

PROJECT REPORT

on

Random Password Generator

(CSE III Semester Mini Project)

2021-2022



Submitted to:

Dr. Rakesh Patra

(CC-CSE-III -Sem)

Guided by:

Dr. Satvik

(Resource Persons)

Submitted by:

Manmohan Rajpal

Roll. No.: 37

CSE-B-III-Sem

Session: 2021-2022

DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

GRAPHIC ERA HILL UNIVERSITY, DEHRADUN

CERTIFICATE

Certified that Mr. Manmohan Rajpal(Roll No.-37) has developed mini project on “Random Password Generator” for the CS III Semester Mini Project in Graphic Era Hill University, Dehradun. The project carried out by Students is their own work as best of my knowledge.

(Dr. Rakesh Patra)

Class Co-ordinator

CSE-B-III-Sem

(CSE Department)

GEHU Dehradun

(Dr Satvik)

Project Guide

(CSE Department)

GEHU Dehradun

ACKNOWLEDGMENT

We would like to express our gratitude to The Almighty, the most Beneficent and the most Merciful, for completion of project.

I wish to thank our parents for their continuing support and encouragement. I also wish to thank them for providing us with the opportunity to reach this far in our studies.

I would like to thank particularly our project Co-ordinator Dr. Rakesh Patra and our Project Guide Dr. Satvik for his patience, support, and encouragement throughout the completion of this project and having faith in us.

We also acknowledge to teachers like Mr. Chandradeep who helped me in developing the project.

At last but not the least we are greatly indebted to all other persons who directly or indirectly helped us during this work.

Mr. Manmohan Rajpal

Roll No.- 2018471

Student ID: 20011019

CSE-B-III-Sem

Session: 2021-2022

GEHU, Dehradun

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
1.	INTRODUCTION	5
	1.1 Objective	5
	1.2 Overview	5
2.	PROJECT	6
	2.1 Requirements of Project	6
	2.1.1 IDE Software	6
	2.1.2 Prog. Language	6
	2.2 Snapshots	7
3.	Conclusion	8
	3.1 Summary	8
	3.2 Future Goals	8
	APPENDIX: Source Code	9
	REFERENCES	10

INTRODUCTION

1.1 OBJECTIVE

With growing technology, everything has relied on data and securing these data is the main concern. Passwords are meant to keep the data safe that we upload on the Internet.

An easy password can be hacked easily and all the personal information can be misused. In order to prevent such things and keep the data safe, it is quite necessary to keep our passwords very strong.

Let's create a simple application that can generate random password, with the combination of letters, numeric, and special characters. One can mention length of the password based on requirement and can also select the strength of the password.

1.2 OVERVIEW

In this project, the user has to select the password length and then click on the "Generate Password" button. It will show the generated password below. The user can also choose the strength of the generated password:

- "Low" is a combination of random lowercase letters and digits.
- "Medium" is a combination of random lowercase and uppercase letters and digits.
- "Strong" is a combination of random lowercase and uppercase letters, punctuation symbols and digits.

and if the user clicks on the "Copy to Clipboard" button, then it will copy the password automatically.

PROJECT

2.1 REQUIREMENTS OF PROJECT

2.1.1 IDE Software:

IDE stands for integrated development environment; it is a software that combines all the feature and tools needed by software developers. In this project, we have used PyCharm for compiling the programs.

2.1.2 Programming Language:

For the source code, Python programming language is used; developed by Python Software Foundation primarily by Guido Van Russom. Python is an interpreted high-level general-purpose programming language. Its design philosophy emphasizes code readability with its use of significant indentation. Its language constructs as well as its object-oriented approach aim to help programmers write clear, logical code for small and large-scale projects.

2.2 SNAPSHOTS:

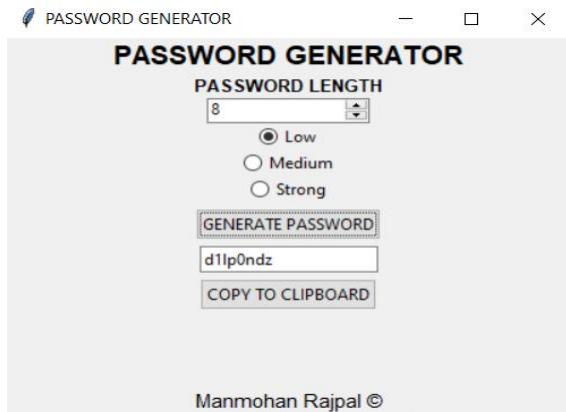


Fig. 1: Password Strength set to “Low”

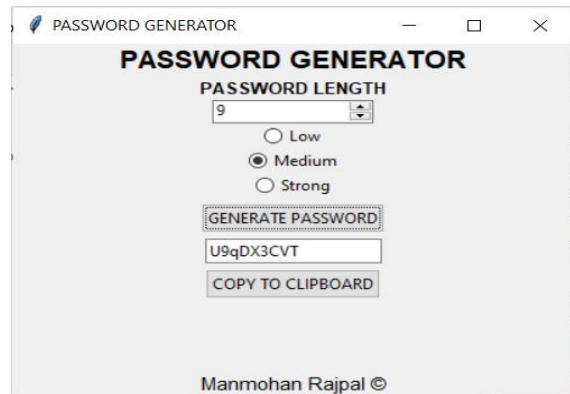


Fig. 2: Password Strength set to “Medium”

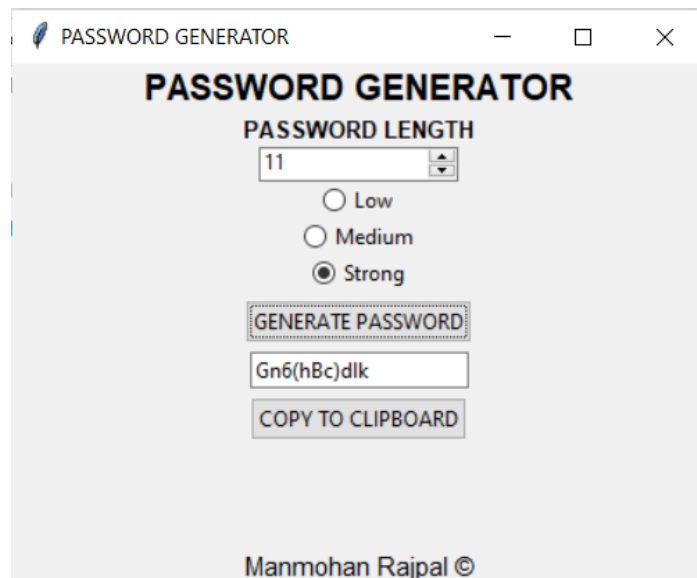


Fig. 3: Password Strength set to “Strong”

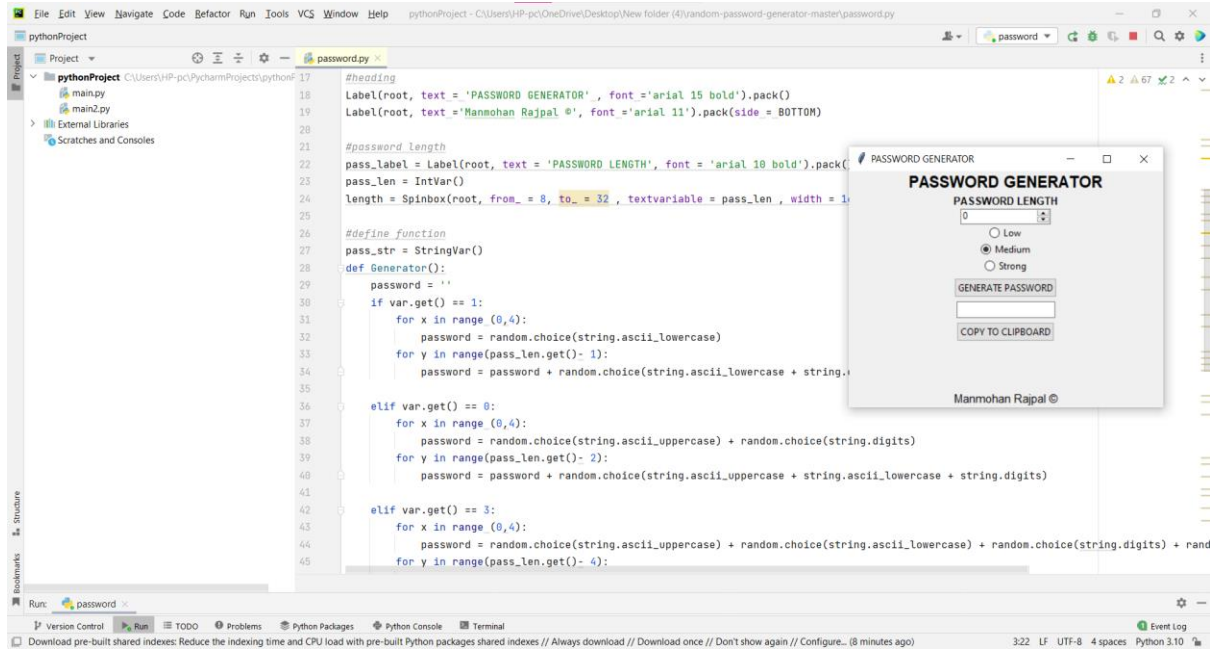


Fig. 4: Running application with Source Code

CONCLUSION

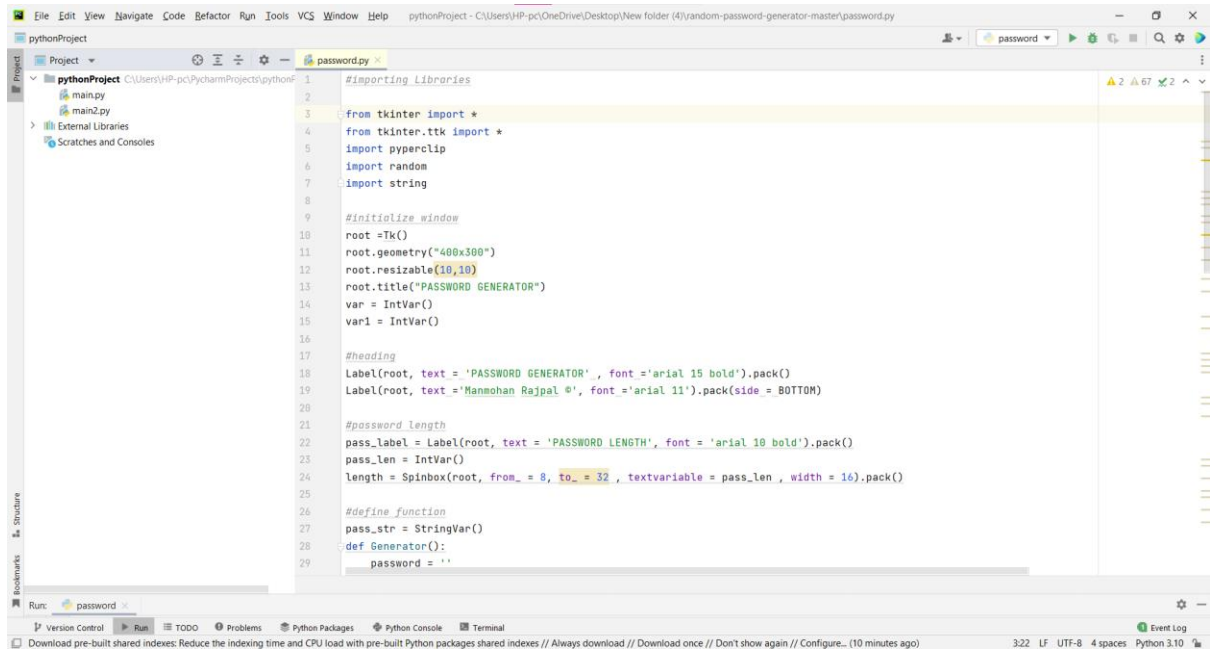
3.1 Summary:

Password generator is a Random Password generating program which generates a password mix of upper and lowercase letters, as well as numbers and symbols strong enough to provides great security.

3.2 Future Goals:

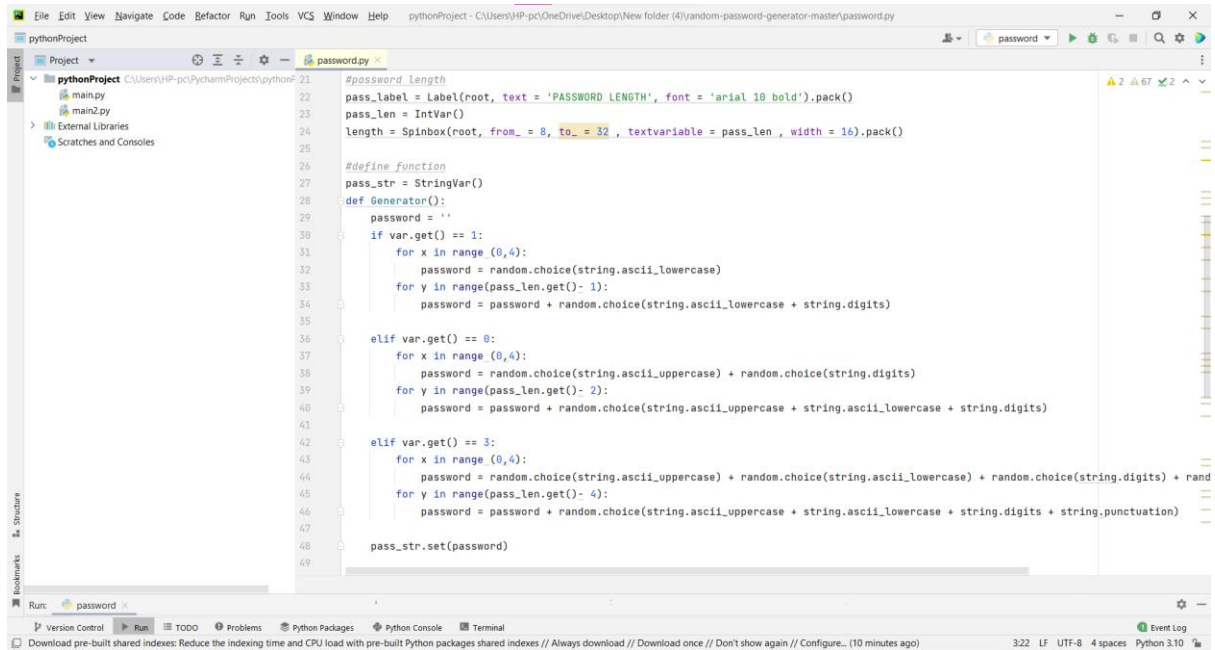
Future goals will include the password storing the generated passwords in a separate database and running a test to see if the newly generated password isn't the same as the previous generated passwords. The application will also have a separate timer that will remove the generated password within the limit.

Source Code



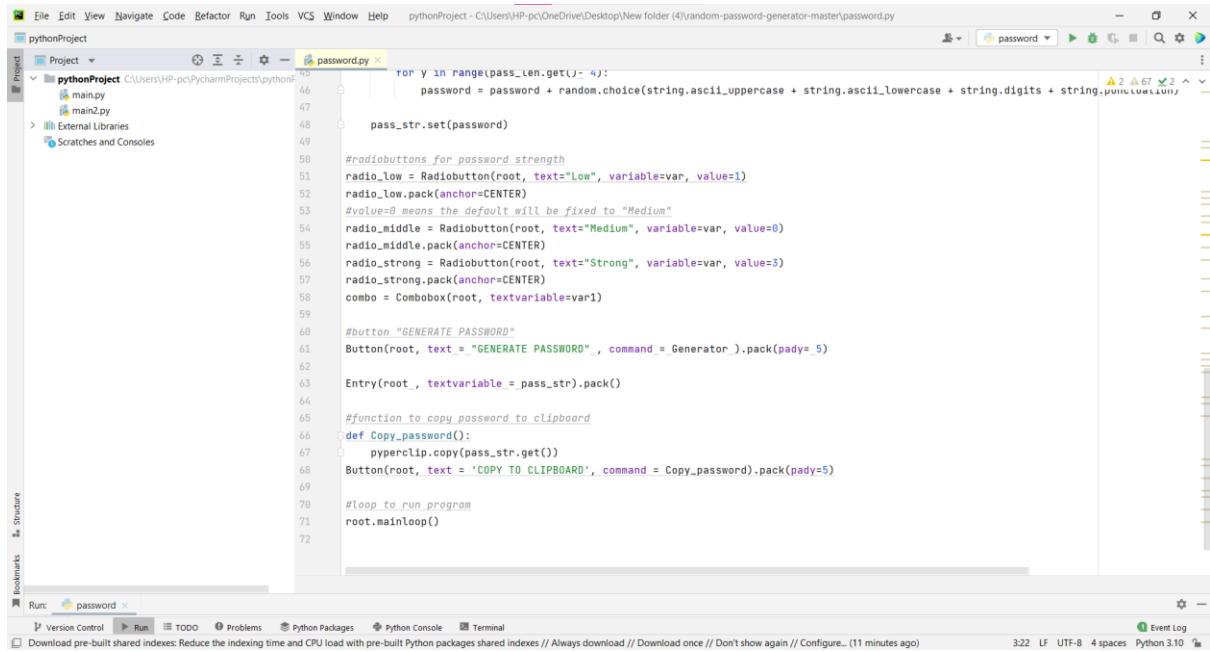
This screenshot shows the first 29 lines of the `password.py` file in an IDE. The code includes imports for Tkinter, ttk, pyperclip, random, and string. It initializes a Tk window titled "PASSWORD GENERATOR" with dimensions 400x300. A heading label is added. A spinbox for password length is created, ranging from 8 to 32. A function `Generator()` is defined, which initializes a password string.

```
1 #importing Libraries
2
3 from tkinter import *
4 from tkinter.ttk import *
5 import pyperclip
6 import random
7 import string
8
9 #initialize window
10 root = Tk()
11 root.geometry("400x300")
12 root.resizable(10,10)
13 root.title("PASSWORD GENERATOR")
14 var = IntVar()
15 pass_len = IntVar()
16
17 #heading
18 Label(root, text = 'PASSWORD GENERATOR', font = 'arial 15 bold').pack()
19 Label(root, text = 'Mamohan Rajpal ©', font = 'arial 11').pack(side = BOTTOM)
20
21 #password length
22 pass_label = Label(root, text = 'PASSWORD LENGTH', font = 'arial 10 bold').pack()
23 pass_len = IntVar()
24 length = Spinbox(root, from_ = 8, to_ = 32, textvariable = pass_len, width = 16).pack()
25
26 #define function
27 pass_str = StringVar()
28 def Generator():
29     password = ''
```



This screenshot shows the continuation of the `password.py` file, lines 21 to 49. The `Generator()` function is completed with logic to generate a password based on the selected length. It uses random.choice to select characters from lowercase letters, uppercase letters, and digits. The generated password is then set to the `pass_str` variable.

```
21 #password length
22 pass_label = Label(root, text = 'PASSWORD LENGTH', font = 'arial 10 bold').pack()
23 pass_len = IntVar()
24 length = Spinbox(root, from_ = 8, to_ = 32, textvariable = pass_len, width = 16).pack()
25
26 #define function
27 pass_str = StringVar()
28 def Generator():
29     password = ''
30     if var.get() == 1:
31         for x in range(0,4):
32             password = random.choice(string.ascii_lowercase)
33         for y in range(pass_len.get()- 1):
34             password = password + random.choice(string.ascii_lowercase + string.digits)
35
36     elif var.get() == 0:
37         for x in range(0,4):
38             password = random.choice(string.ascii_uppercase) + random.choice(string.digits)
39         for y in range(pass_len.get()- 2):
40             password = password + random.choice(string.ascii_uppercase + string.ascii_lowercase + string.digits)
41
42     elif var.get() == 3:
43         for x in range(0,4):
44             password = random.choice(string.ascii_uppercase) + random.choice(string.ascii_lowercase) + random.choice(string.digits) + rand
45         for y in range(pass_len.get()- 4):
46             password = password + random.choice(string.ascii_uppercase + string.ascii_lowercase + string.digits + string.punctuation)
47
48     pass_str.set(password)
49
```



REFERENCES

- Get Programming, Learn to code with Python by Ana Bell
- Geeks For Geeks
- YouTube
- docs.python.org
- Reference Book – PYTHON PROGRAMMING by Reema Thareja