**Project Proposal: Asset Management System**

**CSC 179**

Members: Roger Diaz, German Lugo, Edward Petruescu

**1. Project Title:**

Asset Management System

**2. Team Profile:**

**Roger:**

I have experience working with web based RESTful API using Springboot. I also have programming knowledge in Java, HTML, CSS, MySQL, GCP, and some Javascript. I’m a good speaker and can communicate and work with a team effectively. Quick learner and am able to learn a new language or skill fast. Good at time management and prioritizing events or items in my school and work schedule. Identifying problems and thinking of solutions is also one of my strengths, which helps with this project.

**Edward:**

I have experience with MVC, tomcat, and java applets and programming experience in asp.net, C++, C#, java, Verilog, Python, javascript, and assembly. I’m good at leading groups, public speak, self study, and will finish whatever i started.

**German:**

I have programming experience in Java, C++, C, and Verilog, assembly and SQL. I worked with java UI for different android application projects. Able to adapt to changes in project when facing problems. Have experience being the line of communication between clients and programmers.

B. We decided not to have a team lead and that we would all contribute to the team's success.

**3. Proposed Project Description:**

Open source software is one of the biggest factors that lead to new innovations in the field of technology. Many individuals and startup companies use existing open source software as the base of their product/project. There are thousands of open source software available that propose to offer certain services and can be utilized free of charge. An Asset Management System is one of these open source software. The problem with this however, is that some of the software available can contain faults/bugs. Some security issues can also pose a threat and let hackers access sensitive data. A hacker finding a vulnerability in a asset management system can create chaos. They could erase or add any inventory they see fit and change important information on individuals as well. Lacking proper testing of a database connection can also cost problems. Writing incorrect data to a database can cause assets to be mismanaged and possibly unauthorized access These bugs can be extremely costly if they are not found. Our solution is to test these vulnerabilities and take the necessary steps needed to prevent these dangers from happening to the system.

**4. Project goals:**

* Find security flaws and code faults
* Create solutions for these flaws and faults
* Define how security for the system is to behave
* Provide documentation for developers
* Test database entries
* Test common attacks and data with expected outputs

**5. Plan of work and ownership:**

Functionality:

* Encryption
  + Encrypt data so it is transferred securely
* Authenticating
  + Validate that the user has access to the data being requested
* Secure Connection
  + Validate the connection is made to the database and is secure
* Database interaction
  + Validate database entries

Qualitative:

* Secure Connection
  + Transport data with high levels of security
* Confidential
  + User private information stored securely from prying eyes
* Security
  + User data is safe from attacks such as SQL inject etc.

Find major security flaws and data integrity fault by examining the most common flaws. First, we are going to examine the web application system for any obvious faults. Second we are going to check to see if the data we input are constrained properly and not let loose to run amok. Once any data vulnerabilities/integrity issues are discovered we will diagnose it and fix it. For example, the application has a data entry field for an asset number. We will check to see if we can mix other characters along with integers and see if it properly handles invalid and valid user input. We will be documenting, and mapping the issues so that others may recreate the same instances and receive the same results. Create a guideline for the developers how they can minimize the issues we found.

**6. Deliverables:**

The goals of the project is to research security flaws along with database interactions. At the end of the project a document will be produced containing background information, security flaws, and database flaws in a detailed report, The document will also include proposed policies that can be used to increase reliability, security and database integrity. The policies should be build on a framework that will allow further contingencies to be put in place since technology and its flaws are only advancing.