A Platform for Managing Security Evaluations

Project Proposal (Draft)

SYSC 4907 Fall 2021

Team Members
(Last name in alphabetical order)
Zijun Hu 101037102
Tiantian Lin 101095243
Jiawei Ma 101034173
Ruixuan Ni 101092506

Supervisor
Jason Jaskolka, Ph.D., P.Eng.

Date: October 1st, 2021

Table of Contents

1.1 Statement of Objectives 1

1.2 Functional Requirements 1

1.3 Non-Functional Requirements 1

1.4 Progress Measurement 1

First Milestone: Preparation: 1

Second Milestone: Develop the program separately: 1

Third Milestone: Integrate Different Parts, Test and Fix Bugs: 2

Fourth Milestone: Documentation and Presentation: 2

2. Background 2

3. Project Description 2

3.1 Purpose 2

3.2 Structure of Project 2

3.2.1 Front End 3

3.2.2 Back End 3

3.3 Conclusion 3

4. Discussion 4

4.1 Individuals 4

4.1.1 Zijun Hu 4

4.1.2 Tiantian Lin 4

4.1.3 Jiawei Ma 4

4.1.4 Ruixuan Ni 4

4.2 Group 5

5. Methodology 5

5.1 Program languorous selection——Python 5

5.2 Software Design Process Model——Spiral model 5

5.3 Web Interface vs Graphical User Interface 5

6. Timetable 6

7. Potential Risks and Mitigation Strategies 6

8. Components and Facilities 6

References 8

1. Introduction

1.1 Statement of Objectives

The goal of this project is to design a platform for developers to upload security evidence. This platform can store and manage a large amount of security evidence, and it can also provide evidence tracing functions for subsequent security assessments.

1.2 Functional Requirements

- The platform should allow users to edit their passwords and their profiles.
- The platform should allow users to upload the security evidence.
- The platform should store a large amount of security evidence and organize the data based on each evidence's attribute.
- The platform should allow users to search the security evidence using keywords.
- The platform should allow users to trace the history of the uploaded files.

1.3 Non-Functional Requirements

- The platform should prevent all stored evidence from being threatened and attacked, such as unauthorized disclosure, deception, and disruption.
- The platform should ensure that all authorized developers can use this platform to store and manage evidence anytime and anywhere.
- The platform should only allow authorized developers to access and manage the existing evidence and store new evidence.
- The platform should be able to recover once it has been attacked or any evidence is lost.
- Users could use web browser such as Chrome, Safari, and Microsoft Edge to open the platform webpage.

1.4 Progress Measurement

There are four milestones set for this project. They are *Preparation*, *Developing*, *Integrating* and *Documenting*.

First Milestone: Preparation:

During this milestone, the main goal is preparing for the project/ program as much as possible. This milestone has several procedures: making a plan for the whole project, analyzing the project's functional and non-functional requirements, choosing an appropriate model and pattern to develop the program, and unifying the programming development environment and tools.

By the end of milestone1, each member should have a clear view of the project and acknowledge why we need this project, what functions and features we should develop and how to develop the program. In addition, our group should be fully prepared to develop the program.

Second Milestone: Develop the program separately:

In milestone2, our group starts developing the program. We decided to use the MVC pattern to develop this program. The program can be divided into three parts: the front-end, the back-end and the database. Each part contains interfaces that help to connect other parts. Each member could choose one part and work on it to ensure the program is low coupling and high cohesion.

By the end of milestone2, all functions and features in the front-end, back-end and database should be developed thoroughly. Furthermore, the program should be prepared to integrate and be prepared for the quality assurance testing.

Third Milestone: Integrate Different Parts, Test and Fix Bugs:
After completing development in each part, the entire program will be integrated into a whole through the developed interfaces. The test suites should also be added to this milestone to ensure the program runs as expected.

By the end of milestone3, the development of the entire program should be finished. The program should run as expected. Moreover, the program should not contain any unexpected behaviours or severe bugs.

Fourth Milestone: Documentation and Presentation:
In this milestone, all documentation such as the final report, the oral presentation slides should be completed. Furthermore, each member should be ready to demonstrate and present their work in both oral and written.

2. Background

Nowadays, the reliance on information technology from people is increasing. Corporations are paying more attention to protecting their systems and products with well-implemented security mechanisms in this environment. There are already multiple security evaluation criteria for computer security certification (for example, the Common Criteria). These criteria provide standards for systems to be checked to ensure if the security features in the TOE (target of evaluation) work correctly in these systems.

Security testing and vulnerabilities management tools are already widely used in the system development life cycle. However, these tools concentrate more on vulnerability monitoring and management instead of evidence of security evaluation.

There will be a lot of security evidence in development life cycles. The evidence may come from many different sources, especially for large and complex systems. The Common Criteria tool, which can store and manage the evidence, could help security evaluators and regulatory authorities verify and evaluate the system's security. The evaluation results would help customers to determine whether the products satisfy their security requirements [1].

Besides, the Common Criteria tool can also help developers to facilitate the security assessment process. Therefore, a platform that can store and manage the security evidence would be necessary for a large and complex system.

3. Project Description

3.1 Purpose

This project aims to develop a platform that developers can use to store and manage the security evidence generated during the entire system development lifecycle for future security assessments. When developers design large and complex systems, the storage and traceability of security evidence become a significant problem. The reason is that when designing and developing large-scale systems, the sources of evidence are complex and huge. This is very difficult for the follow-up safety assessment. Therefore, this management system can help security analysts collect security evaluation data and help developers submit evidence.

Besides, one of this project's purposes is to evaluate the skills and knowledge that we learned in the university. Therefore, we should apply our skills such as project design, programming skills, and communication skills to this project. Although we are still engineering students, we all need to act and behave like engineers in this project.

3.2 Structure of Project

The structure of the project can be divided into two sections: Front-end, Back-end. The primary purpose of the Front-end is to interact with the user, allowing users to upload/view the evidence and display needed information

to users. The back-end includes a server and a storage space to categorize and store all involved evidence and information.

3.2.1 Front End

In this project, the front-end will be designed and delivered in web-page format. The page will be written in HTML and styling using CSS. Users need to either sign up or log in using their username and password via the login page to use the system. A security password mechanism will be used to safeguard the confidentiality of the system. When users sign up, the system will enroll them into the access control matrix depending on their role to ensure that they can only read/write to subjects their privilege allows. After users log in, they can choose to upload new evidence or review existing evidence.

To upload new evidence, users need to provide related information via the evidence upload page. The page will provide an online form for users to fill. Required information includes but is not limited to the type of evidence, related project change information and comment to the evidence. The purpose of doing that is to help categorize the evidence later and ensure the traceability of the evidence history.

As well as the upload page, there will be a search and review page provided to users for them to search and review the existing evidence. The system will offer several filters to users to explore the evidence they want. The evidence can be filtered by tags, evidence type, upload users or last modified time.

3.2.2 Back End

The role of the back end is to process the data input by the front end for analysis and storage. In order to realize these essential functions, the back-end design can be divided into three major modules, namely the storage and retrieval module, the data classification module, and the user account management module. Each module performs the corresponding functions, separated from other modules as much as possible. Through the modular design, high cohesion and low coupling of the back-end model are realized. This design is also convenient for later maintenance and the future addition of functions.

The data storage and retrieval module are to manages the security evidence uploaded by users when developing large and complex systems. The evidence is stored in different categories based on its attribute. At the same time, users can also use this module to query security evidence and trace the security evidence data.

The data classification module is used to classify security evidence from the file uploaded by users. After the user uploads the files, this module could provide further evidence with tags. The purpose of this module is also for data storage to be more organized so that subsequent tag searches can quickly find the information that users need.

The user account management module mainly records the user's account information, login password, and the user's uploaded file history. Users can use this module to query their uploaded historical records, modify passwords, modify personal information, and so on.

3.3 Conclusion

Security evaluation is an indispensable part of software design. It can detect the presence of threats and reduce risks. [2] This security evaluation management platform can effectively manage the data uploaded by users for analysis and assessment. In the future design, this platform can also add some functions such as giving strategies to deal with risks or providing users with preventive suggestions. In conclusion, we need to pay more attention to security evaluation and not wait until the safety failure occurs.

4. Discussion

4.1 Individuals

4.1.1 Zijun Hu

As a computer system engineering student, I have learned system security, software communication, and development knowledge. In the project development process, I will focus on the front-end development and the program logic between the front and back-end interaction. I will use the knowledge I learned in the course, Introduction to Software Engineering to make the development process more efficient and systematic. As well as that, I am currently taking an elective course called Fundamentals of Web Development, which will also help me when developing the front-end section for the project.

Since my team members are all coming from the Software Engineering program, I might be less professional than them in software development. But at the same time, I have some knowledge that they do not possess, especially on computer networking and communications software. This knowledge will help me fill the vacancies in the team and make the interaction between the front and back ends of the project more comprehensive.

4.1.2 Tiantian Lin

As a student of software engineering, the design of this project can be connected with many aspects of what I have learned from the previous three years. So far, I have taken many courses related to software, such as database management, software design and software requirements engineering. In this project, I can use what I have learned in these courses to design and develop a back-end system. In the early stage of the project, the knowledge of software architecture can be used to design the back-end system's different components and frameworks. I could design the UML diagrams, sequence diagrams and state diagrams before developing the entire system. In addition, through the internship, I also have some experience in automated test development. Combined with the software verification course currently being studied, it will also help the test development process for the project.

4.1.3 Jiawei Ma

Since my four-year studies in Software Engineering, I have learned and practiced a lot related to programming and software development. My most significant strength in programming skill is Java programming on both front-end and back-end. Similarly, I am also good at other programming languages such as C++ and C on the back-end. Through the project and program design courses, I also have dramatic knowledge of project requirement design and requirement analysis. Therefore, I would apply my project and programming design knowledge, programming skills, and communication skills to this project with my group members.

Besides, through the Co-op study as quality assurance, I now can test the program manually and automatically after each development phase. Despite not being good at python and web programming, I will still communicate and cooperate with my group members by studying related knowledge and applying it to the project.

4.1.4 Ruixuan Ni

I am a student studying in the program of Software Engineering. Since this project requires a complete software development process, this project is directly related to what I learned during my undergraduate study. In the early stages of the project development, I could contribute to the development of requirements, design of architecture and details (for example, drawing UML diagrams). For this project, our group plans to develop a web platform to manage evidence of security evaluation. In the implementation phase, we might use Python, Django and MySQL. I have learned the fundamentals of Python in school and have practiced Python projects during co-op. I have also learned basic SQL commands. This means I could also contribute to the project implementation in the front-end, back-end and database. Generally, since most of my group members are in the program of Software Engineering, we would prefer to cooperate in all stages of development.

4.2 Group

Our team members are from software engineering and computer systems engineering. Everyone has studied or is studying the SYSC 4810, the introduction of network and software security. Therefore, for this project, the safety evaluation management platform, the team members can use the knowledge they have learned to have a general framework. Besides, all team members have studied SYSC3120/SYSC3020. All members can contribute knowledge about analyzing requirements and designing the project to satisfy the requirements. In addition, each team member has his or her field of expertise, including but not limited to web design, database management, automated testing development, network transmission protocol, software architecture design. These skills are all essential for the realization of this project.

5. Methodology

5.1 Program languorous selection——Python

In this project, we would need to implement a front-end (web pages) and a back-end, including a server and a storage space. Our group decided to use Python to implement the server. Python is a high-level scripting language in programming with an extensive library. It has modules and packages which support functions like data management or network transmission [3]. Python also supports accessing databases like MySQL with wrapper, which simplifies data storage and transmission functions [4].

We have also considered Java. Compared to Java, Python is a more readable programming language and easier to learn. Python is also more efficient than Java in development. Besides, all of our team members have essential experience in Python programming. Our group believes that Python is a programming language that is more suitable for our present project architecture and development plan.

5.2 Software Design Process Model——Spiral model

In this project, we choose to use the spiral model as our software process model.

In the spiral model, we will have several iterative processes. We can add additional features, analyze the risks and test the completed requirements in each iterative process. Through these procedures, our team would have strong approval and documentation control.

The most significant disadvantage of the spiral model is that it would have a high overhead. It may take much time for each iterative process. However, we have two terms to complete this project. We can have at least two life cycles in the spiral model to design, identify and resolve risks, develop the new features and test, and plan the next phase. After each phase, our program would be more comprehensive and secure.

5.3 Web Interface vs Graphical User Interface

GUI(Graphical User Interface) is one form of UI(user interface) that allows users to interact with the program to perform needed commands. [5] Using GUI, the designer could easily control each pixel on the users' screen, the access direction and efficiently guide the user to view the information/pages the designer wants. Also, it can force the user to enter information before entering the next step by using the pop-up windows. [6] However, it makes users' operation flexibility become lower. At the same time, it also takes longer for users to familiarize the system and operating methods.

Web Interface is a kind of interface that requires the users to access via the web browser on their phone, computer or tablet. Compared with traditional UI, it provides users more flexibility and is accessible to updated. Users can access through any smart device with a browser. At the same time, because the webpage itself is stored on the service provider's server, developers got chances to update the web page easily without asking users to download any updates packages.

After balancing the pros and cons, the web page format was selected for the front-end development in the project due to the ease of application updating and the flexibility on accessing.

6. Timetable

According to the Project Guideline, our team decided to set our project completion time following the deadline of the Guide. To prevent potential risks that may delay our process, such as illness, our group plans to complete each task and milestone three to five days before the scheduled deadline. If we complete each task or milestone ahead of our schedule, we can double-check our program's existing problems or documentation through the remaining three to five days.

Task Name	**Schedule Complete Time**	**Deadline on Guideline**
Project Proposal Draft	October 1st, 2021	October 1st, 2021
Milestone1 Completion	October 20th, 2021	N/A
Project Proposal	October 20th, 2021	Noon of October 22nd, 2021
Progress Report	December 5th, 2021	December 10th, 2021
Milestone2 Completion	December 31st, 2021	N/A
Oral Presentation Preparation	January 22nd, 2022	January 24th, 2022
Milestone3 Completion	February 10th, 2022	N/A
Draft of Final Report	February 23rd, 2022	February 28th, 2022
Poster Fair	March 14th, 2022	March 18th, 2022
Milestone4 Completion	April 8th,2022	N/A
Final Project Report	April 8th, 2022	April 12th, 2022

7. Potential Risks and Mitigation Strategies

1. No time to complete any particular progress before the planned deadline.
2. Any member gets an illness during the development.
3. There is very little time for the project in some weeks due to other courses' exams, quizzes and assignments.
4. Structure or strategy change in the middle stage of progress (for example, take more time to decide between HTML, Django than expected)
5. Meet problems when coding, which makes progress behind schedule

8. Components and Facilities

1. GitHub for code version control
2. Google Doc for document version control
3. PyCharm (JetBrains) for python programming

4. PostgreSQL for designing database

References

[1] C. Criteria, "Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model," April 2017. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf. [Accessed 27 September 2021].

[2] Synopsys, "Security Risk Assessment," [Online]. Available: https://www.synopsys.com/glossary/what-is-security-risk-assessment.html. [Accessed 26 September 2021].

[3] P. S. Foundation, "The Python Standard Library," Python Software Foundation, 01 October 2021. [Online]. Available: https://docs.python.org/3/library/. [Accessed 01 October 2021].

[4] A. Lukaszewski and A. Reynolds, MySQL for Python, Packt Publishing Ltd, 2010.

[5] "Graphical user interface," Wikipedia, 26 September 2021. [Online]. Available: https://en.wikipedia.org/wiki/Graphical_user_interface. [Accessed 1 October 2021].

[6] "The Difference Between Web Design and GUI Design," Nielsen Norman Group, 30 April 1997. [Online]. Available: https://www.nngroup.com/articles/the-difference-between-web-design-and-gui-design/. [Accessed 1 October 2021].