Snapshot 2.1, Week 5, of

Group AttackFlow4

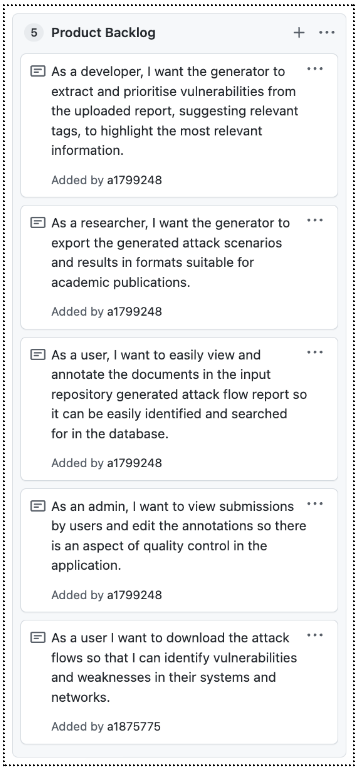
Building a dataset of real-world cyber-attacks with Attack Flow

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:



5 Product Backlog

As a developer, I want the generator to extract and prioritise vulnerabilities from the uploaded report, suggesting relevant tags, to highlight the most relevant information.

Added by a1799248

As a researcher, I want the generator to export the generated attack scenarios and results in formats suitable for academic publications.

Added by a1799248

As a user, I want to easily view and annotate the documents in the input repository generated attack flow report so it can be easily identified and searched for in the database.

Added by a1799248

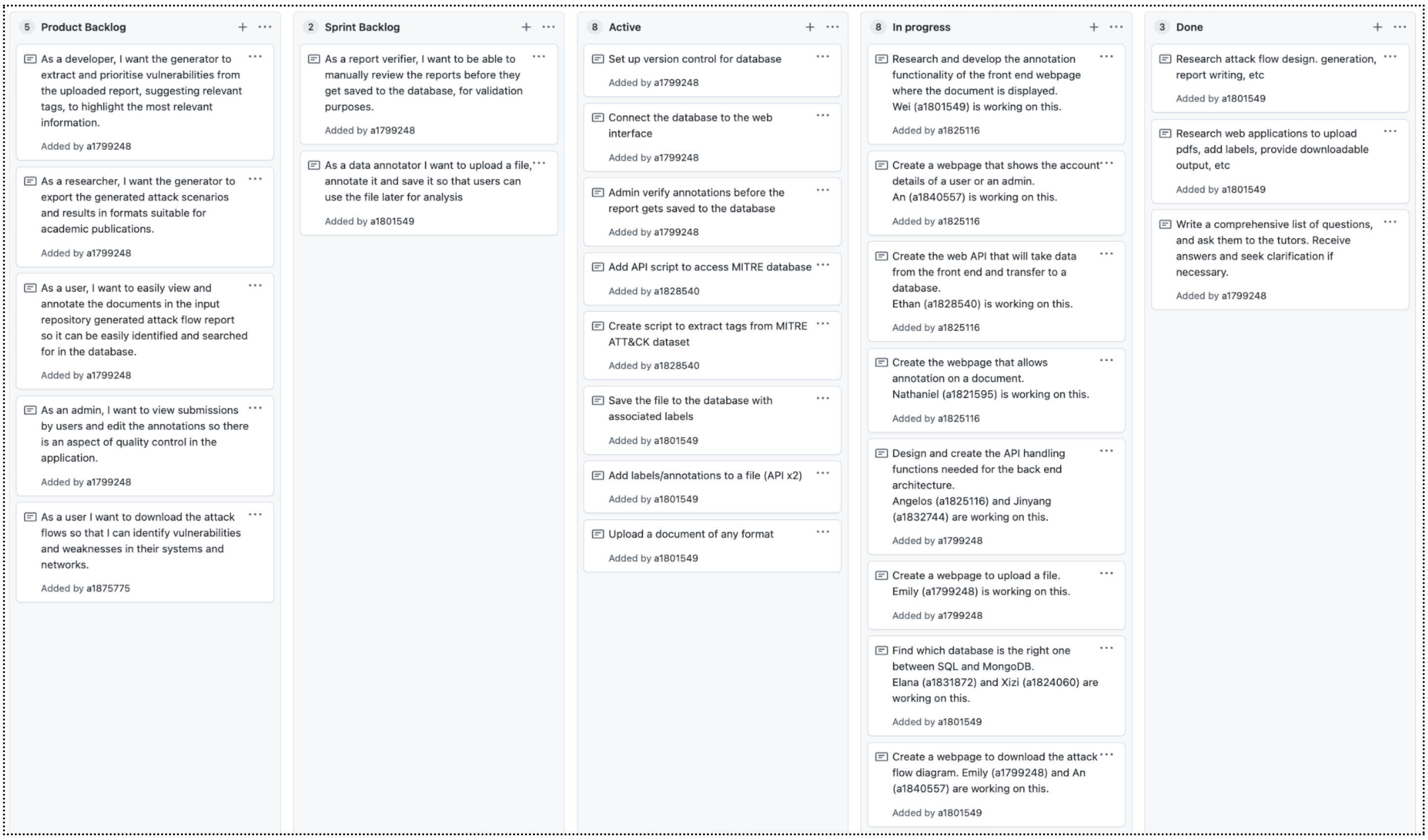
As an admin, I want to view submissions by users and edit the annotations so there is an aspect of quality control in the application.

Added by a1799248

As a user I want to download the attack flows so that I can identify vulnerabilities and weaknesses in their systems and networks.

Added by a1875775

The task board:



5 Product Backlog

As a developer, I want the generator to extract and prioritise vulnerabilities from the uploaded report, suggesting relevant tags, to highlight the most relevant information.

Added by a1799248

As a researcher, I want the generator to export the generated attack scenarios and results in formats suitable for academic publications.

Added by a1799248

As a user, I want to easily view and annotate the documents in the input repository generated attack flow report so it can be easily identified and searched for in the database.

Added by a1799248

As an admin, I want to view submissions by users and edit the annotations so there is an aspect of quality control in the application.

Added by a1799248

As a user I want to download the attack flows so that I can identify vulnerabilities and weaknesses in their systems and networks.

Added by a1875775

2 Sprint Backlog

As a report verifier, I want to be able to manually review the reports before they get saved to the database, for validation purposes.

Added by a1799248

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

Added by a1801549

8 Active

Set up version control for database

Added by a1799248

Connect the database to the web interface

Added by a1799248

Admin verify annotations before the report gets saved to the database

Added by a1799248

Add API script to access MITRE database

Added by a1828540

Create script to extract tags from MITRE ATT&CK dataset

Added by a1828540

Save the file to the database with associated labels

Added by a1801549

Add labels/annotations to a file (API x2)

Added by a1801549

Upload a document of any format

Added by a1801549

8 In progress

Research and develop the annotation functionality of the front end webpage where the document is displayed.
Wei (a1801549) is working on this.

Added by a1825116

Create a webpage that shows the account details of a user or an admin.
An (a1840557) is working on this.

Added by a1825116

Create the web API that will take data from the front end and transfer to a database.
Ethan (a1828540) is working on this.

Added by a1825116

Create the webpage that allows annotation on a document.
Nathaniel (a1821595) is working on this.

Added by a1825116

Design and create the API handling functions needed for the back end architecture.
Angelos (a1825116) and Jinyang (a1832744) are working on this.

Added by a1799248

Create a webpage to upload a file.
Emily (a1799248) is working on this.

Added by a1799248

Find which database is the right one between SQL and MongoDB.
Elana (a1831872) and Xizi (a1824060) are working on this.

Added by a1801549

Create a webpage to download the attack flow diagram. Emily (a1799248) and An (a1840557) are working on this.

Added by a1801549

3 Done

Research attack flow design. generation, report writing, etc

Added by a1801549

Research web applications to upload pdfs, add labels, provide downloadable output, etc

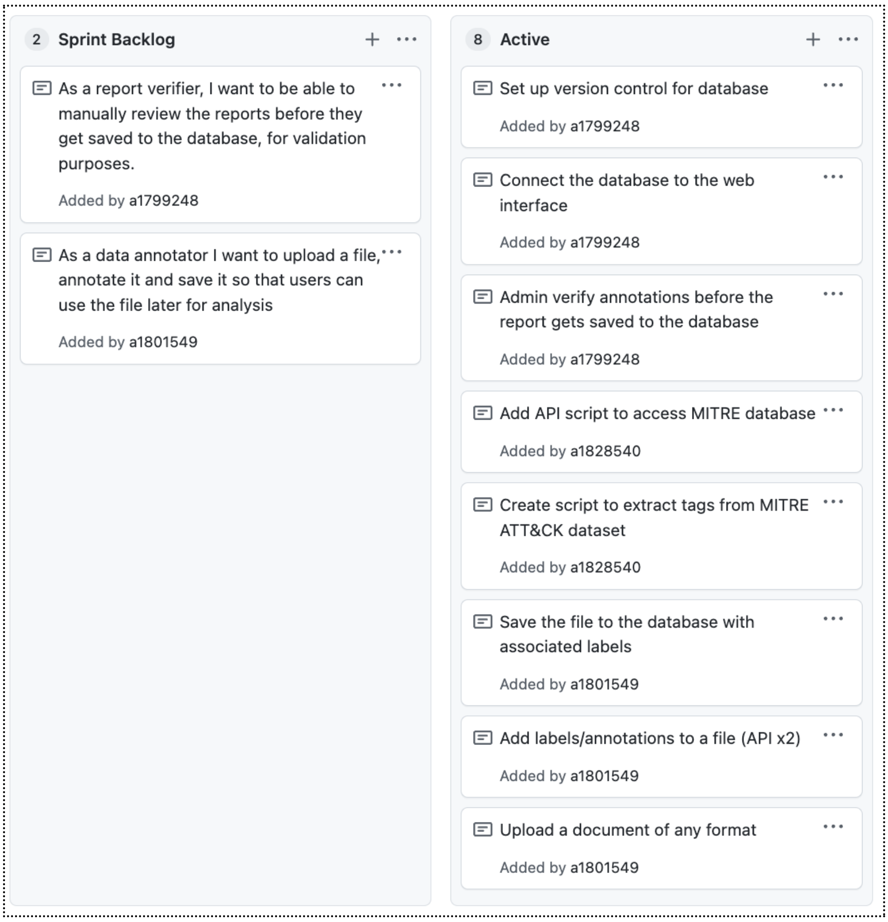
Added by a1801549

Write a comprehensive list of questions, and ask them to the tutors. Receive answers and seek clarification if necessary.

Added by a1799248

Sprint Backlog and User Stories

The sprint backlog:



2 Sprint Backlog

As a report verifier, I want to be able to manually review the reports before they get saved to the database, for validation purposes.

Added by a1799248

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

Added by a1801549

8 Active

Set up version control for database

Added by a1799248

Connect the database to the web interface

Added by a1799248

Admin verify annotations before the report gets saved to the database

Added by a1799248

Add API script to access MITRE database

Added by a1828540

Create script to extract tags from MITRE ATT&CK dataset

Added by a1828540

Save the file to the database with associated labels

Added by a1801549

Add labels/annotations to a file (API x2)

Added by a1801549

Upload a document of any format

Added by a1801549

Description of the user stories selected for the current sprint:

"As a report verifier, I want to be able to manually review the reports before they get saved to the database, for validation purposes."

As a 'report verifier', the user needs to manually review reports uploaded by other users before they are permanently stored in the database. It requires the ability to receive uploaded documents, see all the annotations on the report (whether they were made by the AI or the user who uploaded it), add their own annotations if desired, and then approve the upload of the document to the database. The primary tasks selected from the user story are: display the file upload, annotation of files using tags, and storage of the file with tags in a database.

The primary objective is to ensure the accuracy, completeness, and adherence to specific standards within these reports. The user seeks a feature that empowers them to meticulously inspect the content, data entries, calculations, formatting, and any potential errors or inconsistencies. Importantly, this manual review process must take place before the reports are saved to the database. The user's diligence in reviewing the reports serves as a crucial validation step, guaranteeing the reliability and trustworthiness of the information stored. This user story underscores the user's responsibility in maintaining the quality and integrity of the reports, ensuring that only accurate and error-free data becomes part of the official database records.

“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 supp-database.

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

Given a much deeper understanding of the project and the tasks it requires, we were able to significantly update our taskboard, including many more user stories added to the product backlog. For this specific sprint, another user story was added to the sprint backlog, was broken down into tasks, and moved into active or in-progress as appropriate.
It has not been required to update our definition of done.