*Week 4 Progress Report on password Manager*

UpSkill Campus, UniConverge Technologies Pvt.Ltd.

Submitted by: VADDIREDDY SWAPNA

Correspondence Address: VADDIREDDY SWAPNA

Madanapalle Institute of Technology and Science, Department of Computer Science and Engineering, Angallu, Andhra Pradesh, 517326,

India.

Mail: [vswapna788@gmail.com](mailto:vswapna788@gmail.com)

Phone: +91 9603689259

**Overview**

During the fourth week,I took my step towards the source code of my project work,I am almost there to complete my project this is the last step to my project

Tasks Completed

As the implementation have three stages

* Configure
* Add new entries
* Get entries

Get Entries:

* Input the field to search for. Like site name, site url, email, username
* Display all the entries that match the search. Password hidden by default.
* It user chooses to get the password (with p flag), then
* Ask for MASTER PASSWORD
* Validate MASTER PASSWORD by hashing and checking with existing hash
* Make hash(DEVICE SECRET +MASTER PASSWORD) =Master key
* Decrypt the password and copy to the clipboard

This task has been completed

Challenges Faced

* This week is really better , as I am good enough to deal with sql(rows & columns)
* As always this week motives me with some errors

Lessons Learned

Overall, the lessons learned from the "Password Manger" project highlighted the importance of data security and it is a real-world application. These insights will guide us in future projects and contribute to our professional growth.

Code progress

from utils.dbconfig import dbconfig

from rich import print as printc

from rich.console import Console

from rich.table import Table

def retrieveEntries (mp, ds, search, decryptPassword = False):

db = dbconfig()

cursor = db.cursor()

query = ""

if len(search) == 0:

query = "SELECT FROM pm.entries"

else:

query = "SELECT FROM pm.entries WHERE

for i in search:

query+= "{i} = ‘{search[1]}’ AND "query query [:-5]

cursor.execute(query)

results = cursor.fetchall()

if len(results) == 0:

printc("[yellow][-][/yellow] No results for the search")

return

if (decryptPassword and len(results)>1) or (not decryptPassword):

table Table (title="Results") table.add column ("Site Name")

table.add\_column("URL",)

table.add column("Email")

table.add column("Username")

table.add\_column("Password")

for i in results:

table.add\_row(i[0], i[1],i[2], i[3], "{hidden}")

console = Console()

console.print(table)

return

if len(results)==1 and decryptPassword:

mk = computeMasterkey (mp, ds)

decrypted = utils.aesutil.decrypt (key-mk, source=results[0][4], keyType="bytes")

pyperclip.copy(decrypted.decode())

printc("[green] [+] [/green] Password copied to clipboard")

db.close()