Part A: Planning

My client is an internet user who uses many different web services requiring separate accounts and logins. He has trouble remembering different passwords for each account, so he has been using the same password for most websites. However, he has recently become worried that this could lead to all his accounts being compromised. He wants to increase security on his accounts, but he doesn't want to remember many different passwords. He also doesn't want to use an already existing password manager as he does not trust them to keep his passwords secure. Therefore, he asked me for advice.

I met with the client and consulted with him (a transcript is available in the Appendix). I suggested that I make him a password manager, to which he enthusiastically agreed. We decided on a list of tasks that the *Solution* should be able to do, which is shown in the Success Criteria below. The client specifically requested that the software have a user-friendly interface to enable him to use the password manager more easily.

The *Solution* is suitable for the client's problem because it allows the client to have secure, alphanumeric passphrases with special characters (that are almost impossible to remember), but to only have to remember one passphrase.

Success Criteria

- The client can create an account with an email and passphrase
- The client is prevented from choosing an unsecure passphrase
- The client can easily add new passwords for different websites
- The client can easily remove passwords
- The program stores different passwords for different websites under secure encryption
- The program has a user-friendly interface
- The program can sync passwords across multiple devices
- The program has an inbuilt password generator
- The program supports two factor authentication