During the project we faced the following challenges:

* **No Direct Access to Official Documentation:** A major difficulty is the lack of direct access to ChatGPT’s official security policy. Depending on information from the internet might result in incomplete or outdated information. In order to address that, we chose and verified information from trustworthy sources. We gave preference to peer-reviewed articles, official statements, and recognized security platforms to ensure the dependability of the information collected.
* **Reliability of External Sources:** There’s a possibility that the information from the internet is not correct or does not reflect the current state of ChatGPT’s security practices. With that, we review the sources that we found on the internet to verify if it is credible.
* **Changing Nature of Security Policies:** Security policies can change, and the internet may not always show the most recent changes. This changing nature makes the review process more complicated. To address this problem, we evaluated ChatGPT’s security posture based on fundamental security principles, since we did not have specific policy details. This enabled us to examine general security practices and identify possible areas of improvement, even without detailed policy information.
* **Acknowledgment of Limitations:** Without direct access, it’s hard to comprehend the specific contexts and nuances of ChatGPT’s operations that might affect security decisions.
* **Prioritization of tasks:** Identify and prioritize tasks based on their importance and deadline. Since we have different subjects, we allocate time to our project for every task.