For the last two semesters I lead a team of engineers and worked with the Naval Education and Training Command (NETC) to create a DevSecOps ecosystem that allows the passing of digital documentation. Our goal was to utilize the automation tool known as Jenkins to define a pipeline that connects to an input source, extracts the metadata from files, and deploys them to an artifact repository. The pipeline handles the passing of four main file types: Word Documents, PDFs, PowerPoints, and Excel files. It works by using GitHub as the input hub, here a user can upload any type of file to a specified folder. When the pipeline is built, it will clone the repository and will gain access to the files in its directory. For the functionality, we used a jar file that runs within the pipeline and extracts the metadata then writes the information to a JSON file. Then all the files are deployed to JFrog artifactory to be housed securely and allow easy access for the user to overlook them. Lastly, there are post build actions that send out an email to inform the user of the build's status and provide a copy of the build log.

Our project will directly impact the NETC since they are responsible for the distribution of various documents throughout the Navy and prospective cadets. Their main line of communication to their cohorts is through these files, whether physical or digital, so it is important that the information inside is accurate. This pipeline will provide them with a platform to upload files and validate them without needing to check them individually. The scope of our project created the initial ecosystem where future groups will be able to build on top of what we accomplished. This will include creating security functionalities that check URLs, grammar, spelling, etc. As this organization deals with national defense, these security issues in documents can cause damaging misunderstandings, so it is imperative that they are verified. For our project, we had to consider the teams that would continue the effort. Applying these morals meant making sure that everything we did was recyclable and maintainable. This is why we decided to make a plugin that mirrors the Jar we are currently using. This is because the plugin will allow future groups to update it to their needs, while a Jar file is not as flexible.

Overall, our group finished everything we set out to complete for the NETC and they will now be able to pursue new functionalities to further develop the security aspect of the pipeline. It is exciting to know that what we did will help the United States Navy in their pursuit to train and recruit members to their organization. Working on this project was a huge challenge for me since I had no experience with DevSecOps, CI/CD pipelines, Java, or plugin implementation. Everything I encountered was a learning curve and required time, effort, and research to understand. Through this, however, I learned how to write pipeline scripts, the set of rules the pipeline follows, in Groovy. As well as using Java to create the Power Point metadata extractor class and a URL checker Method for each file type. Along with the technical portion of the project, I faced many hurdles being the leader of the group. It was difficult for me to manage everything, but I overcame these obstacles by constantly communicating with my team and delegating tasks efficiently. It took me a bit to get it right, but now I can see the fruits of our labor and am proud of what we accomplished.