

Snapshot Week 7 of Group AttackFlow1

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

Se Jin Yoon: a1706219
Ting-Wei Chin: a1782423
Faisal Hawsawi: a1822781
Lina Nehme: a1802697
Ran Qi: a1675122
Joseph Toubia: a1753547
Zemin Wong: a1780385
Jixing Ye: a1798631
Yu Zheng: a1739446

September 17, 2023

Product Backlog

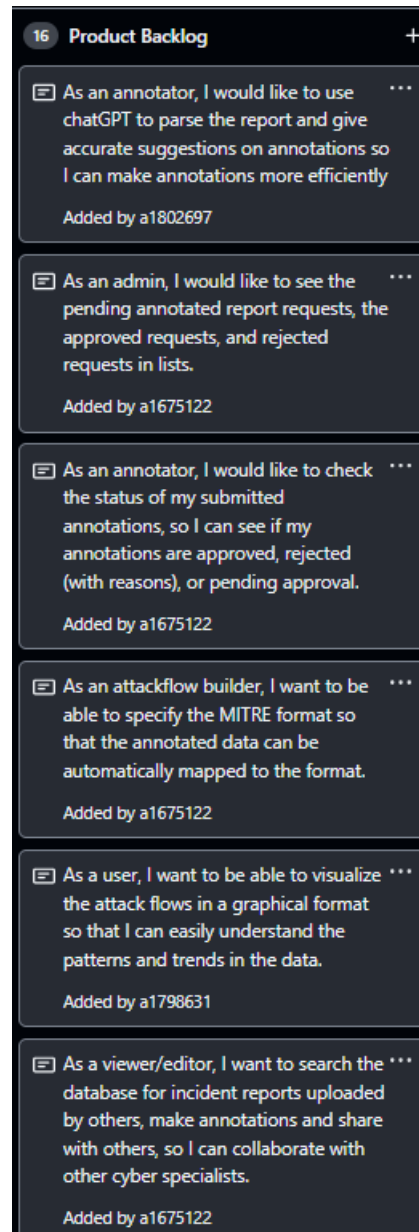


Figure 1: Product Backlog (Sprint 3) 1 of 3

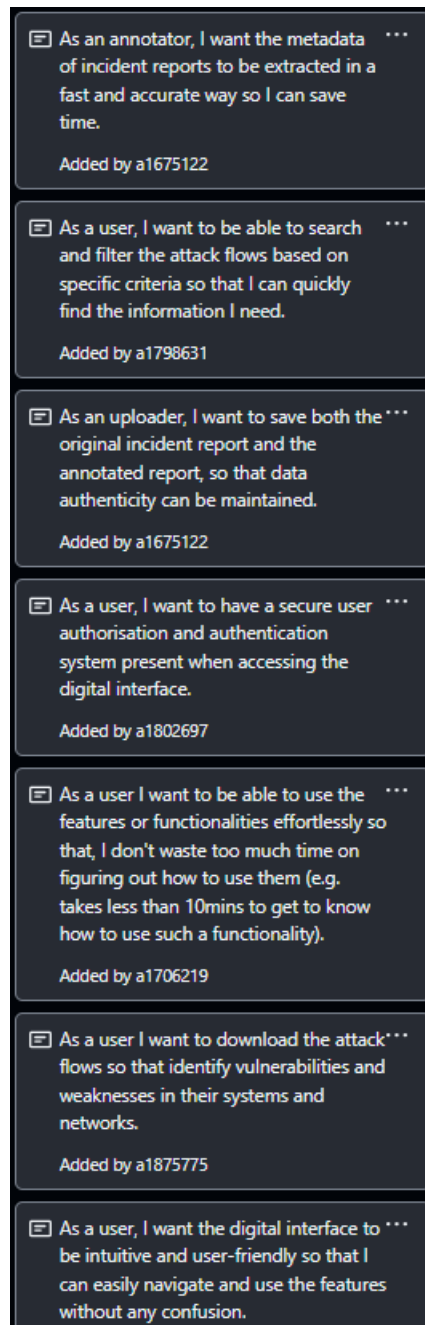


Figure 2: Product Backlog (Sprint 3) 2 of 3

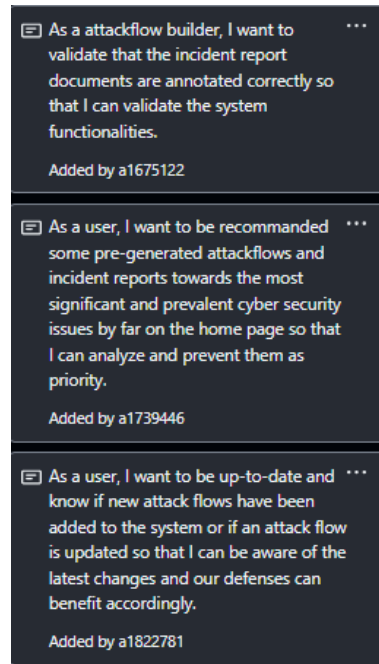


Figure 3: Product Backlog (Sprint 3) 3 of 3

Task Board

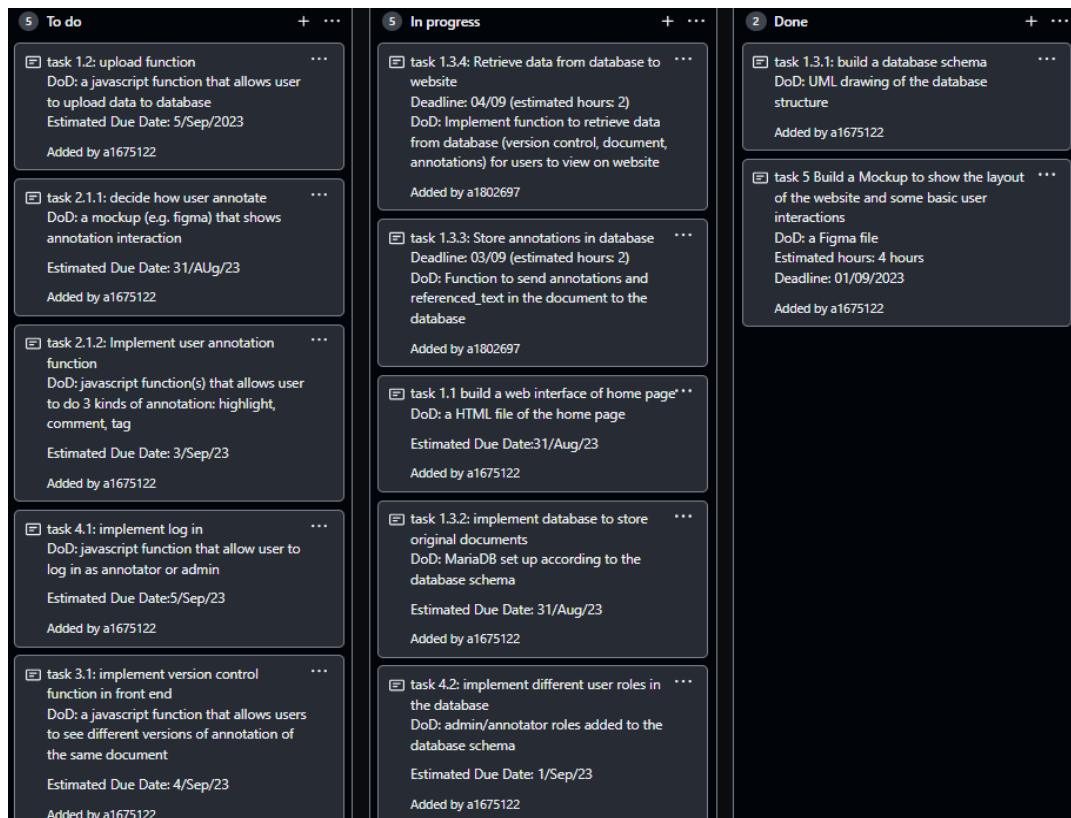


Figure 4: Task board (Sprint 3)

Sprint Backlog

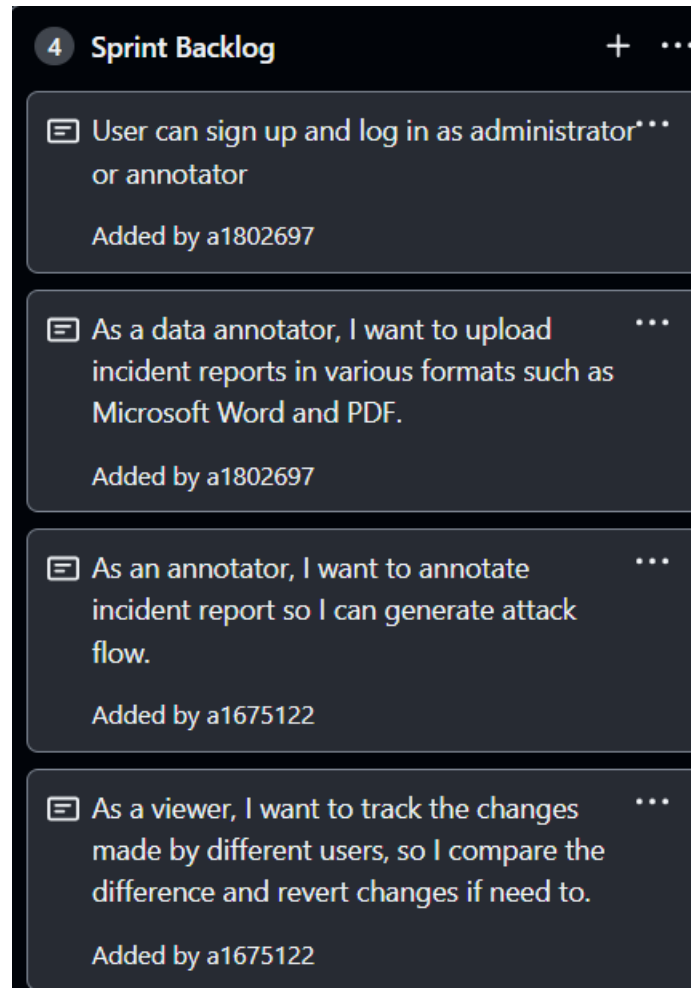


Figure 5: Sprint Backlog (Sprint 3)

User Stories

We have identified that some user stories like upload and annotate selected from the product backlog for sprint 2 remain incomplete due to underestimating the time complexity needed to complete the tasks. Therefore, we have selected the user stories document upload and annotate, as well as user sign ups and logins for this sprint. From this, we have determined the following tasks for sprint 3:

- “As a data annotator, I want to upload an incident report and save it so that I can further edit the file.”
 - Related tasks:
 - task 1.2: upload function
 - task 1.3.2: implement database to store original documents
- “As an annotator, I want to annotate incident report so I can generate attack flow.”
 - Related tasks:
 - task 2.1.1: decide how user annotate
 - task 2.1.2: implement user annotation function
 - task 2.1.3: integrate ChatGPT to parse report and give accurate annotation suggestions
- “User can sign up and log in as administrator or annotator”
 - Related tasks:
 - task 4.1: implement sign up
 - task 4.2: implement log in
 - task 4.3: implement different user roles in the database

Definition of Done

The individual DoD of each task can be seen on the screenshot of the task board.
In summary, the goals are:

- Testing the integrated backend functions works as we expected.
- Code is well-documented and adheres to our coding standards.
- Explain and ensure that all the scrum members understand the specifics of the tasks and how to construct the implementation.

Summary of Changes

The last snapshot focused on the functional requirements upload and annotate. While this snapshot will continue to focus on upload and annotate, we will also emphasise the functional requirements of user sign ups and logins. Some additional aspects that have changed since our last snapshot are:

- **Added new user stories-** During our meeting with the tutor we discovered new user stories. The first user story involves enabling annotators to check the status of their submitted annotation which can be either approved, rejected (with reasons) or pending approval. We also discovered a second user story regarding admins being able to see the pending annotated report requests, the approved requests, and rejected requests in lists. Lastly, we have clarified that ChatGPT will be integrated to parse the report and give suggestions to accurate annotations for the annotator to select. Thus, we have added a user story to reflect this requirement.
- **Refined our user stories to better align with the tutor's requirements.** We have updated our login user story to include both user logins and sign ups only for administrator and annotator after determining that end users from the general public do not need to make their own account to interact with the web application.
- **We have simplified our user story for uploading reports from the previous snapshot.** After discussions with our tutor, we determined that the functionality of saving incomplete annotated reports pre-submission for further edits was unnecessary. Therefore, we have updated our upload user story to exclude this functionality and enabled users to only upload, annotate and submit their reports without saving incomplete annotations during the annotation process.
- **This snapshot emphasises the major role of ChatGPT in parsing the report and providing accurate annotation suggestions.** We have integrated ChatGPT in our web application to give standard responses. Our next steps involve learning the mechanisms that enable ChatGPT to deliver consistent and accurate annotation suggestions including technique IDs and associated tags based on our inputs.