COMP SCI 7412 Secure Software Engineering Group Project Individual Reflection - Group 2

Tinson Lai
a1812422

1 Project Overview

Our choice of the project topic is the first one, *Electronic Senate Voting System*.

1.1 Project GitHub

`https://github.com/laitingsheng/COMP-SCI-7412-Group-Project` which will be made public and archived after the formal deadline.

1.2 Tech Stack

The project is using

- ReactJS and related libraries
- Google Firebase
- Google reCAPTCHA

1.3 Contribution

- I am the coordinator and leader of the group, and I've coordinated and arranged all necessary meetings throughout the semester.
- I've written most of the functioning code in the project. I am also the code reviewer to ensure code submitted by other members can integrate with the current implementation.
- The report is reviewed by me as well.
- I am responsible for the demo part of the presentation.

1.4 Focus

Our project set-up has native advantage against most of the common vulnerabilities including (but not limited to)

- XSS attack, since ReactJS has built-in functionality to prevent and neutralisation all special characters. All modules we use contains only safe React Elements[1], which means we don't need extra

[1] `https://reactjs.org/docs/dom-elements.html#dangerouslysetinnerhtml`

steps in our implementation.

- CSRF and other man-in-the-middle attacks, which relies on the security of Google Firebase itself. Google Firebase only supports HTTPS (SSL) requests, which means all transmitted data will be encrypted before sending out. Google Firebase provide a way to even enhance the security apart from normal CSRF token[2]. In our implementation, we even clear the session cookie after the user close the tab.
- SQL-related attacks, since Firebase Authentication doesn't expose explicit SQL interfaces to the client, and Firebase Firestore is a NoSQL-like database.
- NoSQL-related exploits, but Firebase Firestore has built-in validation to eliminate the possibility of such attacks, and the internal API was not exposed to the client as well.
- DoS attacks such as repeatedly registering account can be prevented by Google reCAPTCHA, though this is not formally enabled in our final version since we are using the testing key. But the concept here is it can prevent robots from repeating actions which potentially creates a DoS attack.

2 Reflection

Actually, this is a quite interesting project as I've learned different way to integrate security measures into a website. Initially, we even considered using AusPost's Digital ID to perform an actual Personal ID check, but this has been put into the future works since it needs to sign a lot of contracts and agreements. But I indeed had a glance at their documents about Digital ID's API after contacting AusPost, and the API is quite simple and can be easily integrated into the project, provided that we now need a backend server other than Firebase.
Initially, we indeed planned a backend server, but eventually we realised that it is redundant since Firebase has all functionalities we need, and the statistical part is not mandatory (as per Jason said in the last presentation).
Our teamwork is quite nice except that there is someone who eventually did no contribution to the project, even though we have made work arrangements during the meeting. However, the way we collaborate on coding could be improved, as most of the code written by other members are not functioning or functioning improperly. I didn't give clear instructions on how to implement the code beforehand, so what they've implemented cannot fit the expectation. I think I have to improve my management and leadership skills in the future.
There are quite a lot techniques we proposed to use as well, including containerising then deploying it to GKE, but we don't actually want to have extra expenses for this course, so we eventually cancel the plan to deploy it. But the Dockerfile is still provided in the repository.
In general, the project is quite interesting to me, and I also learned a lot of details about the AEC voting rules.

[2] `https://firebase.google.com/docs/auth/admin/manage-cookies`