Snapshot 1.1, Week 4, of

Group AttackFlow4

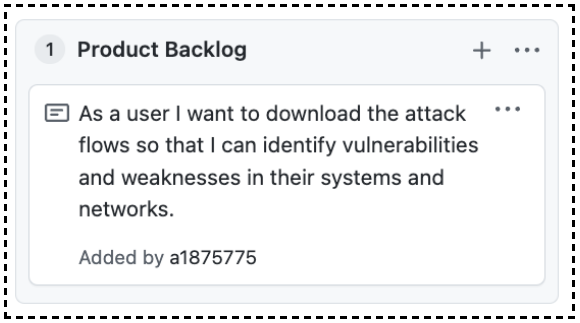
Building a dataset of real-world cyber-attacks with Attack Flow

Team members:

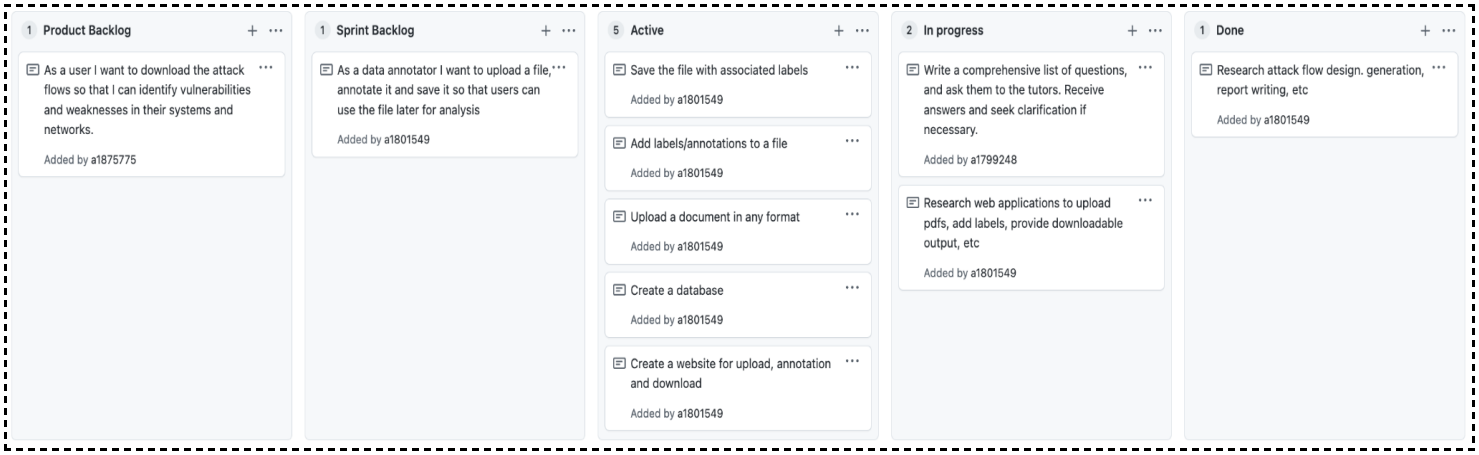
Nathaniel Chang | a1821595
Emily Miller | a1799248
An Nguyen | a1840557
Elana Parnis | a1831872
Ethan Pratt | a1828540
Angelos Sohan | a1825116
Wei Long Wan | a1801549
Jinyang Li | a1832744
Xizi Wang | a1824060

Product Backlog and Task Board

The product backlog:

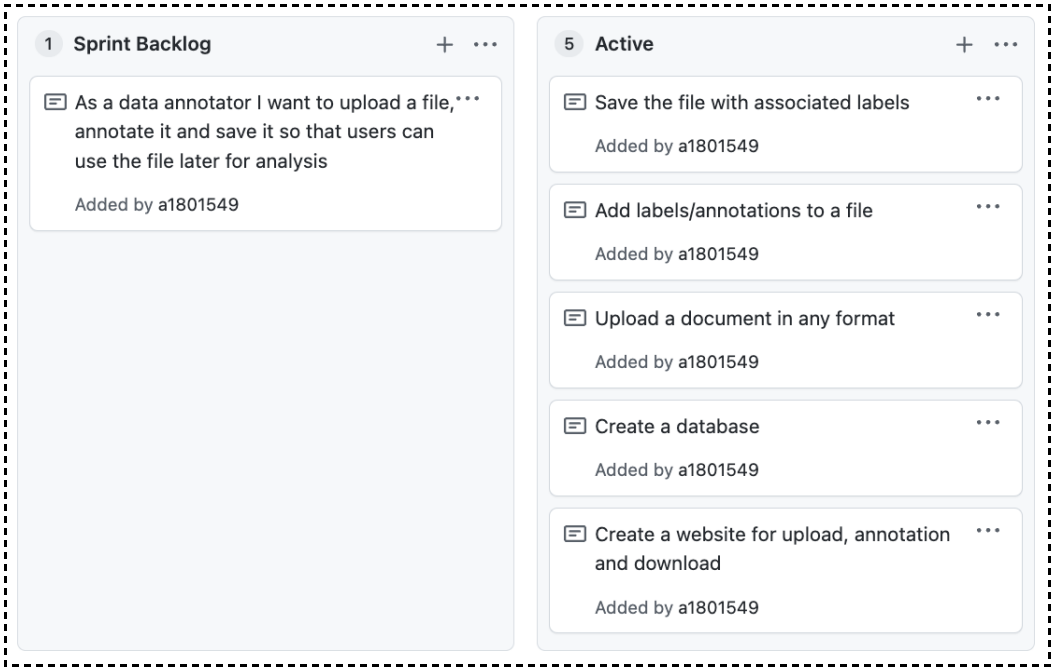


The task board:



Sprint Backlog and User Stories

The sprint backlog:



Description of the user stories selected for the current sprint:**

For the first sprint we have selected the user story;
"As a data annotator I want to upload a file, annotate it and save it so that users can use the file later for analysis"

This describes a user, 'data annotator' which requires the need to upload a data file (of various types), a need to annotate the file (using labels/ tags) and the ability to save the file along with its provided tags for later analysis (which will likely need to be searchable using file name and associated tags). The primary tasks selected from the user story are: the web platform required to access the software, file upload, annotation of files using tags (both predefined and user-defined) and storage of the file with tags in a database.

*** Note that due to delay in receiving information, progress was limited and this week was entirely theoretical in the work achieved. The user story below was unable to be worked on, but was discussed in theory as part of our design.*

Definition of Done

At the conclusion of this project, our application should be ready for deployment and actualisation. Throughout the project, the term "done" denotes the completion of a particular component. It is attained after a thorough review by both a team member and the featured client, has incorporated feedback, and undergone subsequent review. Additionally, a component achieves "done" status when it aligns with the client's brand guidelines, ensures a consistent and integrated visual identity, encapsulates technical proficiency, and adheres to design standards. A more specific definition of “done” for each of the predicted aspects is outlined below:

1. **Website Functionality:**
    - The website is fully functional, allowing users to upload files.
    - Annotations are automatically generated based on the uploaded file's content.
    - Users have the capability to manually add annotations to the file.
    - The website's user interface is responsive, intuitive, and accessible.
    - User reviews all annotations prior to saving data to the database
2. **Attack Flow Creation:**
    - An attack flow is generated accurately based on the report's content.
    - The attack flow represents the sequence of events and vulnerabilities identified in the report.
    - The attackflow generator already built by the client will be used to produce attack flows based on the annotations extracted.
3. **Database Integration:**
    - The annotated report is inserted into the database after manual annotation.
    - Data integrity is ensured during the database insertion process.
4. **Report Download:**
    - Users can successfully download the annotated report from the website.
    - The downloaded report includes all annotations and attack flow visualisations.
5. **Testing and Quality Assurance:**
    - The website functionalities are thoroughly tested to ensure proper behaviour.
    - Any bugs, errors, or inconsistencies are resolved before considering the user story "done."
6. **Documentation:**
    - Comprehensive documentation is provided, including user instructions and technical details.
    - The documentation assists users in understanding how to utilise the website's features effectively.

Summary of Changes

As this is the initial snapshot, there are no changes to summarise. Therefore, its purpose is to mark the foundation of this project, and be a reference point for future developments where alterations may have occurred.