[1. Technical Progress 2](#_Toc176893791)

[1.1 AI to Identify Cybersecurity Vulnerabilities 2](#_Toc176893792)

[1.2 Website Design and Development 3](#_Toc176893793)

[1.5 Significant Changes 6](#_Toc176893794)

[1.6 Flow Chart 7](#_Toc176893795)

[2. Completed Task 7](#_Toc176893796)

[2.1 Problems from Business and Technical Perspective 7](#_Toc176893797)

[2.2 Specification of Requirements 8](#_Toc176893798)

[2.3 Selection of Network and Security Technologies 8](#_Toc176893799)

[2.4 Design of Network/Security architecture 9](#_Toc176893800)

[2.5 Network and security policies 10](#_Toc176893801)

[2.6 Industry Analysis for GenAI 11](#_Toc176893802)

[2.7 Stakeholders’ identification 12](#_Toc176893803)

[3. List of Issues and Challenges and Mitigation 13](#_Toc176893804)

[4. Priority Tasks Up Until the End of Project 14](#_Toc176893805)

[5. Project Plan 16](#_Toc176893806)

[6. Contribution Table 18](#_Toc176893807)

[7. Weekly Report 18](#_Toc176893808)

[7.1 Week 1 18](#_Toc176893809)

[7.2 Week 2 19](#_Toc176893810)

[7.3 Week 3 19](#_Toc176893811)

[7.4 Week 4 20](#_Toc176893812)

[7.5 Week 5 20](#_Toc176893813)

[7.6 Week 6 21](#_Toc176893814)

[7.7 Week 7 22](#_Toc176893815)

[7.8 Week 8 22](#_Toc176893816)

# 1. Technical Progress

## 1.1 AI to Identify Cybersecurity Vulnerabilities

We have completed the basic task of developing AI which is able to detect cybersecurity vulnerabilities, and we have checked using url of the website and got positive result. The AI is basically generated in VS code using programming language python, where we have used the basic models available on python library and used AI ML model such as isolation forest and tensor flow for anomaly detection and we have also used pre trained AI model Microsoft/codebert-base for making our task easy. Basically, the generated AI isa able to detect vulnerabilities on the different areas of the websites through SQL injection, Cross site scripting, brute-force attack and we have tried Cross-site Request Forgery (CSRF) and Server-site Request Forgery (SSRF). The result has been shown below.

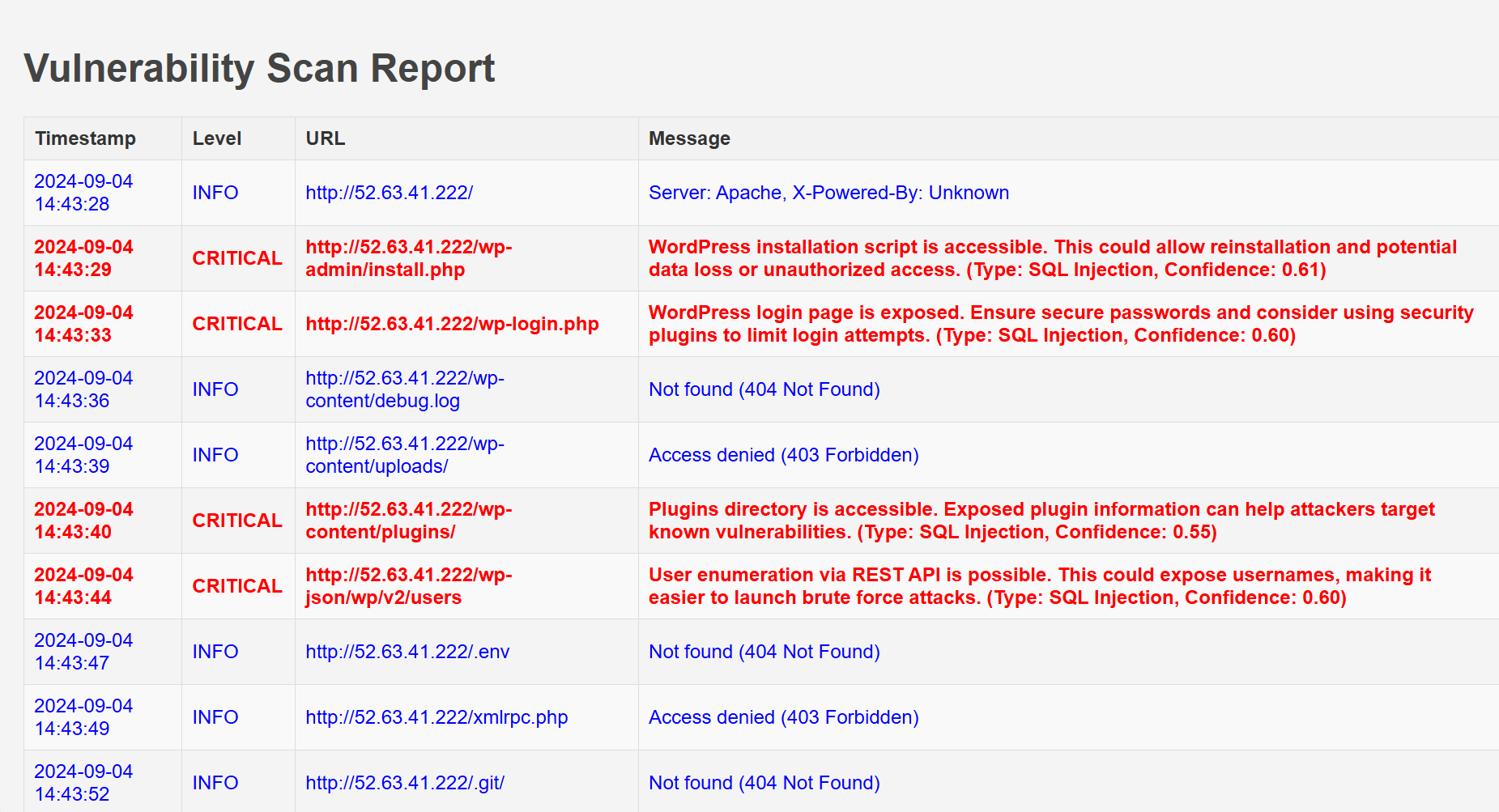


Fig 1: Vulnerability Scan Report

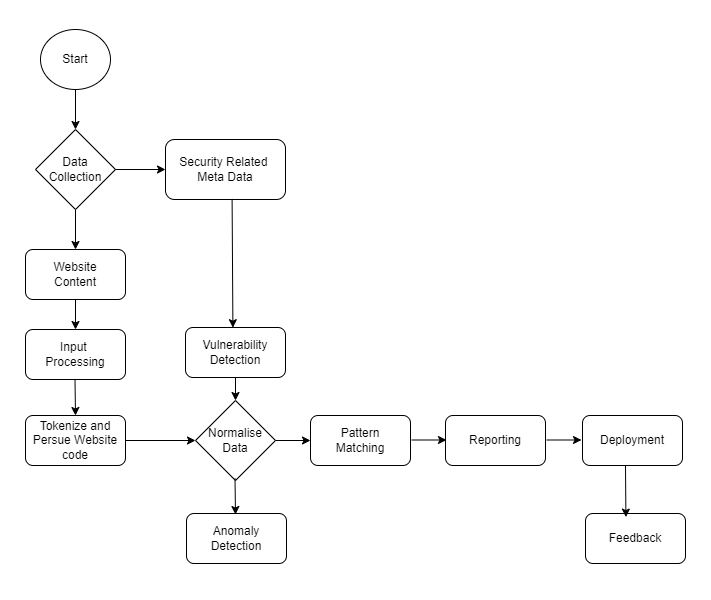


Fig 2: Flowchart for GenAI Tool

## 1.2 Website Design and Development

Regarding the technical progress of the project till now, we have developed and designed a website for the WaterTunnel Car Wash company. For developing websites, we deployed WordPress certified by Bitnami by using AWS web server involving several steps. The main reasons for choosing AWS cloud service for deploying WordPress are security and cost-effectiveness. When we completed the process of launching instances in EC2 we received a public IPv4 address and login username and password for the WordPress website.

A screenshot of a computer

Description automatically generated

Fig 3: Launching WordPress in AWS.

When creating websites then we collected different resources from online sources and some of them are designed by yourself. The website contains everything that needs to be a perfect website. The website is all about company’s information and car wash features. The website includes service details, Wash Menu, contact details etc. Here are some glimpses on our websites.

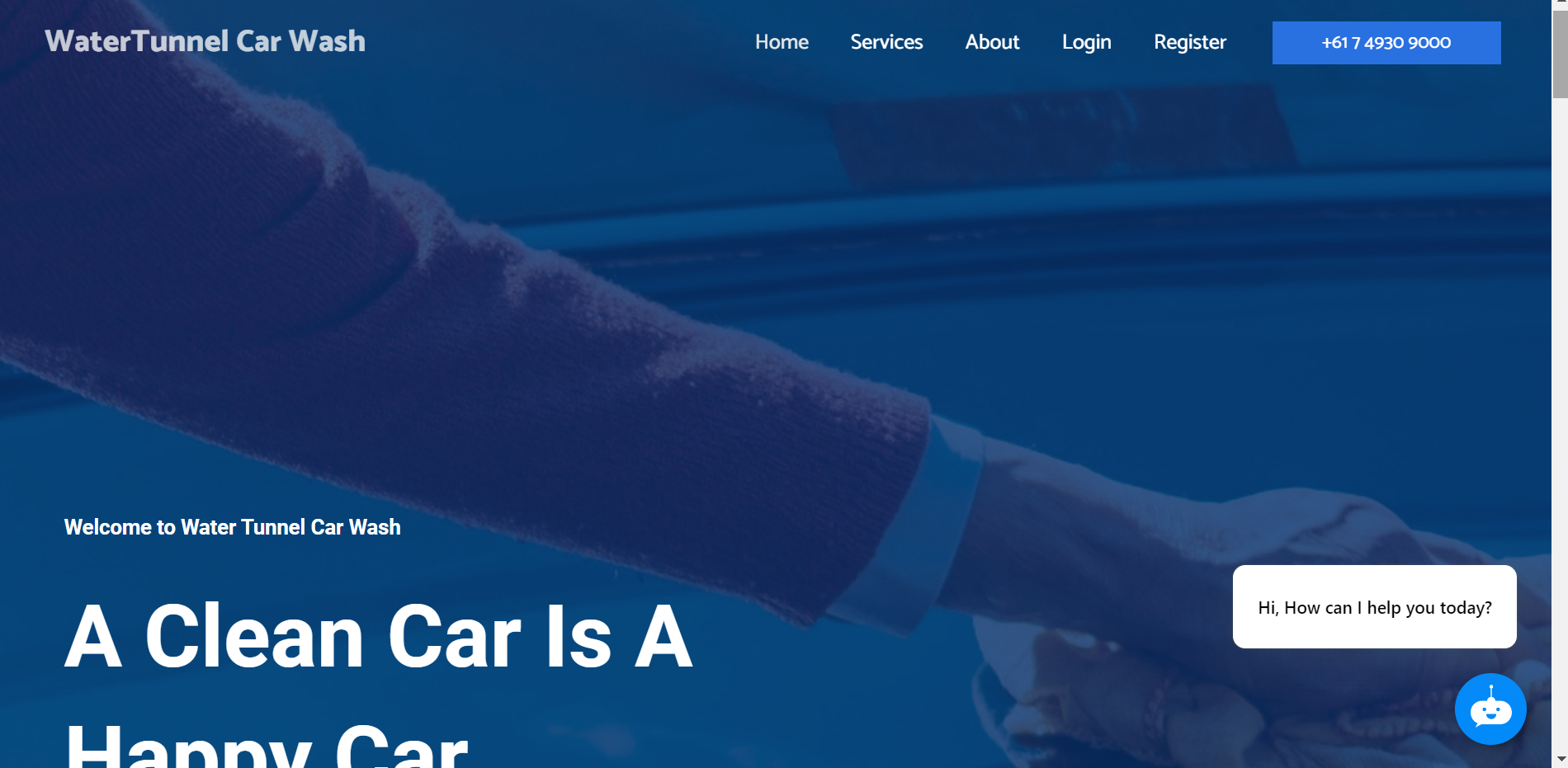


Fig 4: Company Website

A hand on a red towel

Description automatically generated

Fig 5: Company Website

A diagram of swot analysis

Description automatically generated

Fig 8: SWOT analysis for chatbot

A diagram of ethical framework

Description automatically generated

Fig 9: Ethical AI Framework for CS Chatbots in Automotive Industry

## 1.5 Significant Changes

We have significantly modified our original idea multiple times during our project. When we first deployed our chatbot, we didn't specify the industry. Since then, we've decided to concentrate on the automotive sector, aiming our chatbot system installation at the WaterTunnel car wash company. We expanded the scope of our project to include the development of a website for the WaterTunnel car wash firm. This website was effectively created, and we even managed to include our chatbot into it. Although deploying our project on Azure was our first intention, we ran into some problems and ended up deploying our system on AWS. Finding security holes on the website we developed became our project's main goal.But when we saw how difficult it would be to achieve this goal directly, we made the decision to create a GenAI system for vulnerability identification. This system has been developed successfully, and we have created a thorough vulnerability report that is attached to our documentation. We have been able to accomplish the project's main goals while addressing real-world issues thanks to these changes.

## 1.6 Flow Chart

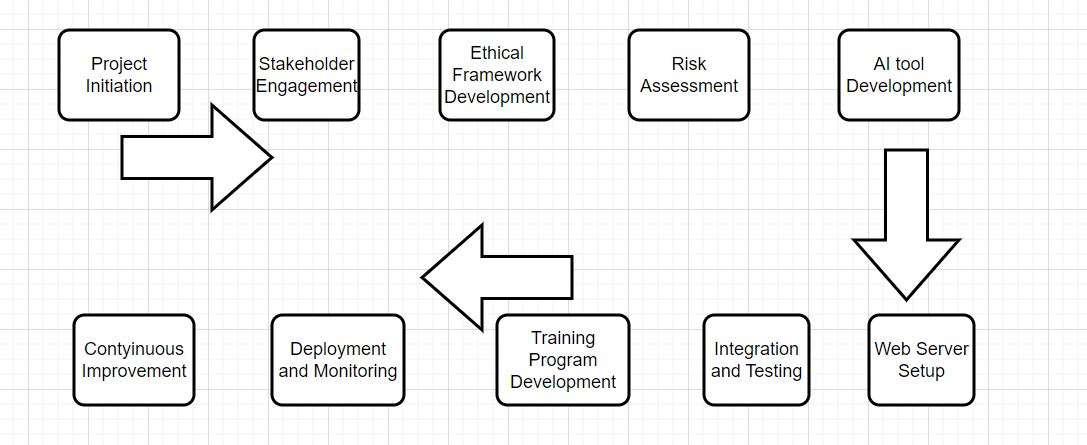


Fig 11: Flowchart of whole process of the project

# 2. Completed Task

## 2.1 Problems from Business and Technical Perspective

This is the end of eight week, we are almost at the end of our project report, we mentioned that we have completed almost every part of the technical progress, and we are looking for slight changes into it. Apart from that, for the report writing we have covered almost every part that needs to be included in our final project report. Till the date of today we have gone through problem form business and technical prospective. The problems from business perspective includes:

1. Intellectual Property Concerns
2. Economic Disruption
3. Managing Expectations

Similarly, problems from technical perspective includes:

1. Security Threats and Vulnerabilities
2. Ethical Implementation
3. Data Quality and Bias
4. Technical Expertise and Collaboration
5. Social engineering attacks
6. Phishing attack

To address these problems, we recommend using AI like ChatGPT and Gemini, we can use AI to detect the vulnerability and other cybersecurity vulnerabilities:

1. Password protection
2. Vulnerability scanning and filtering
3. Threats hunting queries
4. Amazon location service
5. AWS CloudFront

## 2.2 Specification of Requirements

As we know the short-term limitations of GenAI and its long-term benefits. This project report is all about using AI to identify vulnerabilities in cybersecurity; to fulfil these requirements the AI should cover the following specific requirements:

1. Functional requirements: The Gen AI such as ChatGPT, Gemini and other AI tool should be able to understand the customers queries and respond accordingly, should be able to respond and analysis unauthorized activities within the system.
2. Usability: The GenAI should be intuitive and user friendly, accessible through various devices and supporting natural languages and offers various options such as test, voices and visual interactions with clear and concise responses.
3. Reliability requirements: The GenAI should be able to operate unbiased, result should not be varied based upon users, time, devices and other factors, the result must be reliable and universal acceptance.
4. Performance Requirements: The GenAI should always be available to answers the questions as quick as possible ideally within 2 sec of questions being asked. The system should optimize for low latency and source utilizations ensuring smooth performance during peak hours.
5. Security performance: The security of the system and information stored inside the system in key factors. Any form of data must be prohibited in GenAI and communication should be encrypted and secure authentication method should be used in compliance with data protection laws.

## 2.3 Selection of Network and Security Technologies

The selection of appropriate network and security technologies is important while implementing GenAI into cybersecurity vulnerability detection and website hosting. In this section we have described about the identification, selection and justifications of network and security technologies while addressing cybersecurity concerns using GenAI should focuses on following aspects:

1. Secure AI platform: select AI platform of secure and robust cloud-based infrastructure such as AWS web server or Microsoft Azure should be implemented specially for developing and deploying GenAI.
2. TLS (Transport Layer Security) for GenAI: “Transport layer security plays an important role to ensure secure communication because of end-to-end encryptions” (Granjal, 2013).
3. OAuth 2.0 and OpenID Connect: “OAuth 2.0 and OpenID Connect can be used to manage authentication and access control” (Thorgersen and Silva, 2021).
4. Web Application Firewall (WAF): “Web application firewall can help protect GenAI applications from common web attacks such as SQL injection, cross-site scripting etc” (Gupta et al., 2023).

A diagram of a cloud computing process

Description automatically generated

Fig 19: Network Design

## 2.4 Design of Network/Security architecture

When deploying website into a AWS web server it is essential to ensure the security of website where multiple number of users/customers visit website and login/registers with their personal information. So, it is important to protect such information for being attacked. To short out such problems we have proposed the design of network/security architecture, which has shown below:

A diagram of a computer network

Description automatically generated

Fig 20: Design of network/security architecture

The entire system will be hosted on AWS infrastructure, which provides reliability and scalability for the deployment of website and other services. VPC will be applicable to logically isolate the network resources within the AWS cloud server. Internet gateway is attached to the VPC to allow inbound and outbound traffic of user’s interactions with the website. Load balancers id used to distribute incoming traffic across multiple AWS web servers and private key and public is used for secure connection, encryptions and verification.

We have also discussed about the security architecture/protocols/algorithms, where we have explained 1. Trasport Layer Security (TLS) 2. Distributed Denial of Service (DDoS) Protection and 3. AWS Web Application Firewall (WAF).

## 2.5 Network and security policies

In our project report we have described about the network and security policies such as password policies, disaster recovery plan and business continuity plan. The password policies include:

1. Increase password length and complexity
2. Enforce password uniqueness
3. Implement multi-factor authentication
4. Secure password storage and transmission
5. Implement account lockout policies
6. Regular password audits

Disaster recovery plan includes:

Disaster scenarios:

* Cyber-Attacks: All possible cyber-Attacks including Ransomware, data breaches, DDoS and so on.
* Hardware Failures: Server crashes, network failures
* Human Errors: Accidental deletion, misconfigurations
* Software Failures: Bugs, performance issues

Recovery plan:

* Incident Detection and Notification
* Assessment and Strategy:
* Execution of Recovery Procedure
* Post recovery
* Communication etc.

In business continuity plan we have discussed about:

* Data recovery as a service
* Zero trust data security
* Operational continuity
* IT infrastructure resilience

## 2.6 Industry Analysis for GenAI

Before choosing Automotive industry, we have gone through different industry where we can see the significant impact of GenAI regarding cybersecurity related issues. We have described the impact of cybersecurity in healthcare industry, banking industry, and organizations or company and telecommunication industry. in this project we are focused only on Automotive industry for describing the impact of GenAI in cybersecurity. For the cybersecurity related issues and solutions using AI tool in Automotive industry we have explained 1. Data privacy and security concerns 2. Network security and vulnerability 3. Secure AI integration and 4. Regulatory compliance and ethical considerations.

Inside the Automotive industry we have designed and developed website of a particular company (WaterTunnel Car Wash) as shown in above. Where we have identified the stakeholders inside this company to explain in more details about roles and responsibilities of IT experts inside this company for the integration of AI into the company’s website.

## 2.7 Stakeholders’ identification

The key stakeholders within the Automotive industry (WaterTunnel Car Wash) who have been impacted by AI and chatbots implementations are staff who work within the company, manager, shareholders and customers. Here we have explained briefly about what impact may have on the stakeholders and how they overcome this. We have provided the detailed report on stakeholders’ engagement report and prepared the stakeholders engagement matrices. The key characteristics of stakeholders are interest, influence and impact. We have described two key stakeholders into our project report.

1. Internal Stakeholders: These are individuals or groups within the organization, such as employees, managers, and shareholders.
2. External Stakeholders: These are individuals or groups outside the organization, such as customers, suppliers, regulators, and the community.

A diagram of a company's management

Description automatically generated with medium confidence

Fig 21: Stakeholder Engagement Matrix

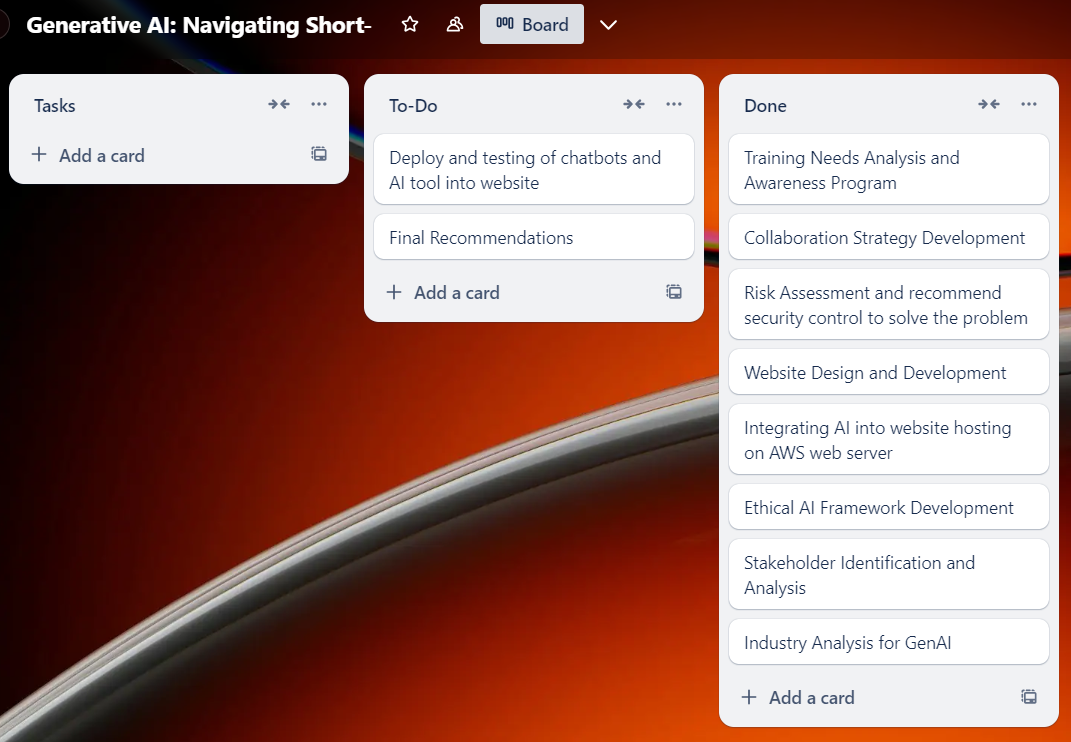
The above stakeholder engagement matrix shows that IT staff have high influence but low interest so they should keep satisfied. Managers have high influence and high interest regarding the implementations of chatbots so they should manage closely. Customers have high interest but low influence so they should keep informed. At last, a few other customers have low influence and low interest so they should monitor.

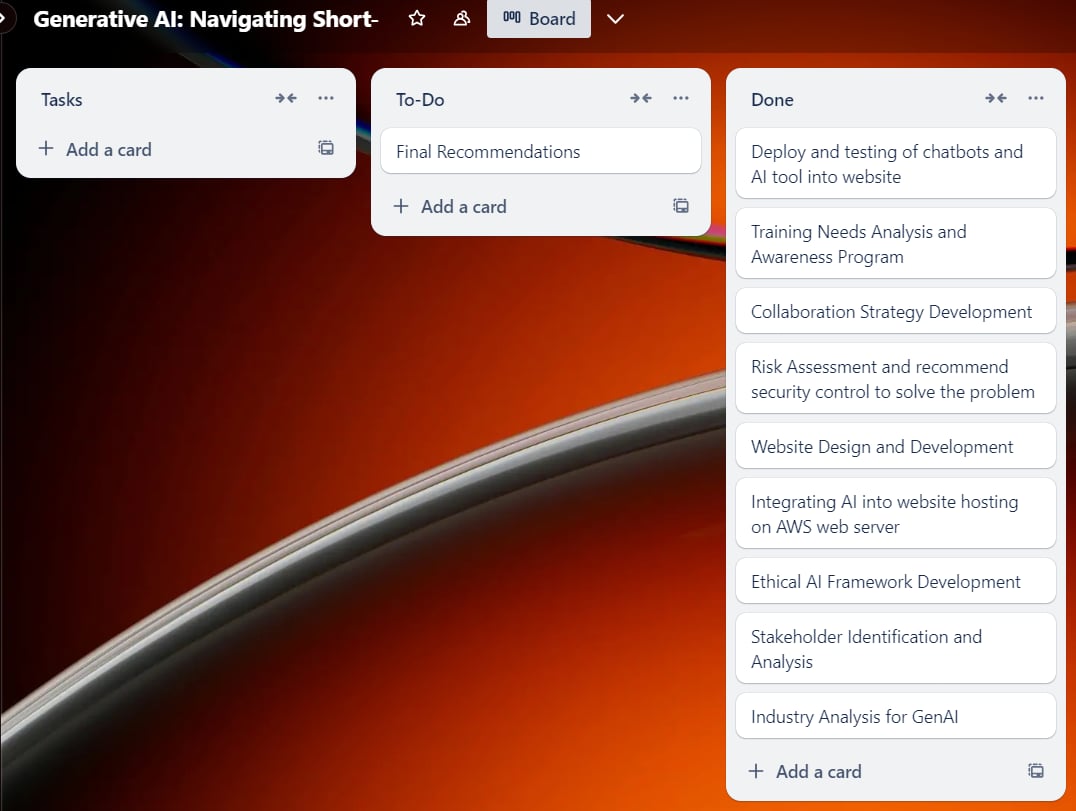
# List of Issues and Challenges and Mitigation

|  |  |
| --- | --- |
| **Issues and Challenges** | **Mitigation** |
| Finding official WordPress. | We went through most of AMI in AWS most of them were paid, we chose WordPress certified by Bitnami because of its cost-effectiveness. |
| Selecting security group configuration while launching. | We were confused about whether to select SSH, HTTP or HTTPS. Later, we did google research and found out to select all three. |
| Finding WordPress admin password. | We waited up to 1 hr after completing launch in EC2 to receive username and password. |
| Unexpected cost. | The cost for launching WordPress will be deducted per hour rate so we must visit AWS web server regular. |
| Installing MS Project software was challenging because it is a paid tool | We searched online and watched YouTube videos to find a solution. Eventually, we managed to install a free version of MS Project software. |
| While creating the Gantt chart, errors indicated by red lines appeared on the start and end dates of some tasks | We resolved this issue by adjusting the predecessors and re-entering the data, which corrected the errors and allowed us to generate the Gantt chart successfully. |
| It was difficult to select an appropriate industry and identify the relevant stakeholders. | We chose the automotive industry, specifically a water tunnel car wash. With the help of the manager, we gathered information about the stakeholders. |
| Scanning urls or multiple tests cases network latency can cause timeouts. | Use reasonable timeout values for ‘requests.get’ and ‘requests.post’ that we have used. |
| Automated vulnerability scanners can produce false positives. | Refined payloads for SQL injection and XSS have been used. |
| Using an anomaly detection model can yield false positives. | Training data for the anomaly detection model is representative of both normal and abnormal responses. |
| Training data for the anomaly detection model is representative of both normal and abnormal responses. | Our program includes memory-efficient data structures. |
| Pre-trained CodeBERT model might not always produce accurate result. | Fine-tune the CodeBERT model with a dataset of labelled vulnerability reports specific to our use case. |

# Priority Tasks Up Until the End of Project

According to our project plan, we are almost at the end of our project progress. Our next target will be to review the project draft and include/exclude the comment provided by tutor. Another task will be to integrate the generated AI into website system and do the Vulnerability scan test. Finally, we will provide executive summary of our project and provide the final recommendations. Kanban board figure below shows the completed project task and tasks remaining to-do.

Fig 22: Week-8 Kanban Board

Fig 23: Week-9 Kanban Board

# Project Plan

|  |  |  |
| --- | --- | --- |
| Task | Description | Deliverables |
| Industry Analysis for GenAI | Research current trends, challenges, and opportunities in GenAI implementation for cybersecurity. | Detail industry analysis report. |
| Stakeholder Identification and Analysis | Identify key stakeholders within the organization who will be impacted by implementing GenAI in cybersecurity. | -Stakeholders identification report  -Stakeholder matrix (influence/interest) |
| Ethical AI Framework Development | Create a framework for ethical AI implementation specific to GenAI implementation. | Ethical AI framework document |
| Website design and development | Develop and design website and deploy into AWS web server. | Show designed website. |
| Integrating AI into website hosting on AWS web server. | Design AI tool to detect vulnerabilities in cybersecurity and deploy into the website. | Show the results from security/ penetration testing on a system. |
| Risk Assessment and recommend security control to solve the problem | Identify and evaluate potential risks associated with GenAI implementation cybersecurity | - Risk assessment matrix - Risk mitigation strategies report |
| Collaboration Strategy Development | Develop strategies for proactive collaboration between security leaders and business stakeholders. | -Collaboration framework document  -Communication plan |
| Training Needs Analysis and awareness program | Assess the training requirements for both technical and non-technical staff regarding GenAI. | -Skills gap analysis  -Training need assessment report |
| Deploy and testing of chatbots and AI tool into website | Create and test chatbot into website. | Testing strategy and test case |
| Final Recommendations | Combine all findings and recommendations into a final report. | Executive summary |

# Contribution Table

|  |  |
| --- | --- |
| Bhuwan Thapa | Deploy WordPress into AWS cloud server and create website. Program coding for AI. System diagram. Flow chart. Network design. Design of Network/Security architecture. |
| Pratik Singh Dhami | Program coding for AI. Chatbot design. Helping in WordPress deployment, agile diagram. |
| Basanta Adhikari | Website design, Gantt chart, kanban board and project network diagram. Risk Assessment matrix. Stakeholder Engagement matrix |
| Kiran Bhusal | Resource collection and website design. Building chatbot and deploying in AWS. Implementation of Network/Security in server.Github workflow for CI/CD |

# Weekly Report

## 7.1 Week 1

|  |  |
| --- | --- |
| **Meeting Summary** | **Explanation** |
| Choose Project Topic | We have chosen the project topic name “Gen AI: Navigating Short-term Scepticism and Long-Term Promises”. |
| Setting up Communication Channel | We have shared the phone numbers of each group members for the emergency contact. Apart from that, we have created a messenger group to discuss about the project progress report. Also, we have a group in Microsoft Teams special for project discussion and report submission. |
| Introduction and Project overview | We have discussed about the project topic, goals, objectives and scope, as well as we have divided the individual work to prepare draft for project plan. |
| Initial Brainstorming | We have conducted a brainstorming session to generate ideas, identify source requirements and potential challenges and discussed about the project management plan. |

## 7.2 Week 2

|  |  |
| --- | --- |
| **Meeting Summary** | **Explanation** |
| Progress update on initial task | We had a submission of project plan for starting of week 3 so we keep updated to each member for the task that we have divided previous week. |
| Meeting with Tutor | It was the first meeting with tutor special for this project. We have discussed about the requirements of the project including technical specifications such as creating websites, chatbots and its deployment, and requirements for report writing. |
| Planning for future | We have divided individual responsibilities to complete the project, we have decided to work upon report writing on the topic of project plan such as individual roles and responsibilities, source requirement, risk and mitigation and ethical issues. Each member will contribute to prepare the report. |

## 7.3 Week 3

|  |  |
| --- | --- |
| **Meeting Summary** | **Explanation** |
| Review on previous submission | We had a project plan submission on first day of week 3, we make a review what could have been done and what we missed to include and discussed further with Tutor. |
| Tutor feedback | We have decided to add creating Automotive Industry website to deploy chatbot into, which was missing in the previous project plan. Also, we will add Gann chart along with Kanban Board. Furthermore, we will add flow chart and system diagram in the next submission progress report writing. |
| Individual responsibilities | We have decided to work on first four task that we have mentioned in our project plan. We will also collect the resource requirements and gather information to create a website. |

## 7.4 Week 4

|  |  |
| --- | --- |
| **Meeting Summary** | **Explanation** |
| Progress update on Initial Task | We keep updated about the individual task that we have divided for each member and merged into the same file. |
| Tutor Feedback | The feedback from Tutor was same as previous week 3. We have provided detailed information about how we are going to create websites and other coding part. We have discussed about the requirements of report writing 1 that we have to submit on the first day of week 5. |
| Individual Task division | We have decided to work upon creating flow chart and system diagram. Apart from that, we will finish the work of creating website by the end of week 4. We will prepare a report on what task we have done yet and what difficulties we have faced and how we able to overcome. We will submit the progress report including project progress report, future-plan and task that we have missed in previous submission. |

## 7.5 Week 5

|  |  |
| --- | --- |
| **Meeting Summary** | **Explanation** |
| Discussion progress of the project | In this week, we have discussed about the progress of the project. Mainly focused on the technical artefact for the project and individual contribution. We have a next submission of the assignment progress report 1. We have discussed about the individual contribution to complete the task.  Project progress are:   1. Website design and development 2. System diagram 3. Flowchart 4. Stakeholder engagement metrics 5. Network diagram 6. Gannt Chart 7. Agile methodologies for system development 8. Task divided for future |
| Making plan for future task | We have also discussed about the future task that we have to do. Our next submission assignment is preparing project draft. The mentor has provided the criteria and requirement to complete the task. We as a individual also divided individual task to complete the report. |

## 7.6 Week 6

|  |  |
| --- | --- |
| **Meeting summary** | **Explanation** |
| Discussion on project progress | In this meeting we have discussed about the progress on report writing and technical artefact. We had a submission on at the end of week 6 so We all were preparing report writing. The reporting includes:   1. The problem from a business and technical perspective. 2. Identification, selection and justification of appropriate network and security technologies. 3. Specification of requirements. 4. network designs. 5. Design of network/security architectures. 6. Network and security policies. 7. Risk assessment, 8. Recommended security controls to solve the problem etc.   Regarding the technical progress we have already designed the website and integrate chatbot in it which has proper functionality. |
| Update on project plan. | Our initial project plan was to integrate chatbot into website, but we noticed that chatbot will not be able to identify the cybersecurity vulnerability. Our mentor suggested that to generate a AI tool which detect the vulnerability in the website, which is the primary aim of the project. |

## 7.7 Week 7

|  |  |
| --- | --- |
| **Meeting summary** | **Explanation** |
| Discussion on project progress | In this week we have discussed about the assignment that we have just submitted; mentor gave us some advice to make changes over the report writing. Apart from that we have discussed about the technical artefact of developing AI. Also, mentor provided some advice about the meeting with industry partner, we have meeting with industry partner this Friday, where we will discuss about the project progress and project requirement. |

## 7.8 Week 8

|  |  |
| --- | --- |
| **Meeting Summary** | **Explanation** |
| Discussion on technical progress. | We have discussed about the overall technical progress of the project. We have already developed the website, and we have shown the practice presentation of AI that we developed along with vulnerability scan report and received positive response from the tutor. |
| Discussion on previous submitted assignment and future submission. | Tutor provided feedback on previous submitted project draft report and made some plan for future submission practice presentation and final report. |