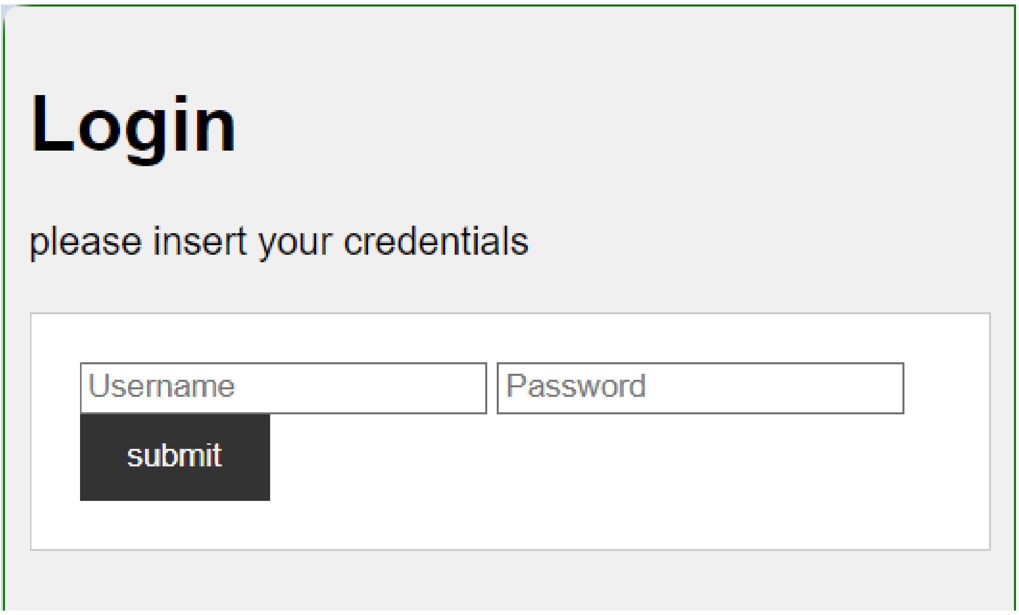
Figure 4.6: The Global Architecture

4.4 The Implementation Of The Solution

In this last section of our project report, I'm excited to present the culmination of our efforts during the internship. Let's dive into the heart of the web application, where I'll provide an in-depth exploration of the various interfaces, each carefully tailored to accommodate the unique roles of our users. We'll take a closer look at the user dashboard, the employee interface, and the administrator's workspace, dissecting the specific functionalities designed to meet the distinct needs and responsibilities of each user group. This deep dive into the implementation of our solution underscores how this project effectively caters to the diverse requirements of the stakeholders and end-users, truly bringing my vision to life.

4.4.1 User Implementation

In the user-focused implementation, I've placed a strong emphasis on creating a customized and secure experience right from the login page. Here, users are required to authenticate themselves, a fundamental step to ensure not only data security but also proper access control. Authentication not only verifies the user's identity but also plays a pivotal role in determining their role within the system. The login page acts as the primary entry point, effectively distinguishing between employees and administrators. This user-centric design enables us to provide the right level of access and privileges based on each user's role, delivering a tailored experience while upholding the highest standards of data integrity and security.



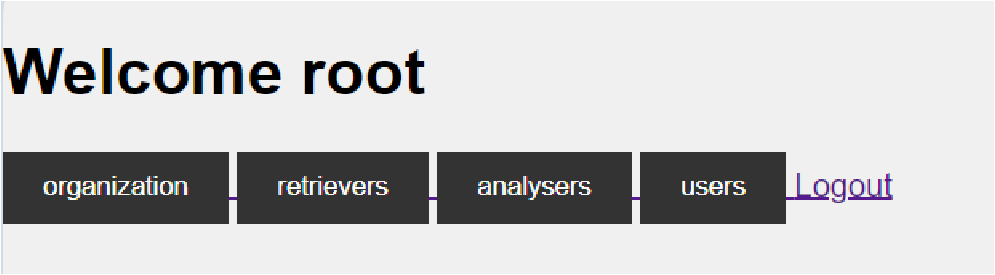
Login

please insert your credentials

Figure 4.7: User Authentication

Admin

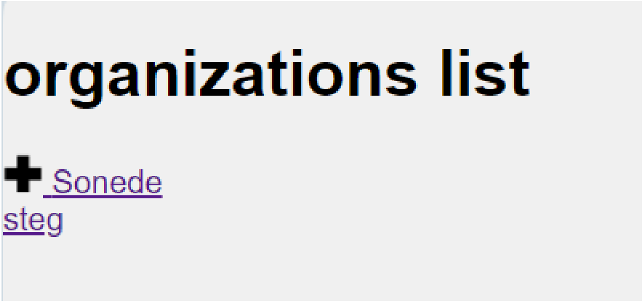
The administrator's interface is the linchpin of our access control and management system. When the administrator, logs in, the backend swiftly engages in a dialogue with the database to ascertain the role and associated privileges. This vital step guarantees that only authorized administrators gain access to the administrative panel.



Welcome root

Figure 4.8: Admin Interface

Organizations List Within the admin dashboard, I've incorporated a powerful feature that allows administrators to manage organizations seamlessly. When the admin selects the 'Organizations' option, they are presented with a comprehensive list of companies affiliated with our system. From here, administrators can dive into the details of each company.

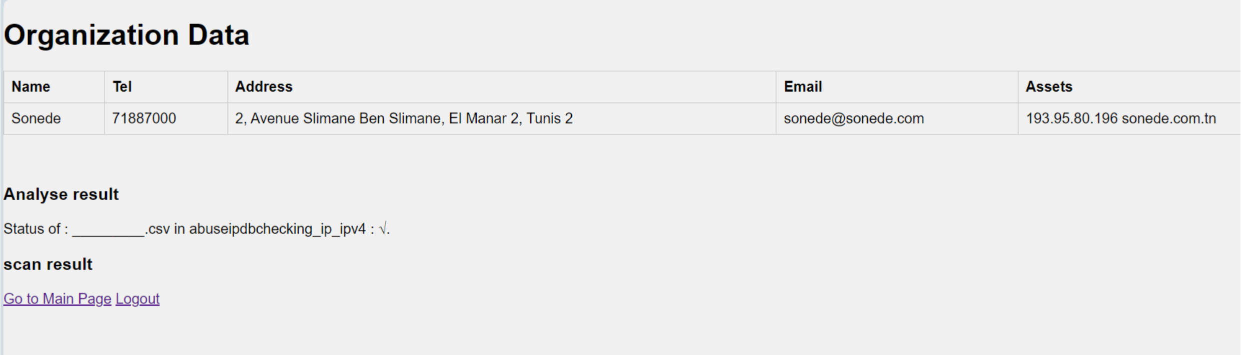


organizations list

✚ Sonede
steg

Figure 4.9: Organizations List

When an admin selects a specific company, such as 'Sonede' from the list, they are granted access to a dedicated page that offers a comprehensive view of the company's details.



Organization Data

Name	Tel	Address	Email	Assets
Sonede	71887000	2, Avenue Slimane Ben Slimane, El Manar 2, Tunis 2	sonede@sonede.com	193.95.80.196 sonede.com.tn

Analyse result

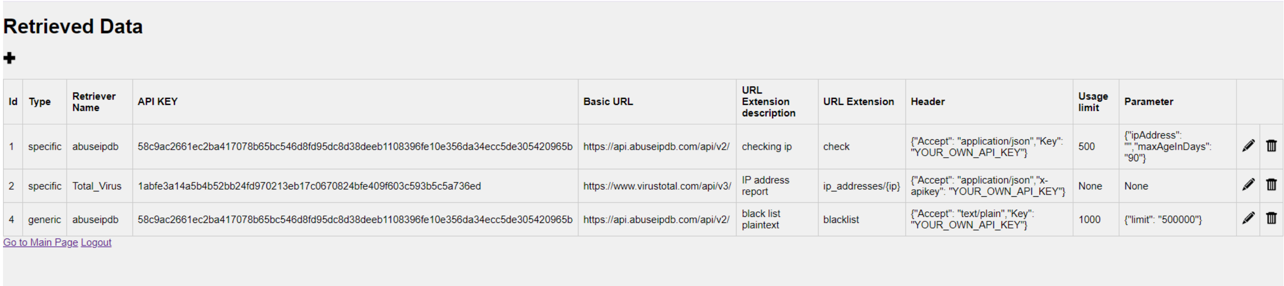
Status of : _________.csv in abuseipdbchecking_ip_ipv4 : √.

scan result

Go to Main Page Logout

Figure 4.10: An organization's Assets

Within the admin dashboard, a powerful feature provides access to a comprehensive list of retrievers, each serving as a crucial data source for our system. These retrievers come in two primary types: 'Generic' retrievers, which offer information about a wide range of subjects and may contain multiple IP addresses, and 'Specific' retrievers, tailored to provide information specific to individual IP addresses. The list includes detailed information for each retriever, such as its name, API key, URL, header, usage limits, and any associated parameters. To streamline administration, we've incorporated intuitive icons that allow administrators to perform actions with ease. With a simple click, administrators can update, delete, or add new retrievers as needed, granting them the flexibility and control required to manage and expand the range of data sources efficiently.



Retrieved Data

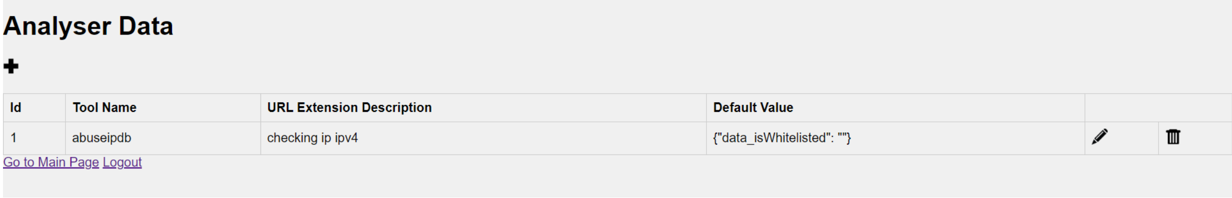
✚

Id	Type	Retriever Name	API KEY	Basic URL	URL Extension description	URL Extension	Header	Usage limit	Parameter		
1	specific	abuseipdb	58c9ac2661ec2ba417078b65bc546d8fd95dc8d38deeb1108396fe10e356da34ecc5de305420965b	https://api.abuseipdb.com/api/v2/	checking ip	check	{"Accept": "application/json","Key": "YOUR_OWN_API_KEY"}	500	{"ipAddress": "","maxAgeInDays": "90"}	✎	🗑
2	specific	Total_Virus	1abfe3a14a5b4b52bb24fd970213eb17c0670824bfe409f603c593b5c5a736ed	https://www.virustotal.com/api/v3/	IP address report	ip_addresses/{ip}	{"Accept": "application/json","x-apikey": "YOUR_OWN_API_KEY"}	None	None	✎	🗑
4	generic	abuseipdb	58c9ac2661ec2ba417078b65bc546d8fd95dc8d38deeb1108396fe10e356da34ecc5de305420965b	https://api.abuseipdb.com/api/v2/	black list plaintext	blacklist	{"Accept": "text/plain","Key": "YOUR_OWN_API_KEY"}	1000	{"limit": "500000"}	✎	🗑

Go to Main Page Logout

Figure 4.11: Retrievers List

The admin dashboard also provides a dedicated section for managing analyzers, a pivotal component of our system. Each analyzer is characterized by its 'Tool Name' specifying the analytical tool used, and its Essential Part which defines the specific aspect of information to be checked and analyzed. Additionally, administrators can set Default Values for analyzers to ensure that they function in alignment with the system's requirements. To streamline administration and ensure flexibility, we've incorporated user-friendly icons that allow administrators to take swift actions. These icons enable admins to effortlessly update, delete, or add new analyzers, providing them with the tools needed to configure and expand the analytical capabilities of the system as per evolving needs and objectives.



Analyser Data

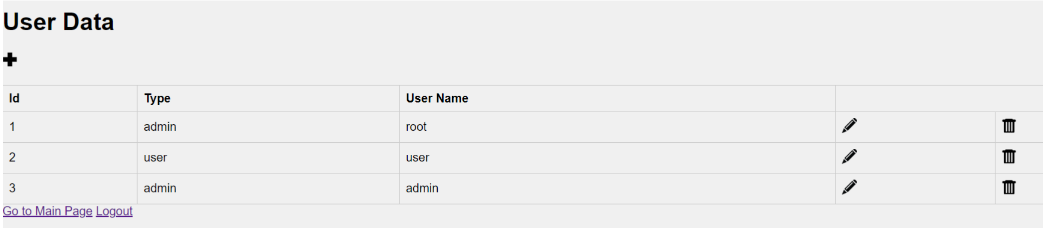
✚

Id	Tool Name	URL Extension Description	Default Value		
1	abuseipdb	checking ip ipv4	{"data_isWhitelisted": ""}	✎	🗑

Go to Main Page Logout

Figure 4.12: Analysers list

Additionally, the admin dashboard empowers administrators to oversee the system's user management. Within this section, administrators can access a comprehensive list of users, each accompanied by their names, user types, and password information. The user list provides a snapshot of the system's user base. Admins can conveniently add new users, update existing user profiles, or remove user accounts as necessary. This comprehensive user management feature ensures that administrators have full control over the system's user base, streamlining the management of user accounts in alignment with the system's evolving requirements and security standards.



User Data

✚

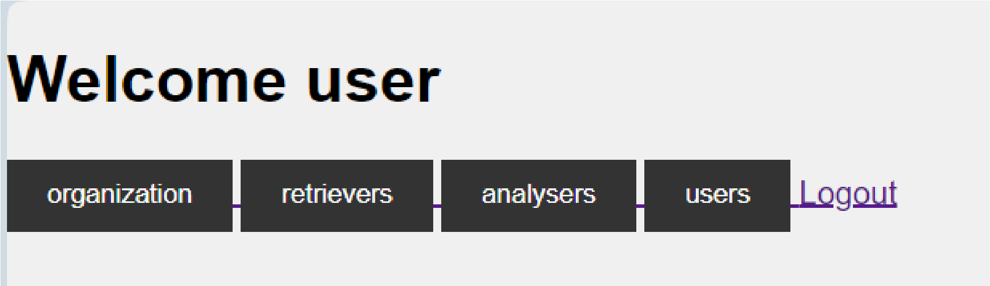
Id	Type	User Name		
1	admin	root	✎	🗑
2	user	user	✎	🗑
3	admin	admin	✎	🗑

Go to Main Page Logout

Figure 4.13: Users list

Employer

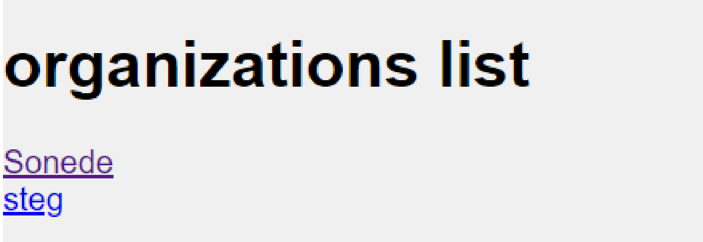
For our everyday users, particularly employees, I've meticulously designed an interface similar to the authenticating, employees step into a welcoming dashboard tailored to their specific requirements.



Welcome user

Figure 4.14: User Interface

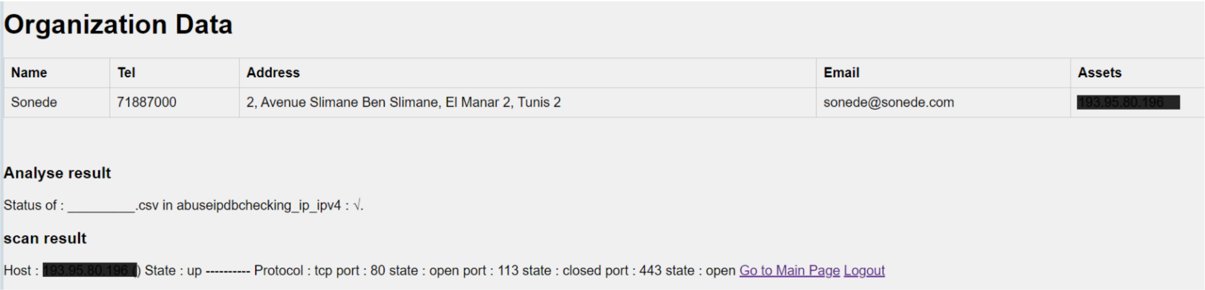
So users, such as employees, have access to view the list of organizations, retrievers, and analyzers, it's important to note that their permissions are limited in this regard. Users can view these components to gain insights and access relevant information. However, they do not have the authority to modify, delete, or add new entities. This restricted access ensures that users can review and utilize the available data sources and analytical tools but do not have the capability to make structural changes to the system. The attached images provide a visual representation of these components, offering users valuable insights without exposing them to administrative functions.



organizations list

Sonede
steg

Figure 4.15: Organizations



Organization Data

Name	Tel	Address	Email	Assets
Sonede	71887000	2, Avenue Slimane Ben Slimane, El Manar 2, Tunis 2	sonede@sonede.com	[redacted]

Analyse result

Status of : __________.csv in abuseipdbchecking_ip_ipv4 : √.

scan result

Host : [redacted]) State : up ---------- Protocol : tcp port : 80 state : open port : 113 state : closed port : 443 state : open Go to Main Page Logout

Figure 4.16: Sonede Assets

The output of the scan plays a vital role in enhancing our security posture by providing valuable insights into the status of open ports on various hosts. It equips us with critical information that allows for the safeguarding of these open ports and the mitigation of potential vulnerabilities. For example, a host with IP address of the sonede organization reveals its state as 'up' along with details about multiple ports. Among these, port 80 is reported as 'open' indicating that it is accessible and potentially vulnerable. On the other hand, port 113 is marked as 'closed' which suggests a different level of security. Port 443 is also listed as 'open' raising awareness about its status. This information enables us to take proactive measures to protect open ports, thus fortifying our overall security strategy

4.5 Conclusion:

In this chapter, I've delved into the implementation of the solution, providing a detailed overview of the user interfaces, administrative capabilities, and data management tools. I've explored how the admin interface empowers administrators to efficiently manage organizations, retrievers, analyzers, and users, while users, in turn, can access vital information for their tasks. These interfaces and features represent the culmination of our project's development, and they are designed to streamline data access and analysis, all while maintaining robust control and security. As we transition into the next phase, the focus shifts to the validation of our solution and its performance in real-world scenarios, where we aim to ensure that our system meets the expectations and requirements of our stakeholders.

Conclusion

As I conclude this project journey, I reflect on the significant strides made in enhancing cybersecurity and data analysis. Throughout the project's lifecycle, I've meticulously designed, developed, and implemented a robust web application that empowers users, administrators, and organizations to access, analyze, and manage critical data sources. this project's foundation, rooted in meticulous UML diagrams, ensured a clear vision of system architecture, fostering precision and alignment with objectives.

The selection of the Flask framework, coupled with diverse data sources, offered a wealth of capabilities to create a multifaceted security analysis tool. Flask's minimalist and extensible design philosophy aligned with our needs, providing flexibility to customize solutions without unnecessary complexity. Our collaboration with data sources such as CriminalIP, AbuseIPDB, TotalVirus, and Censys enriched our application with insights on harmfulness, maliciousness, and broader internet trends.

The global architecture, optimized for user experience, securely facilitated data flow from the front-end to the back-end and database. Access control mechanisms, custom-tailored interfaces, and flexible data management tools ensure that our system aligns with user roles and organizational needs.

As I move forward, our focus transitions to the validation phase, where I will rigorously test the system's performance in real-world scenarios to ensure it meets the expectations and requirements of our stakeholders. I remain committed to the ongoing refinement of the project to deliver a valuable solution that enhances cybersecurity, data analysis, and decision-making capabilities. The journey doesn't end here, as I continue to evolve and adapt to the dynamic landscape of cybersecurity and data intelligence, serving the mission to safeguard digital assets and provide actionable insights for our users."