ReporEE/CprE/SE 491 WEEKLY REPORT 5

10/10/24 - 10/17/24

Group number: sdmay25-07

Project title: Ask Captain Cyber

Client &/Advisor: Doug Jacobson

Team Members/Role:

- ***Ethan Comiskey - Cybersecurity Implementation Principal Manager***
- ***Steven Ragan - Cybersecurity Coordinator & Integration Associate***
- ***Alex Elsner - Lead backend developer***
- ***Casper Run - Cybersecurity and WordPress developer***
- ***Alexander Kronau - Backend developer. Limited Frontend***
- ***Caden Murphy - Frontend developer***

Weekly Summary

The primary goal of this week was for group members to become more familiar with the specific tools we will be utilizing to create our project. Many of the group members worked to gain knowledge regarding Wordpress, some worked on researching best coding practices, AI, etc. Our secondary objective, which will become our primary objective this upcoming week, was to begin the process of laying out the plan for building Ask Captain Cyber. This is the foundational building block that all of our work up to this point has been leading up to, where we will now begin the process of prototyping Ask Captain Cyber and determine what works and what needs to change.

Past week accomplishments

- Ethan Comiskey - Researched how AI could potentially be integrated into the system we have currently been granted access to.
- Steven Ragan - Looked into what coding practices will best suit WordPress and upkeep. Then started looking at WordPress plugin creation and testing.
- Alex Elsner - Finalized wordpress backend plugins and security that will be needed for the backend, along with secure AI integration.
- Casper Run - Researched how the WordPress databases works and the AI plugin WPBot that has good potential. WPBot is a plugin that integrates OpenAI's GPT models.
- Alexander Kronau - Gained a deeper understanding of how generative AI models can be manipulated to provide outputs that violate usage policies. Check Azure OpenAI service "Limited access" requirements.
- Caden Murphy - Compiled list of React Libraries that can be used with WordPress, WP Rest API is developed by WordPress and is arguably the best option. Allows for a React frontend to talk to WordPress backend.
    - WP Rest API - https://developer.wordpress.com/docs/api/

Individual contributions

NAME	**Individual Contributions** *(Quick list of contributions. This should be short.)*	**Hours this week**	**HOURS cumulative**
Ethan Comiskey	Researched how AI could potentially be integrated into the given system	6	32
Steven Ragan	Coding practices WordPress experience	6	32
Alex Elsner	Wordpress security plugins finalized Research creating our own Data set	6	32
Casper Run	WordPress Database and AI Plugin Research	6	32
Alexander Kronau	Explained methods of how generative AIs can be maliciously manipulated - initial prompt eng at startup required.	6	32
Caden Murphy	Found WordPress React Library suitable for project, WP Rest API	6	32

Plans for the upcoming week

- Ethan Comiskey - Work to create a timeline for our project and develop steps for beginning our project implementation
- Steven Ragan - Look into available data sets / web scrapers we can use to generate responses.
- Alex Elsner - Look into methods to create our own LLM data set from trusted sources and research more wordpress backend plugins to use.
- Casper Run - I didn't get the chance to work with Alex on backend database and security functionality, so we plan to make it a focus this upcoming weekend and for next week.
- Alexander Kronau - Curate a detailed AI initialization prompt that will ensure captain cyber will stay on topic and become harder to manipulate.
- Caden Murphy - Work with group to finalize ideal dates/goals to shoot for. Begin frontend development while backend is getting set up as well.

Summary of weekly advisor meeting (*If applicable/optional)*

We are in contact with our advisor regarding access to the tools needed to complete our assigned project. Other than that, we have all agreed upon monthly meetings with our advisor.

- Did not this week