



Cardiff University

School of Computer Science and Informatics

CM3203 - Individual Project Initial Plan

Cyber Security Online Education Portal

Supervisor: Dr Yulia Cherdantseva

Author: Alexander Jones

Date of Submission 07/02/2022

Initial plan – Cyber Security Education Online Portal

1.1 Project Description

The importance of cyber security is increasing day by day, as new technology is developed, new vulnerabilities are also introduced. It is vital that all age groups become cyber aware in order to prevent them from being the victim of a cyber-attack. This project aims to provide a centralised form of cyber security educational content, ranging from content suitable for primary school level and above. In the last few years, cybercrime is up over 600% [1] however, education on cyber security has not scaled accordingly. Providing a wide range of educational material varying in complexity allows this project to be applicable to a wider variety of people. Phishing is the most common cybercrime [3], and this relies on the victim to be less cyber aware. Phishing involves sending a malicious link or a message to a victim designed to trick them into revealing sensitive information (banking information, passwords etc). This situation could be avoided if the victim was more cyber aware, they would be able to identify the primary attributes that reveal it is a phishing scam and avoid being a victim of a scam. Additionally, while it is important to educate the general public to avoid cyber-attacks, it is also important to provide more complex material to those interested in pursuing a career in cyber security. The UK is in dire need for more cyber security experts, 64% of cyber firms have faced problems with technical cyber security skill gaps among staff [2]. This project aims to provide a platform to supplement material taught throughout the education system, while also being accessible by those not in education. The objective of this is to allow the material to be as accessible as possible, as a result, more people are exposed to the educational material and the cybersecurity skill shortage could be reduced. Material uploaded onto the site can range from PowerPoints, links to videos and lab manuals. Access permissions for different roles mean that content uploaded to the site can be moderated to ensure that all material is relevant to the subject of cybersecurity.

2.1 Project Aims:

- Supplement material taught throughout the education system
- Provide a centralised form of cyber security educational content for all ages and proficiency levels
- User-friendly UI
- Access permissions vary based on role

2.2 Objectives:

- Research literature and other services to determine the requirements
- Develop a risk assessment
 - o A risk assessment is designed to mitigate any potential risks I may face when developing the project.
- Use the requirements and use cases to determine the schema of the database
 - o The requirements and use cases allow me to construct a UML class diagram which will aid in the development of the database. The use cases will allow me to identify which queries will be executed the most, from this information I will be able to optimise the database for these queries.

- Use common design patterns to create wireframes of the UI
 - By looking at other software applications, I will be able to take inspiration from the design elements and incorporate them into my own UI designs. Figma will be used to create prototype's varying in fidelity. The UI is subject to change as development progresses, this is part of the agile methodology.
- Use the Vaadin java web framework in conjunction with java and CSS to create the back-end functionality of the web application
 - Vaadin is a web framework for java that enables web applications to be developed in java without the need for HTML.
- Create a minimum viable project before the 15th of March 2022
 - A minimum viable project plays a key role in the agile development methodology, it is a product with the minimum amount of features to address the proposed problem. As the cycle progresses, more and more features are added to the prototype.
- Have a fully working and bug free application by the 12th April 2022
- Evaluate the prototype
 - The prototype will be evaluated using a mixture of white box and black box test cases.
 - These test cases will have primary flows and alternate flows, any test cases that fail will result in more development of the prototype in order to fix any problems.
- Conclusion
 - The project will be concluded in the primary report, covering;
 - Limitations
 - Future work
 - Reflection on learning
- Review meetings
 - Review meetings with the supervisor will take place on the 3rd of March and 19th of April
 - I chose these dates as the first review meeting would occur at the beginning of the implementation, whereas the second would occur after I had the minimum viable product

3.1 Work plan

Week 1 (31st January – 5th February)

- Complete initial plan by February 5th
- Research how to implement log in/registration system using Java
- Milestones/deliverables
 - Initial plan complete and submitted

Week 2 (7th February – 13th February)

- Introduction

- Set the scene for the project
- Explain key concepts relevant to the project
- Project motivation
- Project scope
- Literature review
 - Begin the literature review by reviewing relevant software and literature
 - This will likely continue throughout the implementation of the prototype
- Milestones/deliverables
 - Introduction in final report complete

Week 3 (14th February – 20th February)

- Define functional requirements
 - These will include tasks that the prototype will allow the user to do
- Define non-functional requirements
 - These will define system attributes such as security, usability and scalability
- UI wireframes
 - These will include an initial sketch of the UI as well as a low to mid fidelity prototype. Both will be developed using figma.
- UML diagram construction
- Risk assessment construction
- Database beginning development
- Milestones/deliverables
 - UI mock-ups complete
 - Functional and non-functional requirements complete
 - UML diagram complete
 - Risk assessment finished

Week 4 (21st February – 27th February)

- Continue database development
- Develop login/registration page
- Begin implementation of main page view
- Milestones/deliverables
 - Database complete
 - Login/registration page complete

Week 5 (28th February – 6th March)

- Continue the implementation of main page view
- **Review meeting with supervisor (3rd March)**

Week 6 (7th March – 13th March)

- Finish implementation of main page view
- Implement resource selection view
- Implement resource display view
- Milestones/deliverables
 - Main page view
 - Resource selection view

- Resource display view

Week 7 (14th March – 20th March)

- Implement log out functionality
- Implement task bar
- Begin development of admin page view
- Milestones/deliverables
 - Minimum Viable Product

Week 8 (21st March – 27th March)

- Complete implementation of admin view
- Start implementing ability to favourite resources
 - This is an optional requirement
- Milestones/deliverables
 - Admin view complete

Week 9 (28th March – 3rd April)

- Implement ability to favourite resources
- Implement ability for admins to manage accounts
- Milestones/deliverables
 - Ability to favourite resources complete
 - Ability for admins to manage accounts complete

Week 10 (4th April – 10th April)

- Implement ability to create documents
 - Optional requirement
- Milestones/deliverables
 - Application complete

Week 11 (11th April – 17th April)

- Fix any bugs present in the application
- Write up the implementation in the final report
- Milestones/deliverables
 - Implementation complete

Week 12 (18th April – 24th April)

- Evaluation
 - Create test cases
 - Carry out test cases
 - Fix failed test cases
- Review meeting with supervisor (19th April)
- Milestones/deliverables
 - Evaluation complete

Week 13 (25th April – 1st May)

- Conclusion

- Project summary
- Limitations

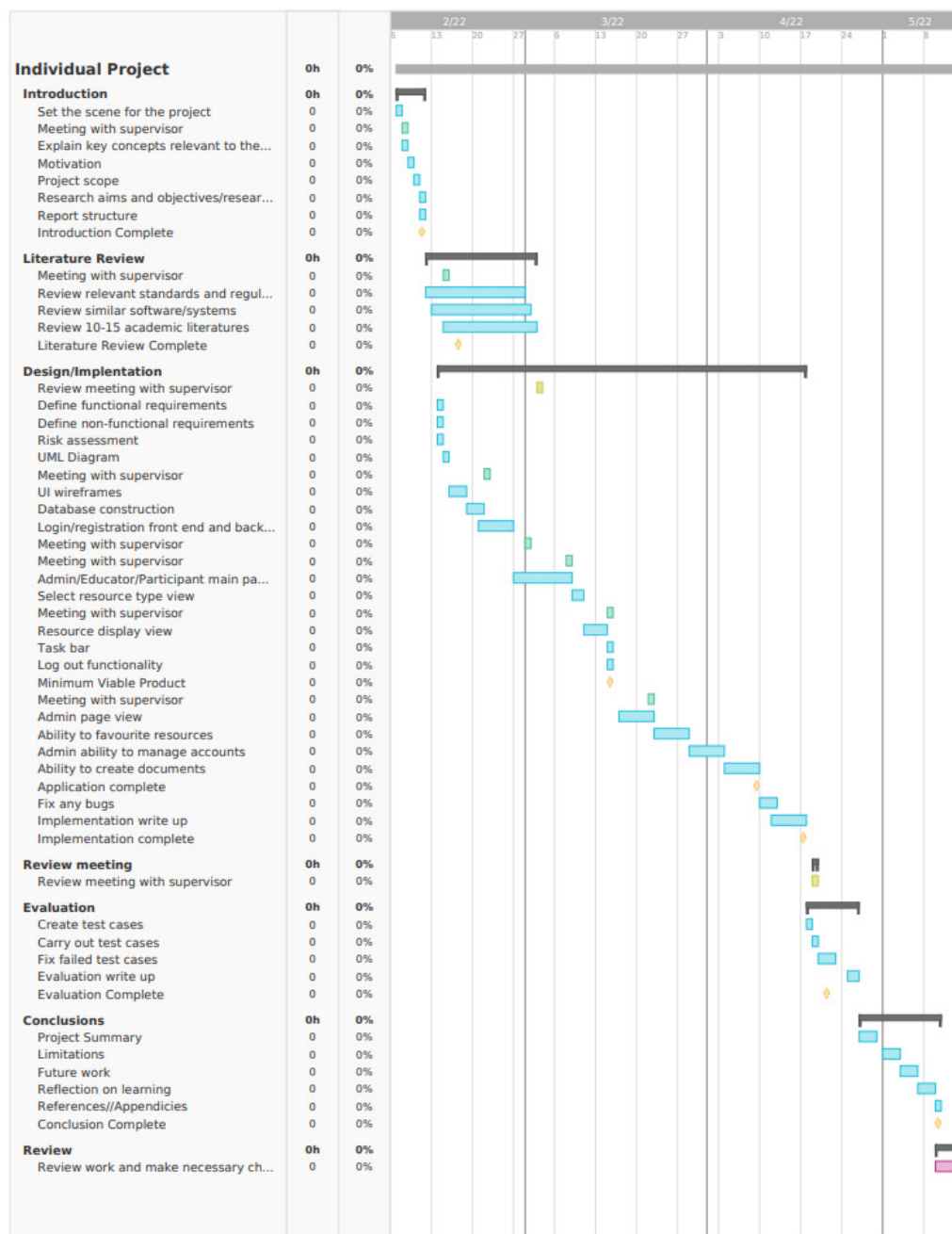
Week 14 (2nd May – 8th May)

- Conclusion
 - Future work
 - Reflection on learning

Week 15 (9th May – 13th May)

- Review work and make necessary changes
- References
- Appendices
- Milestones/deliverables
 - Project complete
 - Final report complete
 - Submitted

3.2 Gantt Chart



4.1 References:

- [1] PurpleSec. 2022. 2021 Cyber Security Statistics Trends & Data. [online] Available at: <<https://purplesec.us/resources/cyber-security-statistics/>> [Accessed 2 February 2022].
- [2] GOV.UK. 2022. Cyber security skills in the UK labour market 2020. [online] Available at: <<https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020>> [Accessed 2 February 2022]
- [3] Poza, D., 2022. The 7 Most Common Types of Cybersecurity Attacks in 2021. [online] Auth0 - Blog. Available at: <<https://auth0.com/blog/the-7-most-common-types-of-cybersecurity-attacks-in-2021/>> [Accessed 5 February 2022]