EE/CprE/SE 492 STATUS REPORT 3

Feb 14 - Feb 27

Group number: sdmay25-07

Project Title: Ask Captain Cyber

Client / Advisor: Doug Jacobson

Team Members/Role:

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

Weekly Summary

These past two weeks, we spent time formally assigning goals and tasks and going into full development mode. Unfortunately, we ran into some issues getting a meeting scheduled with a TA for a progress check-in due to our busy schedules, but we overcame that and met with Mohammed Zakariah at 11:00 am this past Monday. Mohammed was confident in our current knowledge and implementation plan. Alex E. and Casper have started developing the backend and have performed the initial setup of the FlaskAPI and MySQL database required to send the OpenAI information and store it respectively. Steven and Ethan have started prompt engineering an OpenAI chatbot and are building a question bank that we can pre-seed the eventual Captain Cyber AI. Caden and Alex K. have familiarized themselves with PHP and are beginning to pivot the front end from React to PHP. Overall, it has been a successful couple of weeks, and it was important that we start to get into a development mindset.

Past week's accomplishments

- Ethan Comiskey - Drafted and tested numerous prompts for the AI assistant. Updated the prompt incrementally to meet more requirements for how Ask Captain Cyber should respond to users.
- Steven Ragan - performed border testing on prompt and returns via open AI and looked into the SQL database on the server.
- Alex Elsner - Set up SQL database and planned out how to organize tables for efficient querying. Started to write a basic script that we will use to fill the database with 100

questions. Worked with Casper to start testing connectivity between FlaskAPI and mySQL database.
- Casper Run - Gained access to the new API server that our advisor set up last week with ETG. Installed Flask and FlaskRest API. Tested some simple API code on a Python development environment
- Alexander Kronau - Discovered critical issue in React, will be switching to php.
- Caden Murphy - Had to pivot from React frontend to building WordPress php frontend, familiarized myself with PHP, and began working with Alex K on developing a new frontend

Pending issues

-

Individual contributions

NAME	Individual Contributions	Hours this week	HOURS cumulative
Ethan Comiskey	Drafted and tested numerous prompts for the AI assistant. Updated the prompt incrementally to meet more requirements for how Ask Captain Cyber should respond to users.	6	18
Steven Ragan	Did some database research on keys and how to org the information. Some border prompt engineering.	6	18
Alex Elsner	Created SQL database and worked on creating tables. Did some basic testing for connecting FlaskAPI and mySQL database.	6	18
Casper Run	Gained access to the new API server. Started development of python-based FlaskReset API to connect the DB and OpenAI API.	6	18
Alexander Kronau	Figured out WP integration with PHP. Helped Caden with the environment. GPT Playground jailbreak attempt	6	18
Caden Murphy	New technology stack for frontend	6	18

Plans for the upcoming week

- Ethan Comiskey - Write numerous test cases to attempt to jailbreak the AI Assistant and test how effective the existing prompt is. Update the prompt as needed.
- Steven Ragan - Work on more prompts and test cases for prompts to verify the safety and security of the prompt.
- Alex Elsner - Work with Casper to connect FlaskAPI to mySQL database and potentially start doing basic queries. Start working on code for front end access to database information for ambassadors.
- Casper Run - Continue developing the Flask API and write code to connect to the OpenAI API and WP DB—research secure development practices for RestAPIs. Work with Alex E. to get database queries and requests working.
- Alexander Kronau - Learn the fundamentals of and practice development for PHP. Set up a PHP environment. Analyze what we have and what needs to be done.
- Caden Murphy - Begin implementing php solutions for the front end within WordPress.