EE/CprE/SE 492 STATUS REPORT 4

Feb 28 - March 13

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

Over the past two weeks, we have continued to develop and work on our respective parts of the project. Due to midterms progress has slowed, but we are still on track to complete all required aspects of the project on time. We met with our advisor, Doug Jacobson, on March 12th where we updated him on our progress and discussed project specifications. Our backend worked on writing a python program that inserts data into the WP database. The frontend worked on frontend features and discussed plugins that could be used for other features. The AI Assistant prompt development testing is effectively finished, some testing left to be done for border cases. Once spring break is over, we will be able to get right back on track and continue development in full force.

Past week's accomplishments

- Ethan Comiskey - Wrote numerous test cases to attempt to jailbreak the AI Assistant and test the prompt’s effectiveness. Prompt was updated accordingly and is now in its final draft
- Steven Ragan - performed border testing on prompt and returns via open AI and looked into the SQL database on the server.
- Alex Elsner - Worked with Casper to write a Python program that inserts data into the WP data base, along with setting up correct database permissions and tables.
- Casper Run - Worked with Alex to write a Python program that inserts data into the WP database. Wrote programs to test connections with OpenAI API.
- Alexander Kronau - Helped fix local install, learned more about php (no prior

experience), sorting through existing codebase to determine integration.
- Caden Murphy - Worked with Alex K to split front end features. Talked with Doug about what WordPress plugins could potentially be used for frontend and got contact for Cyber House Rock developer to ask questions in regards to implementation.

Individual contributions

NAME	Individual Contributions	Hours this week	HOURS cumulative
Ethan Comiskey	Ethan Comiskey - Wrote numerous test cases to attempt to jailbreak the AI Assistant and test the prompt's effectiveness. Prompt was updated accordingly and is now in its final draft	6	24
Steven Ragan	performed border testing on prompt and returns via open AI and looked into the SQL database on the server.	6	24
Alex Elsner	Worked with Casper to develop a python script that inserts and queries information into the WP DB. Set up correct database rules and tables.	6	24
Casper Run	Worked with Alex Elsner to develop a Python Script that inserts information into the WP DB. Wrote and tested Python programs for connecting to OpenAI API	6	24
Alexander Kronau	Worked on frontend development progression - vetting dashboard.	6	24
Caden Murphy	Worked on frontend development for Chat feature.	6	24

Plans for the upcoming week

- Ethan Comiskey - Begin curating a list of questions to pre-seed our database so it is not starting from scratch
- Steven Ragan - Start creation of question set in order to pre-seed the database.
- Alex Elsner - Continue middleware development, hopefully get a full loop between DB,

Middleware, and Open AI. Start looking on how to develop WP plugins.
- Casper Run - Continue middleware development. The next goal is to have a full data loop between the database and the chatbot
- Alexander Kronau - Contact previous frontend dev to gain system insight. Begin integration.
- Caden Murphy - Implement a new chat page and establish backend communication.

Summary of advisor meeting

On March 12th, we met with our advisor, Doug Jacobson, to discuss specifications for our project. We discussed the usage of plugins for WordPress and the server we will host Ask Captain Cyber on, in which we can either use existing ones or create our own, considering they are generally just PHP scripts. Based on new information, it is unlikely our project will be hosted on the same server as Cyber House Rock though it was originally supposed to be. This is due to various technical reasons, one of which is that existing plugins on the server may clash with the ones we need to use for the project. Fortunately, this means we have more freedom on the front end since we do not have to abide by previous server specifications and can make our project look however we want it to. The final important thing we discussed was database management, specifically what we currently have set up, which is our categories and questions tables and whether we should create a user table or not, to which the answer was that it was unnecessary.