**Slide 1**

Good evening everyone, my name is Steven. Today I am going to talk about our course project - Password Generator. There are three members in our team, Maribeth, Richard and I.

**Slide2**

This slide shows the contents. In the presentation, I will talk start with *What is a Password Generator* and *why we choose it as our project*, Then, I will introduce all of the *technologies* and *methodologies* that we have used in this project. After that, I will focus on the *Team Work* and *Reflections*. I will be very glad to answer all of your questions before I end the presentation. This presentation will take about 10 mins.

**Slide 3**

Firstly, let’s think about what is a password generator. I would hazard a guess that all of us have the experience of registering an account, either on a laptop or a tablet. Sometimes it is in an Android system, other times it is in an IOS system.

**Slide 4**

But did you feel hard in creating a password? To be honest, I did. Most websites have different requirements for passwords. For example, Goole Account asks for a password including characters, numbers and symbols. Microsoft needs to enter a password including two of the uppercase characters, lower characters, numbers and symbols. As for Air New Zealand, it asks for a password of at least 12 characters, but it cannot contain username, or email address.

**Slide 5**

If you are lucky, finally pass through the password checking. What does your password look like? Is it “123456”, or “qwert”? Not good, it is too simple, right? How about “1qaz2wsx”, or “passw0rd”? These look quite strong, doesn’t it?

**Slide 6**

Unfortunately, according to Wikipedia, they are all weak password, very weak. It is in the top 20 weakest passwords.

**Slide7**

Think about what will happen if your password has been leaked. Of course, no privacy anymore. Of course, all of your relevant information will be exposed. If the account related with purchasing, that usually means money loss. Some times your account will be used in ID frauds. Even more, we are likely to use the same password in all the website because it is hard to remember all kinds of passwords when they are totally different. That is to say if one of the websites didn’t protect well your password, you would be in huge risk.

**Slide 8**

Now, let’s move to the Technologies. As I have mentioned. We are more likely to use the password generator in all of the devices and all of the operation systems. Therefore, we decided to develop it as a web base software. Then we can use it wherever we can access internet. The coding language would be java script and html – we have learned in this course.

**Slide 9**

The methodology we choose to use is waterfall. We have four reasons for using waterfall. Firstly, for this project, the requirements are explicit,

They are:

|  |  |
| --- | --- |
| 1.    Allow input of various input parameters on password such as Password Length, Include Symbols, Numbers, Lower/Upper case Characters, etc |  |
| 2.    Save the above parameter :( save all the settings above for later use) |  |
| 3.    Generate a random password for based on the above parameters |  |
| 4.    Copy function to copy the generated password to the buffer (like Control + C) |  |

Secondly, it is a relatively simple system. It only has four requirements.

Thirdly, it can only be used in certain circumstance, such as, registering an account or reset a password.

Lastly, it is a course project, it is unlikely to be changed in the future.

**Slide 10**

How does our team work? We divided the system into three parts.

The frontend part responsible for interacting with client users. It collects the parameters and initiates a request to the server - nodejs. When server finished processing, it will display either some error information or the password that server part has just created. Another function of this part is to copy the password to the clipboard.

The server part has been divided to two items. One is for dealing with the client request, responsible for parsing parameters and calling the third part, the module part, to create an appropriate password. Of course, before that, it will need to check all the parameters to make sure these parameters are valid. When a password is created by the module part, it will pack all the data and transmit them to the frontend. If all the parameters are correct, an additional job need to do in this part is to save them in a cookie so that the user can use them in the next time.

Maybe the module part is purest, but it is not the simplest. It is in charge of creating a password. Which is the main part of the project.

**Slide 11**

In this project, Richard finishes the part 1, Steven, me, the part2 and Maribeth, part3.

**Slide 12**

In this project, we all have learnt a lot. Ba la, ba la…

**Slide 13**

These are the references.

**Slide14**

Thank you for listening my presentation.

Now, it is time for Q & A. Does anyone have any questions?

Are there any more questions?