A UDP/IDP Project Report On

Random Password Generator

Prepared by

Shaikh Aadilhusen. I
(Enrollment No:190263107006)

Guided by:

Pro. Kruti patel

(Assistant Professor, CE Department)

DEPARTMENT OF COMPUTER ENGINEERING

KALOL INSTITUTE OF TECHNOLOGY
&
RESEARCH CENTRE

GUJARATTECHNOLOGICALUNIVERSITY
June-2021

Acknowledgement

I sincerely feel the credit of the project work could not be narrowed down to only on individual. The development of this project involves many valuable contributions. Getting the opportunity for this project of “Random Password Generator” as fulfilment of B.E (computer engineering) has been brightening experience for the near future to come and a focus on excellence in this venture, we are constantly guided and encouraged by Swho is our internal guide.

I would also thank our Head of the Department Prof. Kruti v. patel for giving us such a wonderful chance to work with this interesting project and perform the project work for the entire duration of 6th semester and also thanks to Sonam mam for project technical guidance and giving inspiration in all the way during project making. Finally, I would like to thank our parents, friends and almighty for being with us to support directly or indirectly while making this project.

KALOL INSTITUTE OF TECHNOLOGY
& RESEARCH CENTRE

Date:

CERTIFICATE

The report entitled "***Random Password Generator"*** prepared by ***Shaikh Aadilhusen. I*** for Summer Internship for the fulfilment of degree of Bachelor of Engineering (Computer Engineering), has been carried out under my supervision in the Department of Computer Engineering, Kalol Institute of Technology & Research Centre. Her present work has been found satisfactory.

Signature of Guide **Date of Submission**

(Name of Guide)

Head of Department

Department of Computer Engineering

KITRC

Table of Contents

Acknowledgement

Abstract

Chapter 1 Introduction……..... 7

1.1 Problem Summary…… 7

1.2 Introduction.....…… 7

1.3 Aim & Objective.....…… 7

1.4 Problem Specification....……. 7

1.5 Tools..... 8

Chapter 2 Implementation..... 8

2.1 Implementation environment...……. 8

2.2 Systems Flow Diagram.....…… 9

For OOAD (Object Oriented)

1.Class Diagram..... 10

2.Use case..... 11

For POP (Procedure Oriented)

1.Data Flow Diagram..... 11

2.ER Diagram..... 12

2.3 Snapshot……..... 13

Chapter 3 Summary……..... 18

3.1 CONCLUSION…….... 18

3.2 Advantages..... 18

3.3 Future Enhancement..... 19

References..... 19

ABSTRACT

Our Aim is to design and create a data management system for a maintain User security. This enables admin can Check authentic user that can be used by a customer This system increases customer relation and Simplify Customer and staff management in an efficient way.

This software random password generator has a very user-friendly interface. Thus the users will feel very easy to work on it. By using this system admin can manage customer confirm and cancel request, customer testimonials, customer issues. The car information can be added to the system. Or exited car information, where needed, car information an be captured very quickly and easily.

The customers can be also uses the system to get car rent. The customer should create a new account before logging in or he/ she can log into the systems with his/her created account. Then he/she can book the available cars and can book this car, this systems will helpful to the admin as well as to the customer also.

Chapter 1: Introduction

1.1 Problem Summary

Password is indispensable and inevitable one in today's communication process and provides security to user's data. Password is a sequence of character string used to authenticate personal identity of user and to provide or refuse the access to system resources. The password is not only denying any access to the system from unauthorized person, but also prevent users who are previously logged in from doing unauthorized process in system.

1.2 Introduction

Security risk from unauthorized entry involves more than the risk to a single user via their system account[1]. User ID and password combination is the one of the simplest forms of user authentication. Password is a secret word, which is used to authorize the user to particular system or particular application. The identity of the user is tested using the password.

1.3 Aim & Objective

- To produce a web-based system that allow customer to register and reserve car online and for the company to effectively manage their password management.
- To ease customer's task whenever they need to Generate password.

1.4 Problem Specification

A **random password generator** is software program or hardware device that takes input from a random or pseudo-random number generator and automatically generates a password. Random passwords can be generated manually, using

simple sources of randomness such as dice or coins, or they can be generated using a computer.

While there are many examples of "random" password generator programs available on the Internet, generating randomness can be tricky and many programs do not generate random characters in a way that ensures strong security. A common recommendation is to use open source security tools where possible since they allow independent checks on the quality of the methods used. Note that simply generating a password at random does not ensure the password is a strong password, because it is possible, although highly unlikely, to generate an easily guessed or cracked password. In fact, there is no need at all for a password to have been produced by a perfectly random process: it just needs to be sufficiently difficult to guess.

A password generator can be part of a password manager. When a password policy enforces complex rules, it can be easier to use a password generator based on that set of rules than to manually create passwords.

1.5 Tools

Hardware Requirement

- Processor: 64-bit Operating System 2 GHZ
- Primary Memory: 1 GB RAM or Higher
- Hard Disk: 20 GB free space HDD
- Network Configuration: Internet
- Browser: Chrome, Firefox, Opera, Safari

Software Requirement

- Linux/Windows or Any Operating System
- LAMP/WAMP/XAMMP Server
- My SQL server
- Browser
- Dreamweaver (Editor)
- Java Script Enabled Web browser

Chapter 2: Implementation

2.1 Implementation Environment

- Notepad++

Notepad++ is a text editor and source code editor for use with Microsoft Windows. It supports tabbed editing, which allows working with multiple open files in a single Window. The project's name comes from the C increment operator. Notepad++ is distributed as free software. At first the project was hosted on SourceForge.net, from where it has been downloaded over 28 million times, and twice won the Source Forge Community Choice Award for Best Developer Tool. The project was hosted on Tux Family from 2010 to 2015; since 2015 Notepad++ has been hosted on GitHub. Notepad++ uses the Scintilla editor component.

Notepad++ was first released on Source Forge on 25 November 2003, as a Windows-only Application. It is based on the Scintilla editor component, and is written in C++ with only Win32 API calls using only the STL to increase performance and reduce Program size.

Notepad++ is a source code editor. It features syntax highlighting, code folding and limited autocompletion for programming, scripting, and markup languages, but not intelligent code- or syntax checking. As such it may properly highlight code written in a Supported schema but whether the syntax is internally sound or compliable cannot be verified. As of version 4.7.2, Notepad++ can highlight the syntactic elements of:

Notepad++ also has features that improve plain text editing experience in general, such As:

- Autosave
- Finding and replacing strings of text with regular expressions
- Guided indentation
- Line bookmarking
- Macros
- Simultaneous editing
- Split screen editing and synchronized scrolling
- Line operations, including sorting, case conversion (Uppercase, lowercase, camel case,
- sentence case), and removal of redundant whitespace
- Tabbed document interface

- MYSQL

MySQL is an Oracle-backed open source relational database management system (RDBMS) based on Structured Query Language (SQL). Although it can be used in a wide range of applications, My SQL is most often associated with web applications and online publishing.
MySQL is a freely available open source Relational Database Management System (RDBMS) that uses Structured Query Language (SQL). SQL is the most popular language for adding, accessing and managing content in a database. It is most noted for its quick processing, proven reliability, ease and flexibility of use.

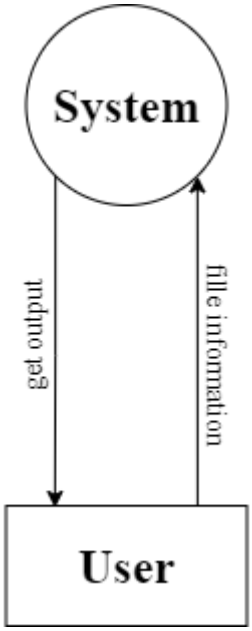
2.2 System Flow Diagrams

Fig 2.1 System Flow Diagram

For POP(Procedure Oriented)

1.Data Flow Diagram

A Data Flow Diagram (DFD) is a graphical representation that depicts the information flow and the transforms that are applied as data moves from input to output.



In this diagram, User and System are the two entity sets.

Functions of user:

- Open software.
- Fill important details.
- Hit the button display show password
- And user satisfied with this it’s a copyable facility will be there.

2. ER diagram

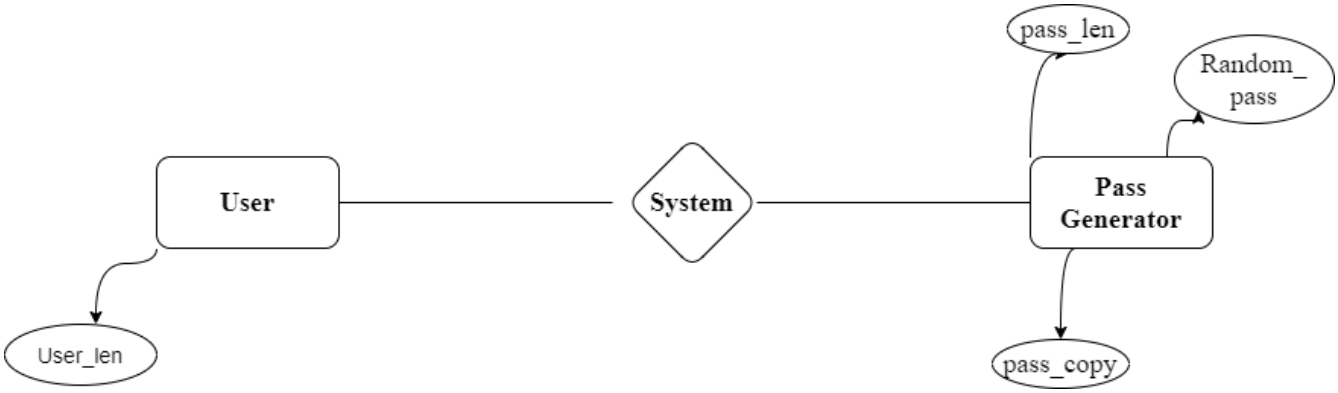
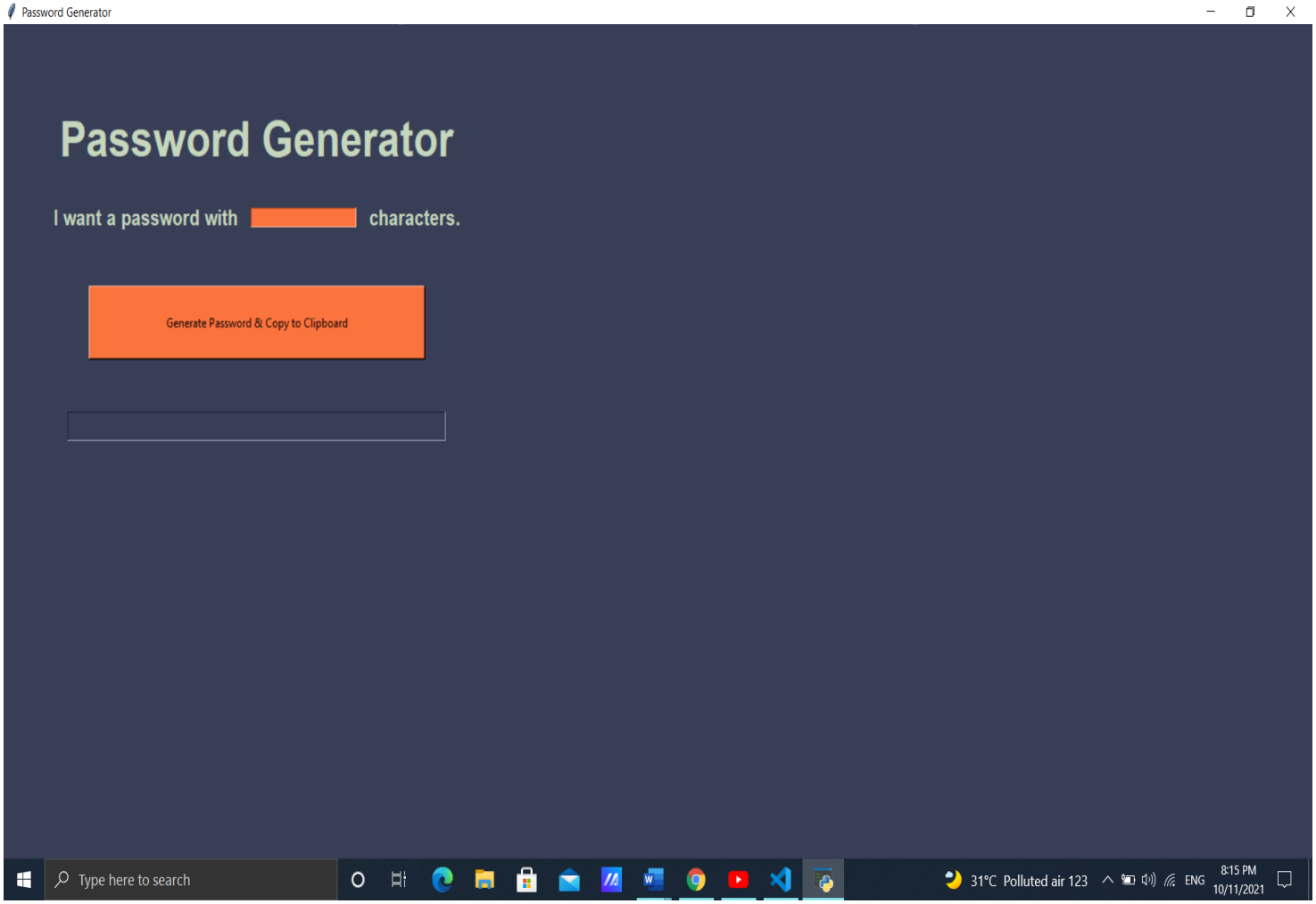


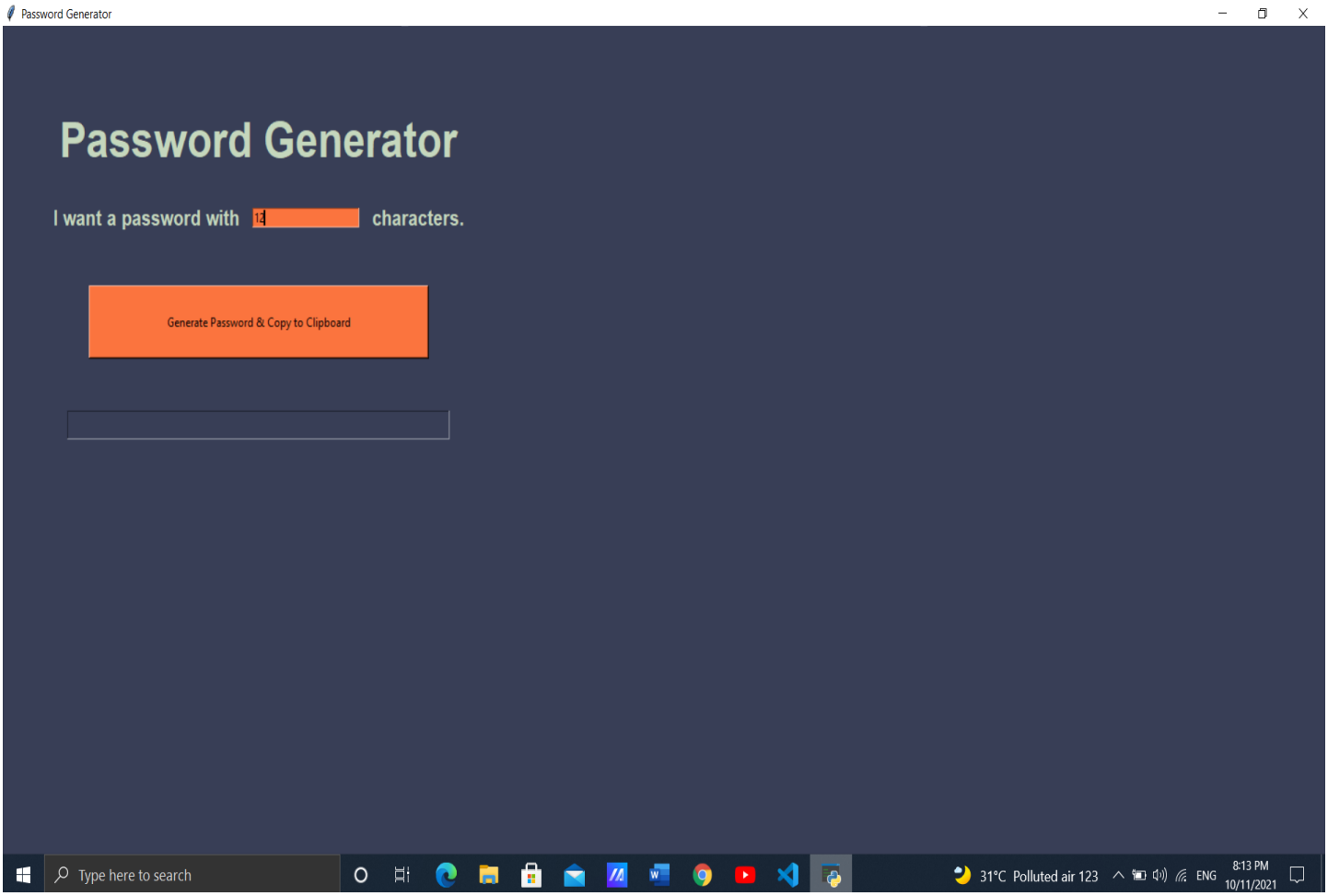
Fig 2.2.1 Er Diagram

2.4 Snapshots

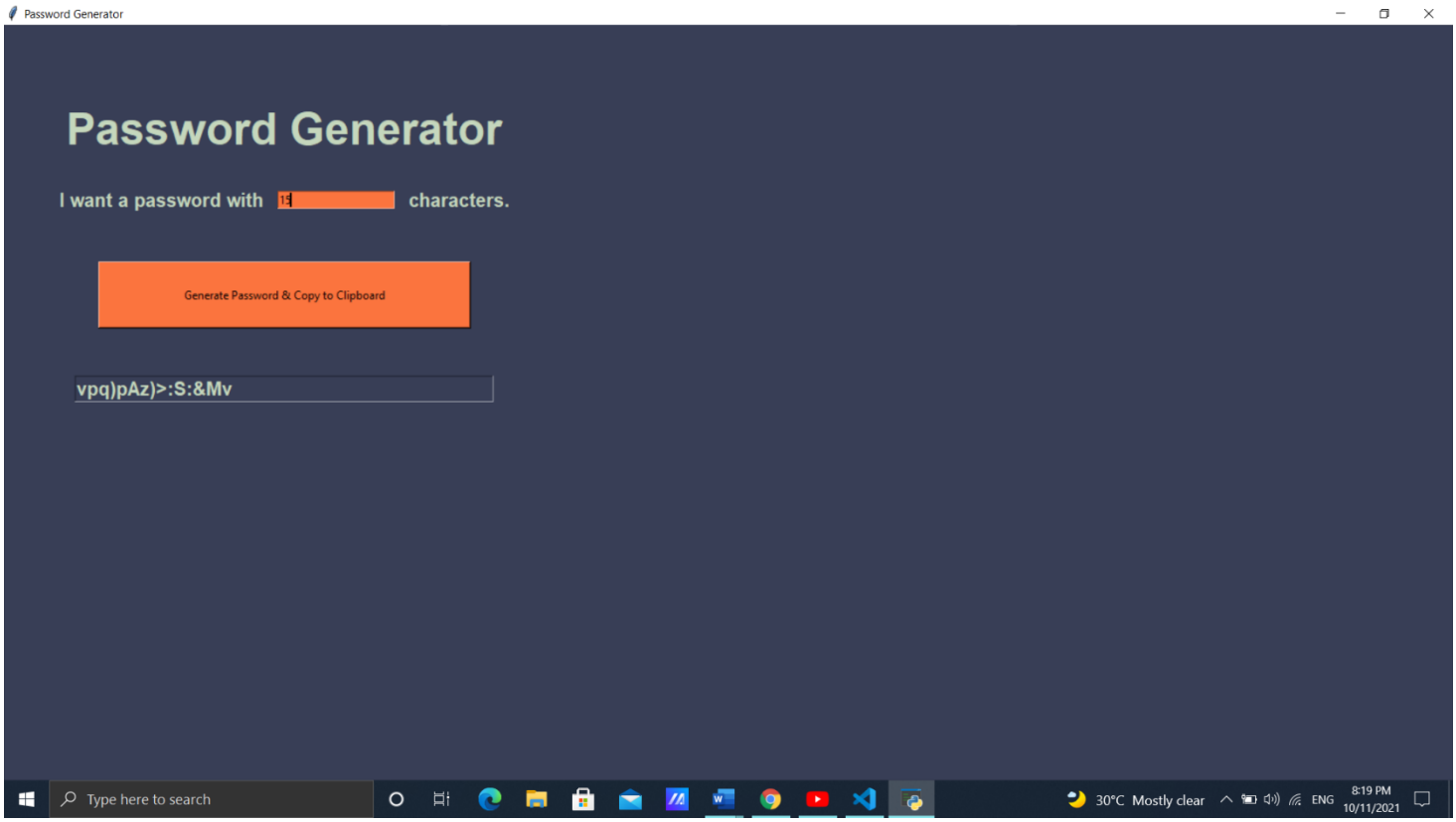
1: Run the software



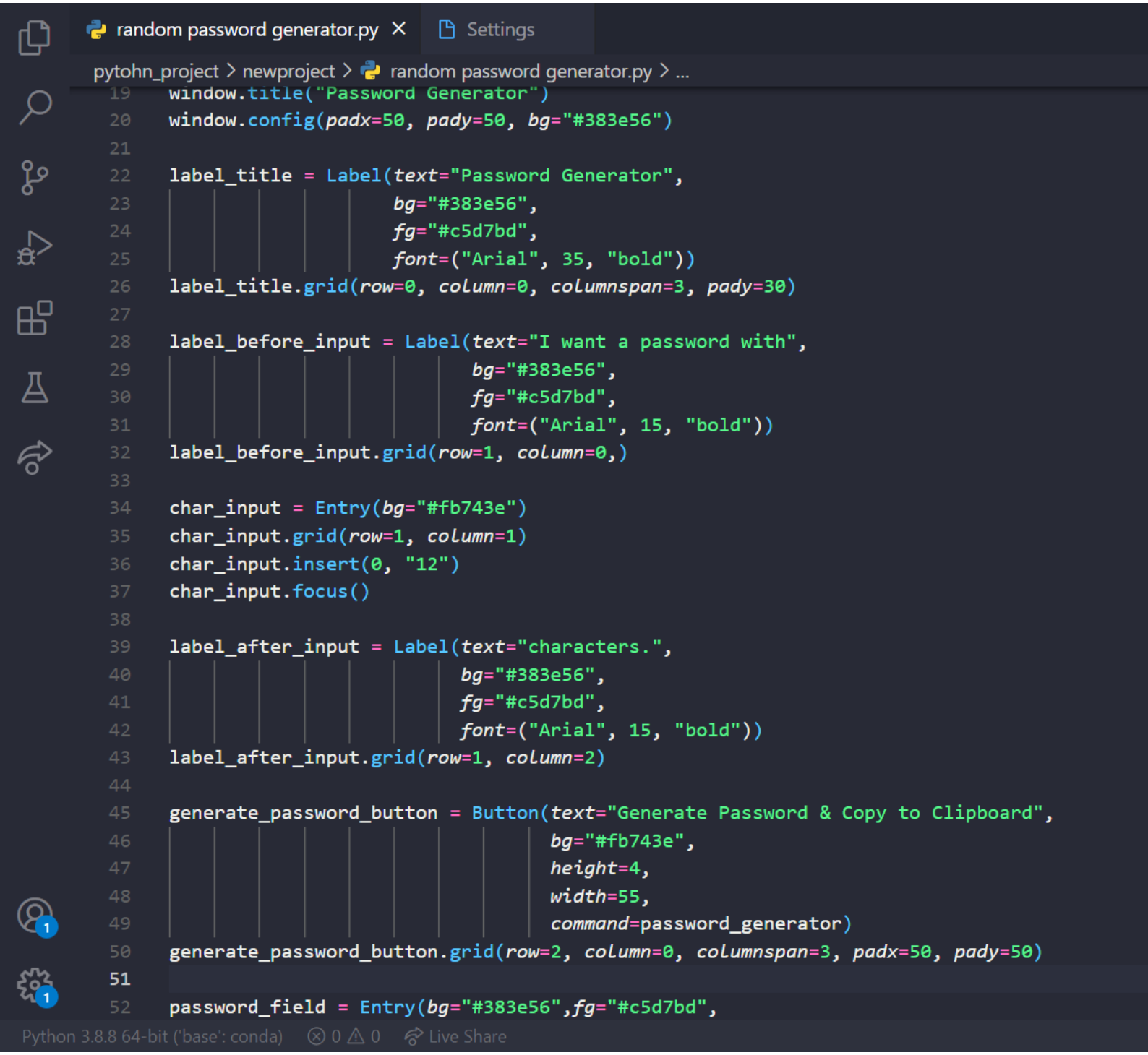
2 : Select the length of password

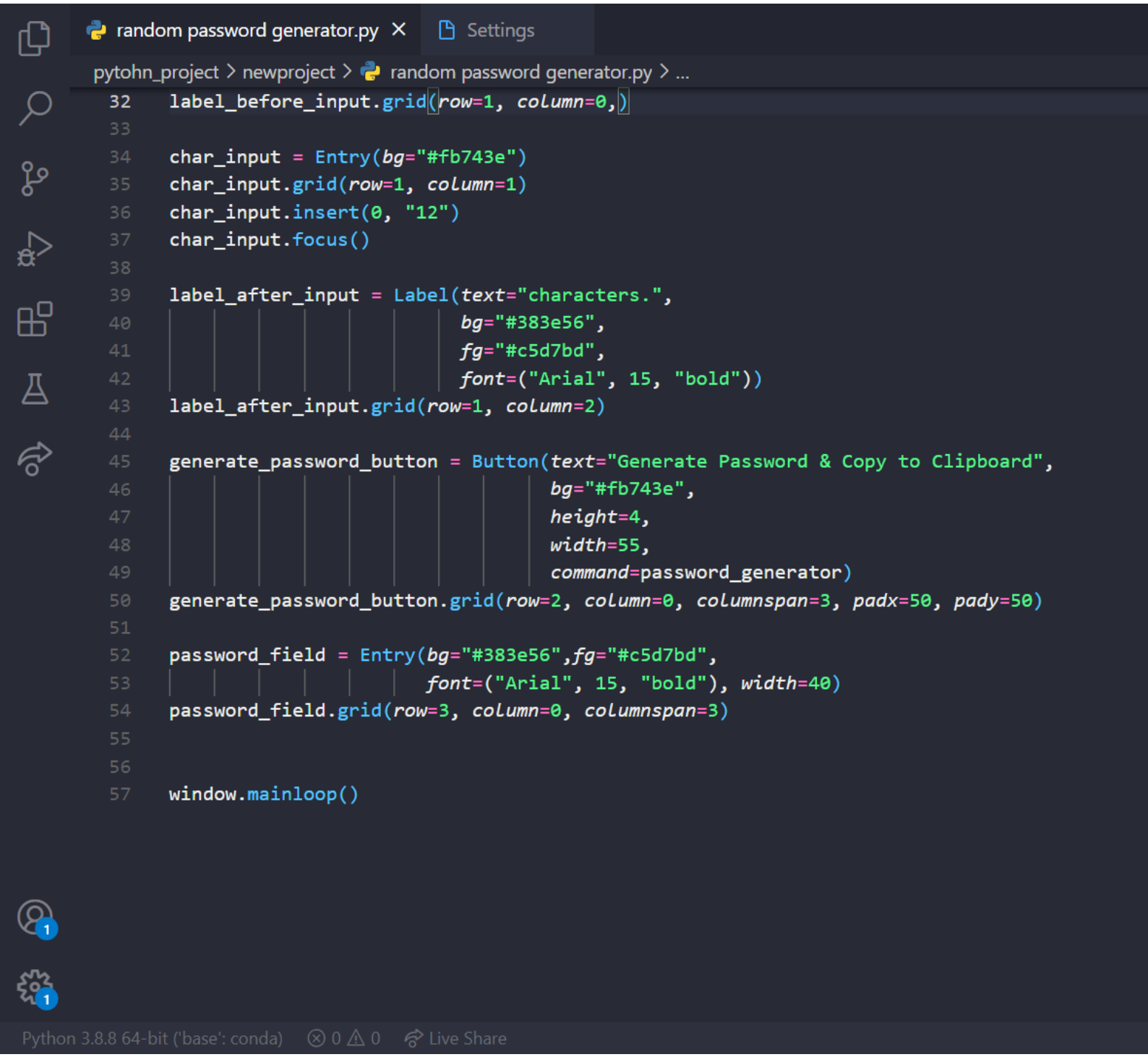


3: submit and auto copy to clipboard



4: demo code


random password generator.py
Settings
pytohn_project > newproject > random password generator.py > ...
window.title("Password Generator")
window.config(padx=50, pady=50, bg="#383e56")
label_title = Label(text="Password Generator",
bg="#383e56",
fg="#c5d7bd",
font=("Arial", 35, "bold"))
label_title.grid(row=0, column=0, columnspan=3, pady=30)
label_before_input = Label(text="I want a password with",
bg="#383e56",
fg="#c5d7bd",
font=("Arial", 15, "bold"))
label_before_input.grid(row=1, column=0,)
char_input = Entry(bg="#fb743e")
char_input.grid(row=1, column=1)
char_input.insert(0, "12")
char_input.focus()
label_after_input = Label(text="characters.",
bg="#383e56",
fg="#c5d7bd",
font=("Arial", 15, "bold"))
label_after_input.grid(row=1, column=2)
generate_password_button = Button(text="Generate Password & Copy to Clipboard",
bg="#fb743e",
height=4,
width=55,
command=password_generator)
generate_password_button.grid(row=2, column=0, columnspan=3, padx=50, pady=50)
password_field = Entry(bg="#383e56",fg="#c5d7bd",
Python 3.8.8 64-bit ('base': conda)
0 0
Live Share


random password generator.py
Settings
pytohn_project > newproject > random password generator.py > ...
label_before_input.grid(row=1, column=0,)
char_input = Entry(bg="#fb743e")
char_input.grid(row=1, column=1)
char_input.insert(0, "12")
char_input.focus()
label_after_input = Label(text="characters.",
bg="#383e56",
fg="#c5d7bd",
font=("Arial", 15, "bold"))
label_after_input.grid(row=1, column=2)
generate_password_button = Button(text="Generate Password & Copy to Clipboard",
bg="#fb743e",
height=4,
width=55,
command=password_generator)
generate_password_button.grid(row=2, column=0, columnspan=3, padx=50, pady=50)
password_field = Entry(bg="#383e56",fg="#c5d7bd",
font=("Arial", 15, "bold"), width=40)
password_field.grid(row=3, column=0, columnspan=3)
window.mainloop()
Python 3.8.8 64-bit ('base': conda)
0 0
Live Share

Chapter 3: Summary

3.1 : CONCLUSION

The password generated using alpha-numerical random password mechanism that was illustrated above is practical and can be used with great results. When the password is selected manually, most of the time, the users select the password that are related to himself or herself and related to any of the event. This gives the space for the intruders to deploy various attacks in breaking the passwords. The random generated passwords avoid this particular situation. One of the drawbacks could be the difficulty in memorizing the randomly generated password. But when comparing the security achieved through the randomly generated password, it is much preferable than the manually chosen password. The encryption and decryption standard provided here also strengthens the security measures. Since, the encryption and decryption standards are simple, it is cost effective. The above done work also creates awareness and interest to start exploring this field more

3.2 Advantages

- This online password generator solution is fully functional and flexible.
- It is very easy to use.
- It saves a lot of time, and secured as to hacking attacks.
- The software acts as an office that is open 24/7.
- It increases the efficiency of the management at offering quality services to the customers.
- It provides custom features development and support with the software.

3.3: FUTURE ENHANCEMENTS

Since all the applications are protected with passwords, more research can be accomplished for secured automatic password generations. The proposed method uses only the alphabets and numerical values for random character list. Still special symbols could be considered for strengthening the password. The password length also can be extended to make the password strong. New encryption and decryption standard could be implemented with the randomly selected passwords. The experimental study can be done with large number of samples in future.

References :

- www.stackoverflow.com
- www.w3schools.com
- www.slideshare.com
- www.codecademy.com