**A yellow shield with blue and black logo

Description automatically generated**

**Hardhat Enterprise Structure & Objectives**

**Trimester 1 2024**

**(Mid-Trimester Update)**

**Executive Summary**

Hardhat Enterprises is an organization that enhances and strives to improve white hat operations' cyber security posture by safeguarding assets, reducing threats, and thwarting vulnerability exploits. This vision will be the focus of each project's deliverables throughout the trimester. The open-source security architecture, tools, processes, and mitigation techniques that are generated satisfy market gaps and requirements. Some deliverables due to their nature, like testing reports, are private to the appropriate parties.

Hardhat Enterprises will keep offering its staff members the following chances during this trimester:

• To improve their technical position by upskilling and putting their talents into practice.

• To provide students with networking opportunities so they can expand their networks and fortify their bonds with their teams by cooperating and working together.

• As students work toward the company's vision, demonstrate their abilities through the development, testing, and implementation of deliverables.

• By developing and improving the flow of deliverables throughout the organization and expanding on each project's area of expertise, strengthen the company's posture through inter-connectivity of projects.



Dr. Naeem Syed

Acting Director,

Hardhat Enterprises

Table of Contents

[**Company Structure and Project Overview**](#_bookmark37) 5-6

[General Overview](#_bookmark36) 5

[Trimester Goals and Objectives](#_bookmark35) 5

[Leadership Team](#_bookmark34) 5

[Project Relationships](#_bookmark33) 6

[**Company Projects**](#_bookmark32) 7-15

[App Attack 7-](#_bookmark31)9

[Overview, Goals, and Objectives](#_bookmark30) 7

[Aims for the Trimester](#_bookmark29) 7

[Trimester Deliverables](#_bookmark28) 7

[Long Term Deliverables](#_bookmark28) 8

[Project Members](#_bookmark26) 9

[Project Mid-trimester Progress 9](#_TOC_250043)

[Project Plan Updates 10](#_TOC_250042)

[Project Team Member Key Achievements 12](#_TOC_250041)

[Website Development](#_bookmark25) 10-11

[Overview, Goals, and Objectives](#_bookmark24) 10

[Aims for the Trimester](#_bookmark23) 10

Trimester [Deliverables](#_bookmark22) 10

[Project Members 1](#_bookmark21)1

[Project Mid-trimester Progress 9](#_TOC_250043)

[Project Plan Updates 10](#_TOC_250042)

[Project Team Member Key Achievements 12](#_TOC_250041)

[Penetration Testing GUI (PT GUI) 1](#_bookmark14)2-14

[Overview, Goals, and Objectives 1](#_bookmark13)2

[Aims for the Trimester 1](#_bookmark12)2

Trimester [Deliverables 12-13](#_bookmark11)

[Project Members 1](#_bookmark10)3-14

[Project Mid-trimester Progress 9](#_TOC_250043)

[Project Plan Updates 10](#_TOC_250042)

[Project Team Member Key Achievements 12](#_TOC_250041)

[Smishing Detection 15](#_bookmark9)-16

[Overview, Goals, and Objectives 15](#_bookmark8)

[Aims for the Trimester 15](#_bookmark7)

[Deliverables 1](#_bookmark6)5

[Project Members 1](#_bookmark10)6

[Project Mid-trimester Progress 9](#_TOC_250043)

[Project Plan Updates 10](#_TOC_250042)

[Project Team Member Key Achievements 12](#_TOC_250041)

[Deakin Threat Mirror 1](#_bookmark4)7-19

[Overview 1](#_bookmark3)7

[Objectives](#_bookmark28) 17

[Goals](#_bookmark28) 18

[Aims for the Trimester 1](#_bookmark2)8

Trimester [Deliverables 1](#_bookmark1)8

[Long Term Deliverables](#_bookmark28) 18-19

[Project Members 1](#_bookmark0)9

[Project Mid-trimester Progress 9](#_TOC_250043)

[Project Plan Updates 10](#_TOC_250042)

[Project Team Member Key Achievements 12](#_TOC_250041)

[Deakin CyberSafe VR](#_bookmark4) 20-21

[Overview](#_bookmark3) 20

[Objectives](#_bookmark3) 20

[Goals](#_bookmark3) 20

[Aims for the Trimester](#_bookmark2) 20

Trimester [Deliverables](#_bookmark1) 21

Long Term [Deliverables](#_bookmark1) 21

[Project Members](#_bookmark5) 21

[Project Mid-trimester Progress 9](#_TOC_250043)

[Project Plan Updates 10](#_TOC_250042)

[Project Team Member Key Achievements 12](#_TOC_250041)

# Company Structure and Project Overview

## General Overview

During Trimester 1, 2024 (this trimester), Hardhat Enterprises is working on six (6) projects, with each of the projects working towards the shared company goal. The projects are as follows:

* AppAttack
* Website Development
* Penetration Testing GUI (PT-GUI)
* Smishing Detection
* Deakin Threat Mirror
* Deakin CyberSafe VR

## Trimester Goals and Objectives

In Trimester 1 2024, Hardhat Enterprises aims to:

* Provide opportunities to students to engage in an active learning experience.
* Allow opportunities for students to gain project experiences, with opportunities to develop and share the expertise within hardhat both within and between projects.
* Mature and further the existing projects – AppAttack, Website Development, Smishing Detection, PT- GUI and Deakin Threat Mirror.
* Incubate new projects – Deakin CyberSafe VR.
* Provide interproject collaboration opportunities, shaping Hardhat Enterprises into an interconnected and formal company structure.

## Leadership Team

This trimester, Dr. Naeem Syed is the acting Director of Hardhat Enterprises. The below outlines Hardhat Enterprises leadership team for Trimester 1 2024.

A diagram of a company's company

Description automatically generated

## Project Relationships

A diagram of a computer security system

Description automatically generated

# Company Projects

## App Attack

### Overview, Goals, and Objectives

The goal of AppAttack is to provide a thorough security analysis of ThotTech's OnTrack Project, a web application that instructors and students use for formal assessment in coursework-based topics. To find vulnerabilities and improve the project's overall security posture, the focus will be on doing a secure code review and penetration test. The goal of AppAttack is to provide a thorough security analysis of ThotTech's OnTrack Project, a web application that instructors and students use for formal assessment in coursework-based topics. To find vulnerabilities and improve the project's overall security posture, the focus will be on doing a secure code review and penetration test.

All team members participating in the testing may access a secure, sandboxed OnTrack environment that AppAttack has set up and housed within a Kali Linux virtual machine. A forked copy of the code is used to build this sandboxed instance, ensuring a controlled testing environment while protecting the privacy of the live system. To thoroughly examine OnTrack for flaws in its security posture, code errors, and vulnerabilities, testers will assume the viewpoint of external attackers. We employ both automatic and manual attack techniques to thoroughly evaluate OnTrack's security. After the assessment is finished, AppAttack will provide ThotTech with a thorough security report that lists all vulnerabilities found and suggests fixes.

This study will improve the security status of the OnTrack application by providing guidelines for properly hardening the application and its underlying code. AppAttack hopes to provide ThotTech with useful insights to strengthen the security of the OnTrack Project with this thorough security evaluation.

### Aims for the Trimester

Establishing a fruitful partnership with ThotTech's Ontrack Project is the main goal of AppAttack, with an emphasis on carrying out a comprehensive security assessment of their web application. AppAttack simultaneously looks at potential joint ventures with other Capstone firms. AppAttack hopes to create a collaborative atmosphere through this effort where our experience in secure code review and penetration testing can be used to different projects, providing a synergistic effect. By working together, we hope to maximise the effectiveness of our security evaluations and promote the sharing of knowledge.

### Trimester Deliverables

* Pentest and SCR Finding and Remediation Report: A thorough report including the findings from secure code reviews and penetration tests, as well as suggested corrective actions.
* Sandboxed testing environment hosting: To enable safe testing and experimentation, a sandboxed testing environment may be established inside a virtual machine.
* Planning and Reporting for Incident Response: creating an incident response strategy and offering a thorough report on how it was carried out.
* Strengthen Security standing: set measures in place to strengthen the security position of the organization.

### Long Term Deliverables

* Collaboration Establishments with other capstone projects: Forming partnerships with additional capstone projects to encourage the exchange of knowledge and promote synergy.
* Research and build upon AppAttack Future vision: Conducting research and refining the long-term vision for the advancement and prosperity of AppAttack.
* Update upskilling resources and testing methodologies: Regularly updating resources for skills enhancement and testing techniques to ensure they are up to date.
* Establish a safe security culture amongst team members: Cultivating a secure culture within the team by fostering awareness and accountability for cybersecurity.

To meet our objectives for this trimester and provide the groundwork for AppAttack's ongoing development and success, these deliverables are crucial.

### Project Members

|  |  |
| --- | --- |
| **STUDENT NAME** | **ROLE** |
| **ROOCHA THAKKAR** | Project Co-Lead |
| **CHARANPREET SINGH** | Project Co-Lead |
| **NABIHA MASOOD** | Penetration Testing Team Lead |
| **OLIVER POWER** | Penetration Testing Team Lead |
| **PAARTH DANDONA** | Penetration Testing Member |
| **SEHANDU MATHIKA KURUKULARATNE** | Penetration Testing Member |
| **NATALIA KHOBOTOVA** | Penetration Testing Member |
| **MOHAMMAD AREF NOURI** | Penetration Testing Member |
| **SHAYNE ROBERT DAWSON** | Penetration Testing Member |
| **DEV NITESHKUMAR PATEL** | Penetration Testing Member |
| **HASHINI UPAMALIKA WEERASURIYA DASSANAYAKAGE** | Penetration Testing Member |
| **HARPREET SINGH** | Penetration Testing Member |
| **DONTE MARC VELONA** | Penetration Testing Member |
| **JOSHUA ERIC JANSEN** | Penetration Testing Member |
| **SHARIQUE AIZAZ** | Penetration Testing Member |
| **ALLEN GEORGE THEKKEMURIYIL** | Penetration Testing Member |
| **ALBORUGE POORNA UDAYANGA DABARE** | Penetration Testing Member |
| **VISHNU MADHUSOODANAN NAIR** | Penetration Testing Member |
| **DONGHWAN KIM** | Penetration Testing Member |
| **MOHNISH SHARMA** | Penetration Testing Member |
| **JASPRIYA KAUR** | Secure Code Review Team Lead |
| **PAYAS PAUL** | Secure Code Review Team Lead |
| **ALYSHIA GUSTAFSON** | Secure Code Review Member |
| **GAURISH BHATIA** | Secure Code Review Member |
| **MANASA VALLABOJU** | Secure Code Review Member |
| **SANGEETH SUBBURAM** | Secure Code Review Member |
| **TON HOANG NGUYEN** | Secure Code Review Member |
| **DEAKIN CARR** | Secure Code Review Member |
| **BYEONGNAM CHOE** | Secure Code Review Member |
| **SHAMAIL HAIDER** | Secure Code Review Member |
| **PUSHKAR GOEL** | Secure Code Review Member |
| **KHUSHLEEN KAUR DHINDSA** | Secure Code Review Member |

## Website Development

### Overview, Goals, and Objectives

The Hardhat Website Development project is designed to develop and enhance the company website with the view of showcasing the company to its potential clients and stakeholders. The objective and goal of this project is to construct and consolidate the state-of-the-art web application which can be used to-

* Display Hardhat’s projects, products, and services.
* Allow students and significant customers to get involved with the company.
* Streamline the project selection process for students.
* Facilitate an informed decision-making process for students interested in joining the company.

### Updated Aims for the Trimester

Throughout Trimester T1 2024, the Website Development team plans to:

* Develop all the documented product backlogs by converting them into Sprint backlogs.
* Conduct regular standups to discuss updates, hurdles, backlogs, and solutions.
* Consolidate existing features like User Profile, Login Authentication, Interactive front-end UI, and database systems.
* Append new features namely- Blog and Resource Tracker for all projects.
* Deploy website from PythonAnywhere platform.

### Trimester Deliverables

To present the contributions made during the trimester, the following deliverables will be submitted by the project leads:

* A fully working interactive website with the developed features.
* Complete documentation of the project and the product with all the details and backlogs.
* A future recommendation with feature suggestions for the future groups to work on the website.
* A rundown of all the website backlogs that need to be fixed in the upcoming trimesters.

### Long-Term Deliverables

Besides the short-term trimester deliverables, the project will also be focusing on the following long-term deliverables:

* Develop a consultation feature on the website which can be used by users or other clients to hire the cyber-security teams advertised on the website.
* Use achievement and past stories as a form of portfolio and advertisement for new customers to rely on.

### Project Members

|  |  |
| --- | --- |
| **Student Name** | **Role** |
| **MD KAVIUL HOSSAIN** | **Project Lead** |
| **UZAIR ZAFAR** | **Junior Co-Lead (Frontend)** |
| **KUSHALPREET KAUR** | **Junior Co-Lead (Quality Assurance)** |
| **NICHOLAS ALEXANDER** | **Junior Co-Lead (Backend)** |
| **MD JALAL FEROJ** | **Project Member** |
| **CALLAM JOZSEF BESLEY** | **Project Member** |
| **GINNI GINISH KUMAR** | **Project Member** |
| **AUSTIN FARAJ** | **Project Member** |
| **JATIN GAUTAM** | **Project Member** |
| **ZOE KIRA CHAMBERS** | **Project Member** |
| **MANAN MEHTA** | **Project Member** |
| **ZEYU CHEN** | **Project Member** |
| **VITTHAL CHANDER SATIJA** | **Project Member** |
| **RAJA SINGH** | **Project Member** |
| **KAWTHAR HASSANADDIE** | **Project Member** |
| **WAQAS SARWAR** | **Project Member** |
| **FANGZHOU ZHAO** | **Project Member** |
| **SAMYAM JEET SHRESTHA** | **Project Member** |
| **DIEP ANH VU** | **Project Member** |

[Project Mid-trimester Progress](#_TOC_250043)

[Project Plan Updates](#_TOC_250042)

[Project Team Member Key Achievements](#_TOC_250041)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** **Key** **Achievements** | | | | | | |
| **MD KAVIUL HOSSAIN** | **Leadership Contributions:** |  |  |  |  |  |
| **UZAIR ZAFAR** | **Leadership** **Contributions:** Produced documents for project, sub-teams like | | | | | |
| **KUSHALPREET KAUR** | **Technical** **Contributions:** Identified 2 PT findings: | | | | | |
| **NICHOLAS ALEXANDER** | **Mentoring** **Contributions:**   * Scheduled a workshop for August 24, 2024, demonstrating scoping, vulnerability exploration, and exploitation.   **Technical** **Contributions:**   * Submitted a vulnerability finding for potential inclusion in the final report and collaborated to merge with a duplicate finding.   **Non-Technical** **Contributions:**   * Provided meeting minutes for an undocumented meeting, summarizing key points and questions. * Actively researched student support in pen testing team chat and private Teams chats. | | | | | |
| **MD JALAL FEROJ** | **Leadership** **Contribitions:**   * Responded to team feedback and onboarding survey, identifying a need for additional support and guidance in pen testing. * Organized multiple workshops led by team members to foster leadership skills.   **Mentoring** **Contributions:**   * Proactively supported team members by tracking their progress and providing assistance, including technical troubleshooting. * Prepared and presented a workshop to benefit the entire AppAttack cohort.   **Technical** **Contributions:**   * Conducted quality assurance on findings and validation of penetration test results. * Developed penetration testing findings and reports, including an email server DDoS exploit (pending release).   **Non-Technical** **Contributions:**   * Facilitated communication between leadership and team members to ensure team-wide awareness. * Encouraged team members to showcase their leadership skills and contribute effectively. | | | | | |
| **CALLAM JOZSEF BESLEY** | **Technical** **contributions:** Finalized PT finding on file path traversal.  **Non-technical** **contributions:** Active communication with PT team. | | | | | |
| **GINNI GINISH KUMAR** | **Technical** **Contributions:** Identified some SCR findings, currently pushing  them to completion. | | | | | |
| **AUSTIN FARAJ** | **Technical** **Contributions:** | | | | | |
| **JATIN GAUTAM** |  | | | | | |
| **ZOE KIRA CHAMBERS** |  | | | | | |
| **MANAN MEHTA** |  | | | | | |
| **ZEYU CHEN** |  | | | | | |
| **FANGZHOU ZHAO** |  | | | | | |
| **RAJA SINGH** |  | | | | | |
| **SAMYAM JEET SHRESTHA** |  | | | | | |
| **WAQAS SARWAR** |  | | | | | |
| **VITTHAL CHANDER SATIJA** |  | | | | | |
| **KAWTHAR HASSANADDIE** |  | | | | | |
| **DIEP ANH VU** |  | | | | | |

## Penetration Testing GUI (PT-GUI)

### Overview, Goals, and Objectives

The Deakin Detonator Toolkits (DDT) aims to simplify penetration testing by integrating a user-friendly interface that narrows the gap between the operator and command line. It includes comprehensive documentation and instructions for each tool which will transform the learning experience for beginner developers and reshape how penetration testing methods are applied.

Currently, DDT comprises of 44 built-in tools, 5 Attack Vectors and 12 walkthroughs, of which 36 tools have achieved basic functionality.

This trimester, the DDT team aims to make sure all the current 44 tools achieve maximum functionality and meet industry standards. Moreover, we have decided to resume integrating new tools into DDT. To make sure every implementation of new tools and functions works as expected we would deploy testing frameworks developed last year to identify underlying bugs before merging them into the main product.

Upon finishing sprint 3, a refurbished version of DDT will be released for Hardhat Enterprise, establishing itself as a benchmark for penetration testing tools. Feedback and analysis generated by real-world usage through Hardhat Enterprise developers will offer valuable insights, benefiting the ongoing development of DDT.

### Aims for the Trimester

* **Refine existing tools:** Enhancement of the usability and functionality of current tools within DDT.
* **Improve usability:** Investigate the implementation of file uploader functionalities and explore other general improvements as well.
* **Standardize coding practice**: Develop a framework to standardize coding practices across all contributors in the project.
* **Integrate new tools:** Research and implement new penetration testing tools into DDT.

### Trimester Deliverables

## Trimester 1, 2024 Deliverables:

* **Enhancement of existing tools:** Fix current bugs that exist within tools in DDT to achieve maximum functionality. The current plan is to eliminate all bugs across various tools existing under the “tools” section.
* **Usability improvement:** Implement file uploader, save output files and process termination functionalities to all tools to improve the functionality and usability of DDT.
* **Coding style framework**: Develop a framework that outlines the coding practices and styles that are currently used to ensure efficiency and quality throughout the whole project.
* **Test Summary Report**: This report tracks the progress made in DDT. This report will serve as a detailed snapshot of the testing process, providing an overview of the testing, highlighting not only pass/fail outcomes but also the test coverage, any issues encountered and any pending tasks.
* **New release of DDT version:** Release an updated and refurbished version of DDT with improved functionalities to Hardhat Enterprise by the end of sprint 3.

## Long-Term Deliverables:

* **Test Summary Report:** To keep a detailed record of progress, a comprehensive Test Summary Report will be generated at the conclusion of each upcoming trimester until the development of DDT reaches completion.
* **Test Automation:** Utilize automated testing to enhance efficiency, uniformity and uphold industrial standards.
* **Test Closure Report:** Once the application has met all its desired functionalities and is set to be deployed to the public, the Test Closure Report will sum up the entirety of the testing process, emphasizing valuable insights, knowledge gained and future recommendation for upcoming projects.

### Project Members

|  |  |
| --- | --- |
| **Student Name** | **Roles** |
| **Bradley Bogg** | **Project Lead** |
| **Zhen Kang Kok** | **Project Co-Lead** |
| **Michael John Pigott** | **Project Co-Lead** |
| **Sebastian Rao** | **Project Member** |
| **Seth Johnson** | **Project Member** |
| **Arshpratap Singh Somal** | **Project Member** |
| **Matthew Mina Mikhail** | **Project Member** |
| **Jashanpreet Singh Kamboj** | **Project Member** |
| **Syed Ubaid Ahmed** | **Project Member** |
| **Stephen Peterson** | **Project Member** |
| **Abbas Biju** | **Project Member** |
| **Neris Sherwell** | **Project Member** |
| **Vittorio Truglio** | **Project Member** |
| **Naveenkumar Yogavijayan** | **Project Member** |
| **Aafiya Irfan** | **Project Member** |
| **Jonathon Guido Schlack** | **Project Member** |
| **Anjo Puthanpurackal Joseph** | **Project Member** |
| **Kevin Jose** | **Project Member** |
| **Naman Bakshi** | **Project Member** |
| **Srujana Sravanthi Gudey** | **Project Member** |
| **Luv Manish Ghodasara** | **Project Member** |
| **Ankit Bhardwaj** | **Project Member** |
| **Siddharth Raj** | **Project Member** |
| **Gurneet Singh** | **Project Member** |
| **K S H M Vihare Walawwe Sameera Buwaneka Senevirathne** | **Project Member** |
| **Shubham Chandel** | **Project Member** |
| **Waqas Sarwar** | **Project Member** |
| **Cyriac Jose** | **Project Member** |
| **Maria Rose Francis** | **Project Member** |
| **Ganga Marx** | **Project Member** |
| **Justin Carr** | **Project Member** |
| **Isaiah Spokes** | **Project Member** |
| **Gia Thien Thai** | **Project Member** |
| **Harsh K Patel** | **Project Member** |

[Project Mid-trimester Progress](#_TOC_250043)

[Project Plan Updates](#_TOC_250042)

[Project Team Member Key Achievements](#_TOC_250041)

## Smishing Detection

### **Overview, Goals, and Objectives**

This project aims to develop an innovative smishing detection app for Android and iOS devices to moderate the risks associated with SMS phishing attacks. The motivation behind this project is the escalating use of smartphones for sensitive communications and transactions, making them prime targets for smishing attacks. Our long-term goals include enhancing mobile security for users, providing tools for cybersecurity awareness, and contributing to the broader fight against scammers. By successfully detecting and alerting users to smishing attempts, we intend to protect personal information and reduce the frequency of fraud.

### **Aims for the Trimester**

For this trimester, the project aims to:

* Review and update the design: Review and finalize the app's design, focusing on user interface (UI) and user experience (UX) to ensure ease of use and accessibility.
* AI research: Investigate and develop AI-based algorithms capable of identifying smishing content in SMS messages.
* Developing a prototype: Build a functional prototype that incorporates AI research findings and demonstrates basic smishing detection capabilities.
* Database development: Initiate the creation of a database for storing patterns, indicators, and characteristics of smishing attacks.
* User testing: Conduct user testing sessions to gather feedback on the app’s usability and effectiveness in detecting smishing attempts.
* Documentation and transition planning: Prepare documentation and resources to ensure a seamless transition to future project teams.

### **Deliverables**

## **Long-term Deliverables:**

* A functional smishing detection app for Android devices.
* A database of smishing patterns.
* Expansion of the smishing detection app to iOS devices.
* Documentation covering all aspects of the project, including design, development, use, future enhancement, and testing methodologies.

## **Trimester Deliverables:**

* Review and update the UI/UX design.
* Initial AI algorithm for smishing detection.
* A prototype version of the smishing detection app.
* Ethical review of the app.
* Beginning database structure and schema.
* Initial user feedback report.
* A progress report and documentation for the next phase.

### **Project Members**

|  |  |
| --- | --- |
| **Student Name** | **Role** |
| **Jasmine Guccione** | Frontend Project Member and Project Co-Lead |
| **Aiden Wiltshire** | Backend Project Member and Project Lead |
| **Ankit Prakash** | Frontend Project Member |
| **Jack Stjepanovic Johnson** | Backend Project Member |
| **Deepak Damodaran** | Frontend Project Member |
| **Shubham Mahajan** | Backend Project Member |
| **Damian Miller** | Frontend Project Member |
| **Harshit** | Frontend Project Member |
| **Nianru/Natasha Jiang** | Backend Project Member |
| **Gladiz Gregory** | Backend Project Member |
| **Oliver Tait** | Frontend Project Member |
| **Nicholas Szyrpallo-Martin** | Backend Project Member |
| **Tashin Bin Shahed** | Backend Project Member |
| **Virantha Bimsara Mudalige** | Backend Project Member |
| **Ulindu Perera** | Backend Project Member |
| **Ajay Ningappa** | Frontend Project Member |
| **Kevin Trieu** | Frontend Project Member |
| **Hnin Ei Khaing** | Backend Project Member |
| **Shan Arunkumar Patel** | Backend Project Member |
| **Hassan Shabeer** | Backend Project Member |

### **Smishing Detection Mid-Trimester Progress:**

Front End

* UI/UX design completed and currently in the process of being implemented.
* Ethical review is being completed.
* Initial testing in being conducted.
* New features are being created and implemented in the app.

Back End

* Database of smishing, spam and harmless messages was built, formated and added upon for use in machine learning
* Setup the base android application
* First prototype algorithm was made utilising the Database giving us the ability to predict whether or not a sample message is either smishing, spam or harmless.
* The functionality of using the algorithm to predict a database of messages identity (smishing, spam or harmless) was added to allow for it to be used on a message base retroactively adding the ability for it to recategorise your messages into smishing, spam and harmless folders
* Login functionality being worked on for the android application
* Research and development to make the smishing detection algorithm more accurate being undertaken

### **Smishing Detection Plan Updates:**

Front End

* Creation of multiple different features for the app. Including an API integrated News feature, reporting feature, notification feature, home page features and finally the detection page summary which will communicate with the database.
* The creation of a Cybersecurity, data regulation, and compliance document has been included into our plans.
* Creation of handover documents have been pushed back to be completed in week 9.

Back End

* Continue development of the smishing detection algorithm testing various models in hopes of improving accuracy of its predictions.
* Continue development of the login functionality for the app and adding functionality to accounts.
* Integrate the machine learning algorithm into the android application.
* Create handover documentation for the backend team around week 9

**Smishing Detection** [**Team Member Key Achievements**](#_TOC_250041)

|  |  |
| --- | --- |
| **Student Name** | **Key Achievements** |
| **Jasmine Guccione** | Technical Contributions   * Currently trying to develop functionality for real-time alerts on smishing scams. * Designed and implemented the login page and notifications settings page; collaborated on UI/UX improvements. * Created pop-up permissions requests and button functionality. * Began learning about API integration for enhancing app news functionality. * Used Java to integrate features smoothly using tools like Visual Studio Code and Android Studio.   Non-Technical Contributions   * Ensured code and project updates were well-integrated and communicated across the team. * Constantly updating Trello board and ensuring other are also.   Leadership Contributions   * Led weekly meetings, managed Trello board, and used MS Teams for effective communication and task tracking. * Provided mentorship and hands-on support, fostering a supportive and collaborative team environment. Especially, helping the team download the correct tools needed for this project. |
| **Aiden Wiltshire** | Technical Contributions   * Developed The main smishing, spam, ham database and added to it building a comprehensive database formatting it so that it could be utilized by a machine learning algorithm. * Developed the initial smishing detection algorithm using linear regression that can detect whether a message was smishing, spam or ham. * Developed functionality to the python code that allows the detection algorithm to be run on a csv file of messages and predict whether each of them is smishing, spam or ham. * Setup our team's working environment of android studio and Github desktop and held a recorded meeting showing how to set it up.   Non-Technical Contributions   * Added many of the backend Trello tasks to our team board and helped assign team members to tasks. * Updated the team in meetings how the backend code is progressing and how it works. * Paired team members that were already friends to work together on tasks to increase productivity   Leadership Contributions   * Conducted weekly team meeting, oversaw the project’s Trello board, and utilized Microsoft Teams to streamline communication and monitor project tasks. * Offered guidance and practical assistance, nurturing a team culture that values support and cooperation. This included ensuring the team had access to and could successfully install the necessary software for the project. In addition, I developed extra tasks that would help the team work more easily toward the common goal. |
| **Ankit Prakash** | Non-Technical Contributions   * Working on documentation for ethical considerations to be considered while developing a smishing detection application * Working on creating a comprehensive document addressing cybersecurity measures, data regulation, and compliance.   Technical Contribution   * Working on setting up the Privacy policy and Term and Condition pop-up feature as well as its documentation. |
| **Jack Stjepanovic Johnson** | Non-technical Contribution:   * I asigned myself to trello tasks that needed to be completed. * I effectively communicated in the weekly meetings and texts.   Technical Contribution:   * Implementation of user login validation in the backend. |
| **Deepak Damodaran** | Technical Contribution:   * Terms and conditions page for the app. Link for T&C on login page and page for T&C has been done in own GitHub repository. Working on Terms and condition document and list of T&C to be included in the page. Once finished will be able to push the code to the company GitHub.   Non Technical Contribution:   * Working as a team member in creating ethical consideration documents. Documenting the research finding of the section assigned to me. * Working on Cyber security documents for the application for both the development team and also for end users. Currently researching on the scope of the document for the application. |
| **Shubham Mahajan** | Technical Contribution:   * Developed sample databases for the backend team for detecting spam or ham messages * Set up android studio and connect it to Github for using it to test code for the app. * Upskilled my ability to write and understand code in Java and python * Tested the sample dataset within the app   Non Technical contribution:   * Assigned myself documentation tasks and started working on them from trello cards * Teamed up with fellow members to boost productivity by working on common tasks. |
| **Damian Miller** | App design in Figma – Completed the design for the app in Figma for the front-end team to follow when implementing into Android Studio. The designing of the app included deciding layouts, content placement, and user flow, ensuring seamless navigation and intuitive interaction throughout the application.  Implementing app design into Android Studio – Completed implementing the app design from Figma into Android Studio for most pages, excluding the login, news, and help/information page. While implementing the design, focused attention was dedicated to specific functionality for items such as the bottom navigation bar, and to/from other page buttons.  Reporting function – Working on functionality for the reporting function, I implemented an idea of the report including the undetected phone number and message being sent to a company email to be analysed. I was successful in the addition of this function through the use of the Java Mail API.  GitHub contributions - After successful implementation of work in Android Studio, I would push multiple contributions to the front-end branch for the team to access. |
| **Harshit** | Preparing a report for UI/UX Testing – I have created a report from many online sources as well as my experience as a UI Tester for a SQL Project  App Structure - Worked alongside Jasmine to design the structure of the app’s pages/screens, focusing on placements and visuals using LucidChart  Implementing help/info page design.  Add new trello cards to the board |
| **Nianru/Natasha Jiang** | **Technical Contribution**   * Collaborated with Gladiz on combining machine learning models * Modularised machine learning code, enhances reusability, flexibility and readability by organising importable functions * Developed a combined model structure utilising modular import functions, enabling testing multiple models and multiple messages * Implemented a voting system to combine outputs from multiple models * Optimised combined code structure to avoid repetitive training process to improve efficiency * Implemented Data balancing and test out in code dataset optimisation   **Non-technical Contribution**   * Research on ways to improve machine learning algorithm accuracy   + Discovered the impact of dataset balance   + Reviewing academic research on machine learning practices for implementation   + Research general directions to improve accuracy, suggest potential features and improvements * Gathered relevant resources for the project (datasets) * Upskill: learning from online resources and research papers on smishing landscape, machine learning, and Python programming * Regularly update progress on Trello, create Trello card, and configured GitHub for effective code collaboration with Gladiz * Participated in weekly mentor meetings and project meetings |
| **Gladiz Gregory** | Technical Contributions:   * Codebase Refinement: Enhanced the readability and clarity of the codebase by eliminating unnecessary functionality * ML model testing: Conducted testing of databases using five distinct machine learning models, discovering that Random Forest (RF) produced the highest accuracy. * Hyperparameter optimization: Implemented GridSearch and RandomSearch into the codebase to enhance accuracy * Feature Engineering: Integrated stemming and tokenization techniques in the codebase to preprocess text data effectively, improving model performance. * Combined AI models: Created a new codebase that integrates input messages with five different machine learning models to determine which model has the best accuracy.   Non-technical Contributions:   * Project management: Updated Trello cards to demonstrate my progress and keep a personal log of findings * Skill improvement: Upskilled in Python, broadening my knowledge to make a more meaningful contribution to the project. * Research: Investigated ways to add new parameters to  improve the algorithm's accuracy and support continuous development. Research was also conducted on feature engineering methods to improve the system's accuracy * Communication: Attended and contributed to weekly meetings. Collaborated with Natasha to achieve some tasks. |
| **Oliver Tait** | Technical Contributions:   * Collaborated in the creation of application pages - specifically the debug page and account settings page * Designed and implemented a notification system for our application - utilizing Java and Object-Oriented Programming principles * Created and collaborated in the creation of the application’s “Design Standard” document - which is a document to provide specific details regarding the style, functionality and flow of the application   Non-Technical Contributions:   * Contributions to team discussion * Attending and setting up meetings with team members i was working with in joint project goals * Actively updating and showing my contributions in Trello |
| **Nicholas Szyrpallo-Martin** | Technical Contributions:   * Created back-end code for the login page. It’s currently capable of receiving the user's email/password and checking to see if it is contained in a pre-filled array. Currently working on implementing a suitable database for storing our users details. * Found training data for the machine learning algorithm.   Non-Technical Contributions:   * Created an evaluation report for our apps installation guide. * Upskilled in Java. * Researched how to use Microsoft Azure as our apps database. |
| **Virantha Bimsara Mudalige** | Non-Technical Contributions:   * Created reports about smishing attacks, how they work, the various types of smishing attacks, and included numerous screenshots of smishing messages. * Conducted research on smishing detection applications and solutions. * Reflected and showcased my latest contributions by updating the trello board.   Technical Contributions:   * Compiled my own dataset to train the AI model. * Currently working on adding account functionality to the android app. |
| **Ulindu Perera** | Technical Contributions:   * Created the two training datasets for the machine learning algorithm. * Currently working on the functions and features of the app.   Non Technical Contributions:   * Created the meeting minutes for the first backend meeting. * Updated and contributed to the Trello tasks which are completed now. * Upskilled in Java, Android Studio, and machine learning concepts. * Currently researching Ethical Considerations. |
| **Ajay Ningappa** | Technical Contribution   * Working on incorporating a Dark theme for the application. * Working on features to develop and display any and all error messages on the application.   Non-technical/Knowledge seeking   * Being aware of the way the unit learning outcomes have influenced the assessment design. and what I need to do to finish the assessments in order to get the grades I want. * Upskilling by learning the basics of the programming language java. * Upskilling by understanding the official IDE for android development Android studio. * Understanding of UI/UX design principles for fundamental design such as layout, typography, color theory and usability. * Understanding of responsive web design techniques to ensure our application looks and functions well across various screen sizes and devices. * Awareness of common security vulnerabilities in mobile applications and how to mitigate them, such as data encryption, secure authentication and secure data storage. |
| **Kevin Trieu** | * Working on research and write up for Documentation for Ethical Considerations for the Smishing Detection App. Working with 3 other members for this task and have collaborated with them through Teams * Working on a Reporting Function to report suspected smishing messages that the AI may have missed. * Used Trello to assign myself to tasks/update other project members on my tasks and MSTeams to communicate and collaborate with team members. * Upskilling by learning how to use Android Studio and Github which is used to run and make changes to code in the Smishing Detection app. * Upskilling in Java |
| **Hassan Shabeer** | Technical Contributions:  1. Spam Detection Development: Developed and refined databases for backend use, differentiating between spam and legitimate messages, and enhancing the project’s spam detection capabilities.  2. Android Studio Integration: Configured Android Studio and linked it to GitHub, streamlining code testing and version control processes for the application development.  3. Innovative Spam Chat Box: Led the research and conceptualization of a spam detection chat box feature, designed to improve user interactions and bolster security measures.  4. AI Tools Configuration: Installed and set up essential AI development tools like Python, pandas, Anaconda, and Scikit-Learn, boosting the project's data analysis and machine learning potential.  5. Skill Enhancement in Java: Improved Java programming skills within Android Studio, now applying this expertise to develop and refine the Add account functionality to the Android Studio (e.g. account creation/deletion and password change functionality), focusing on user experience and system security within Android Studio.   Non-Technical Contributions:  1.      Documentation and Project Management: Managed documentation tasks systematically using Trello, ensuring efficient progress tracking and organization.  2.      Team Collaboration and Support: Enhanced team productivity by partnering with colleagues on shared tasks and supporting team leads to alleviating their workload:- like leading Research into implementing a blacklist of words to make spam and smishing detection more accurate.   Recent Focus and Future Outlook:  - Data Collection and Analysis: Spearheaded the collection and documentation of diverse SMS datasets, gaining deep insights into smishing tactics which inform ongoing detection strategies.  - User Authentication Features: Currently enhancing the signup and login pages, aiming to improve user experience and security—a direct application of upgraded Java skills.  - Continued Professional Development: Committed to further upskilling in technical areas by the end of this week, aiming to contribute even more effectively to the project's technological advancements.  - Active Participation in Meetings: Contributed to weekly project discussions, fostering a collaborative and innovative team environment.  - Ongoing Skill Development: Committed to further developing technical skills, particularly in AI and Java programming, to significantly enhance contributions to the project by the end of this week. |

## Deakin Threat Mirror

### Overview

In today's digitally interconnected landscape, the amount of data produced is vast, with a considerable portion being readily accessible in the public domain (Yadav et al., 2023) and so is, the frequency and complexity of cyber threats. As per cyber threat report by Australian Signals Directorate's Australian Cyber Security Centre, 50 percent of the vulnerabilities are exploited within 2 weeks from the time the patch or mitigation is released, emphasizing the need for prompt patching (ASD’s Australian Cyber Security Centre (ACSC), 2023). On the contrary many SMEs and developing economies do not even know that they have vulnerable or infected digital assets. Cyber Threat Intelligence (CTI) constitutes crucial role in equipping organizations with the necessary knowledge and tools to effectively anticipate and mitigate cyber risks in data driven digital space (Saeed et al., 2023). This process entails the systematic acquisition, processing, evaluation, and dissemination of information pertaining to potential threats and opportunities within the cyber domain.

Recent incidents, such as the widespread ransomware attack on small businesses in Southeast Asia (CYFIRMA, 2023), highlight the urgent need for accessible, affordable, and robust cybersecurity solutions. While there is a plethora of data and tools out there, the inability of developing economies and SMEs to consolidate and make intelligence out of it leaves them exposed.

Therefore, this project aims to technically review the existing open-source threat intelligence platform with an aim to find features and gaps specific to the needs of SMEs and developing economies. In an ever-evolving landscape of digital risks, we aim to provide a robust platform powered by open-source tools to aggregate, process, and convert diverse threat feeds into meaningful intelligence thus enabling organizations that cannot afford commercial Threat intelligence platforms to gain visibility before they are exploited. The long-term vision of the project is to build threat intelligence platform with capabilities to analyze and visualize data from external threat feeds and internal malware analysis data. The ability to integrate the solution into existing security solutions in place including SIEM/XDR, Incident response ticketing system, vulnerability management and malware information sharing platforms will be a priority.

### Objectives

A significant proportion of SMEs and developing economies are underprepared for cyber threats, as evidenced by a survey showing that 50% of SMBs have experienced cyberattacks (Aguilar, 2015)​​. Additionally, McKinsey's research highlights that the cybersecurity needs of SMEs are often not adequately met, with varying requirements based on their IT maturity​​ (Aiyer et al., 2021). This project therefore aims to investigate open-source threat intelligence platforms, assessing their suitability and adaptability for SMEs and developing economies. The objective is to develop a feasible solution that bridges this gap, providing simplified, cost-effective, and efficient CTI platform tailored to the unique challenges and limitations faced by these sectors.

Goals

* Investigate existing open-source threat intelligence platforms for suitability to SMEs and developing economies.
* Identify cybersecurity needs and gaps in terms of policies, frameworks, and unique challenges.
* Design and develop a customizable and scalable CTI platform tailored to SMEs and developing economies.

### Aims for the Trimester

This trimester we aim conduct technical review of more open-source tools and feed sources, conduct in-depth research of challenges unique to SMEs and developing economies, and initiate the design and development of Deakin Threat Mirror.

### Trimester Deliverables

* Research report on unique challenges faced by SMEs and developing economies in terms of threat visibility and intelligence capabilities.
* Research Report on policies and frameworks (national, regional, global) that impact the sector.
* Research Report on use of AI/ML and genAI in Threat Intelligence.
* Metrics for measuring cyber health.
* Technical review report on more open threat intel platforms
* Manuals and configurations for tools that would be integrated to the platform.
* Manual and scripts for identified threats and vulnerabilities.
* Design of Deakin threat Mirror
* Deakin Threat Mirror platform 1st release

### Long-Term Deliverables

* Conduct comprehensive testing of the platform, including functional testing, performance testing, and collaborate with AppAttack for security testing.
* Partner with SMEs and developing economies to roll out the platform.
* Optimize platform performance based on feedback from user testing and pilot deployments.
* Provide comprehensive training sessions and workshops to educate users on platform functionalities, cybersecurity best practices, and threat mitigation strategies. Possibly partner with Deakin CyberSafe VR to design interactive training.
* Offer ongoing support and assistance to users through a dedicated user community forum.
* Monitor user adoption and engagement metrics, including active users, frequency of platform usage, and user satisfaction ratings.
* Evaluate the effectiveness of the platform in enhancing cybersecurity resilience among participating SMEs and organizations.
* Measure the impact of the platform on key performance indicators, such as reduction in cyber incidents, mitigation of vulnerabilities, and improvement in digital immunity.
* Collect qualitative feedback from users through surveys, interviews, and focus groups to assess platform usability, usefulness, and satisfaction.
* Analyze quantitative data on platform usage and cyber health metrics to identify trends and areas for improvement.
* Document lessons learned and best practices for future iterations of the platform and similar initiatives.

### Project Members

|  |  |
| --- | --- |
| **Student Name** | **Role** |
| **RADHIKA ORARI** | **SENIOR PROJECT LEAD** |
| **THARUN EMURI** | **JUNIOR LEAD** |
| **SADIA ANIKA MUMU** | **MEMBER** |
| **MANASVINI DUDDUKURU** | **MEMBER** |
| **MANONARAYANAN JANARDHAN BHAGAVATHI** | **MEMBER** |
| **KEERTHI PRIYA KUTUMBAKA** | **MEMBER** |
| **MISA MANOJBHAI AGHERA** | **MEMBER** |
| **ZACHARY ALEXANDER MCLENNAN** | **MEMBER** |
| **MITCHELL JOHN FERRIS** | **MEMBER** |
| **GAURANG BANSAL** | **MEMBER** |
| **AJITESH ARORA** | **MEMBER** |
| **KAYLA PRATT** | **DOCUMENTATION LEAD** |
| **SHREEYUT SHRESTHA** | **MEMBER** |

[Project Mid-trimester Progress](#_TOC_250043)

[Project Plan Updates](#_TOC_250042)

[Project Team Member Key Achievements](#_TOC_250041)

## Deakin CyberSafe VR (DCyberCafe)

### Overview

The Deakin CyberSafe VR (DCyberSafe) aims to revolutionize cybersecurity training for small businesses. Leveraging interactive virtual reality (VR) technology, the company seeks to bridge the gap between theoretical knowledge and practical application of cybersecurity measures among small business owners and employees.

Goals

Our goal is to develop an immersive VR platform that simulates real-world cybersecurity scenarios tailored for small businesses. Through this platform, we aim to enhance the practical understanding of cybersecurity principles among small businesses, focusing on fundamental topics such as password security, data encryption, network security, safe web browsing, and recognizing common cyber threats like phishing and SMiShing.

Objectives

As this is a new project, our initial objective is to brainstorm cybersecurity objectives and research how these can be effectively depicted in an immersive VR environment. We aim to create interactive VR modules covering essential cybersecurity topics, such as password security, data encryption, network security, safe web browsing, and recognizing common cyber threats like phishing and SMiShing. These modules will feature realistic scenarios tailored to the needs of small businesses, allowing users to actively engage with cybersecurity challenges. Additionally, we seek to build a functional MVP that demonstrates the core features of the DCyberSafe platform, while continuously testing and iterating on the VR modules to enhance their effectiveness for small businesses.

### Aims for the Trimester

* **Module Design/Development:** we aim to develop interactive VR modules focusing on essential cybersecurity topics. Topics for the Minimum Viable Product (MVP) may include password security, data encryption, network security, safe web browsing, and recognizing common cyberthreats such as SMiShing and phishing.
* **User Engagement:** we aim to implement strategies to enhance user engagement with the VR platform. This could include incorporating gamification elements, interactive quizzes, or progress tracking features to encourage active participation and learning.
* **Unity Familiarization:** we aim to familiarize ourselves with the Unity platform, to educate ourselves on how the module designs can be implemented in a VR environment.
* **Prototype Testing:** we aim to conduct thorough testing of the MVP to evaluate its functionality and effectiveness.
* **Scalability Planning:** we aim to begin laying the groundwork for future scalability, including more advanced use of VR components.

### Trimester Deliverables

* **VR Modules**: a document will be delivered detailing potential modules for the VR program. This document may include story boards, showing the visual representation of the modules. It may also include learning objectives, relevant to each specific topic.
* **MVP:** we will deliver a minimum viable product. This will be used to validate the product concept with the minimum set of features required to gather feedback and learn from real-world usage.
* **MVP Delivery Report:** including an executive summary, introduction to the product, MVP features, development and testing process, performance evaluation, lessons learned, and future steps.
* **Scalability Plan Outline**: we will present an outline of the scalability plan for the DCyberSafe platform, detailing infrastructure requirements, scalability options, and potential partnerships for future growth.

# Long-Term Deliverables (Future Trimesters)

* **Fully Developed VR Platform:** Deliver a fully developed and robust VR platform for cybersecurity training, tailored specifically for small businesses.
* **Comprehensive Curriculum:** Develop a range of interactive VR modules covering a wide range of cybersecurity topics, including advanced techniques and emerging threats.
* **Continuous Content Updates:** Commit to providing regular updates and additions to the VR modules to ensure that the content remains current and relevant with the current cybersecurity landscape.
* **Partnerships and Collaborations:** Forge strategic partnerships with other capstone projects, to expand the reach and impact of the platform.
* **Analytics and Reporting:** Implement analytic and reporting capabilities to track user progress, identify areas for improvement, and measure the effectiveness of the modules.
* **Module Success:** Evaluate the effectiveness of the VR modules through KPI’s, such as a reduction in cyber incidents related to human weakness.

### Project Members

|  |  |
| --- | --- |
| **Student Name** | **Role** |
| **Diana Danilovic** | **Senior Project Co-Lead** |
| **Brittany Patterson** | **Junior Project Co-Lead** |
| **Zara Rose Scherger** | **Senior Team Member** |
| **Matthew Jorge Pinazo** | **Senior Team Member** |
| **Vitthal Satija** | **Senior Team Member** |
| **Joshua Manfre** | **Junior Team Member** |
| **Ben Telfer** | **Junior Team Member** |

[Project Mid-trimester Progress](#_TOC_250043)

[Project Plan Updates](#_TOC_250042)

[Project Team Member Key Achievements](#_TOC_250041)