AppDev Team

CPST-4710

Minimum Viable Product (MVP)

The goal of the Minimum Viable Product (MVP) is to facilitate the process of taking orders from a customer, allow for customization of select items, catalog that order, manage the overall inventory of the store, and most importantly fall in line with the Cybersecurity Maturity Model Certification (CMMC) requirements. The MVP should be usable and effectively replace the current manual order intake system and hand cataloging. However, the goal at an organizational level is to attain the CMMC level required to do business with the government. As a result, any solution implemented must adhere to these requirements or risk a complete failure of the project.

Some critical steps must be taken along the way to ensure that the product delivered is effective at making the overall ordering process easier and safer for the consumers, as well as saving time and increasing efficiency for the employees who are at present taking orders over the phone and are manually entering those orders into a spreadsheet. To start the process the team will need to gather the requirements for the application itself. This focuses on the core requirements outlined above: order intake, order management, inventory management, and alignment with CMMC level one.

After all the requirements have been outlined the team will then need to move on to designing the application. This will also include the stage where the final decisions are made regarding the technology that will be used in the project. While this could be subject to change as the project progresses and the scope widens, an initial estimate of the technology required will make the project manager's job easier, allowing them to coordinate with the information security and networking teams to ensure we have the resources needed. The design phase will also include the development of wireframes to iron out any User Interface (UI) decisions before moving to production. This will ultimately dictate what functionality is going to require development.

Some CMMC considerations the team has discussed would help to secure the application and make it a safe and secure shopping experience for customers. For instance, in the control of public information requirements, the team could implement the ability to publish certain listings or control their access otherwise. This helps to control the flow of data to the site which could help lock it down in the case of attempted defacement. Some processes and policies could be implemented within the system forcing a user to meet certain password requirements. This could be taken further by requiring passwords to be changed routinely. This control would fall under Authentication.

Throughout the design process, the team will need to ensure that the functions being proposed are within CMMC standards and will not leave the application vulnerable in any way. Some security considerations the team has proposed are the inclusion of user accounts to manage

and log access. In conjunction with these accounts, the team has proposed the idea of Role Based Access Controls (RBAC) to limit the permissions of individual users. The team currently plans to utilize SQL or something similar as a backend database. Thus, the team must ensure that text entry fields are secured and not vulnerable to SQL injection attacks.

The team's ultimate goal is that the application makes the day-to-day interactions with the ordering process much easier and significantly more streamlined than it currently is. Our hope from customer feedback is that they are engaging positively with the application. The team certainly expects that once a product is delivered to the customer they will find flaws and potential improvements, but that would only allow us to create an even more robust product. Once the baseline is developed it can be improved upon to become more user-friendly, efficient, and resilient.

When looking for feedback from the customers the team will be primarily looking for ways in which the user interface and experience of the application can be changed to better facilitate the day-to-day functions of the end-users. For this application, there are ultimately two different end-users. The customer on the front end customizes and purchases items and the internal employee intaking orders and manages inventory.

To conclude, the MVP will need to meet several requirements to be considered acceptable to all teams. The design should be lightweight and easily understood by untrained customers. The system should through the use of SQL log customer transactions and facilitate a simpler method for inventory management. As outlined above, the team currently has preliminary plans to implement seven different controls: AC.L1-3.1.2 - Transaction & Function Control, AC.L1-3.1.22 - Control Public Information, IA.L1-3.5.1 - Identification, IA.L1-3.5.2 - Authentication, SC.L1-3.13.5 - Public-Access System Separation, SI.L1-3.14.2 - Malicious Code Protection, AC.L1-3.1.1 – Authorized Access Control. Once the application is built to meet the standards outlined the team will begin gathering some user feedback to get a better understanding of any additional changes that might be needed. With this outline, the team hopes to deliver a simple but effective solution that complies with the new CMMC standards.