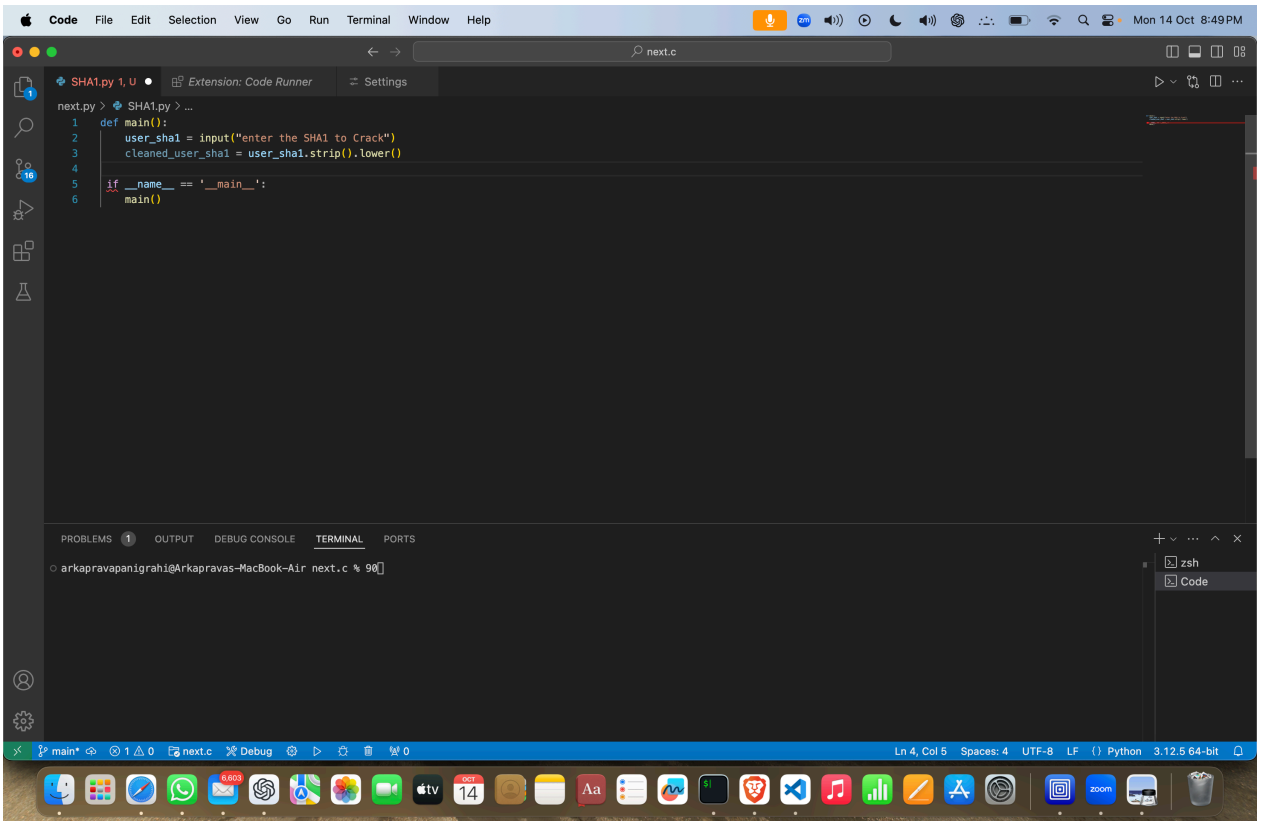
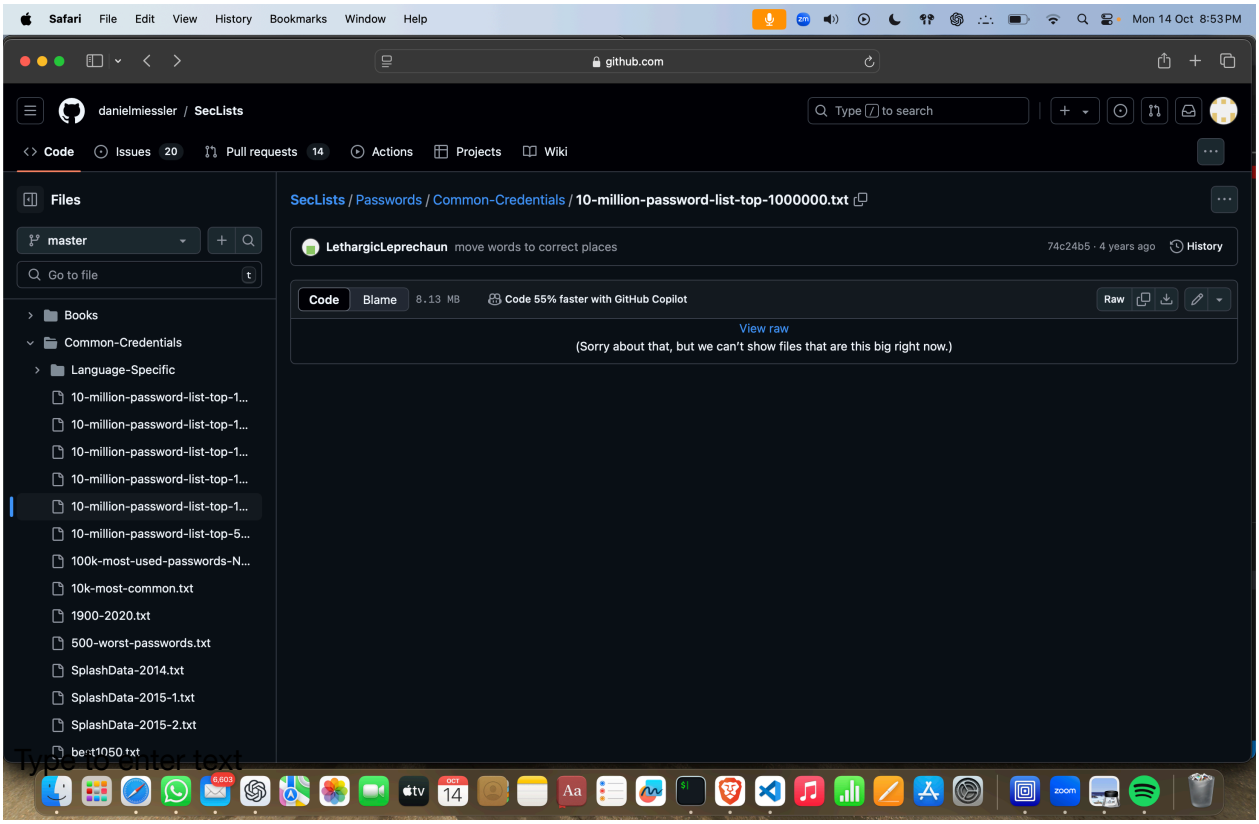
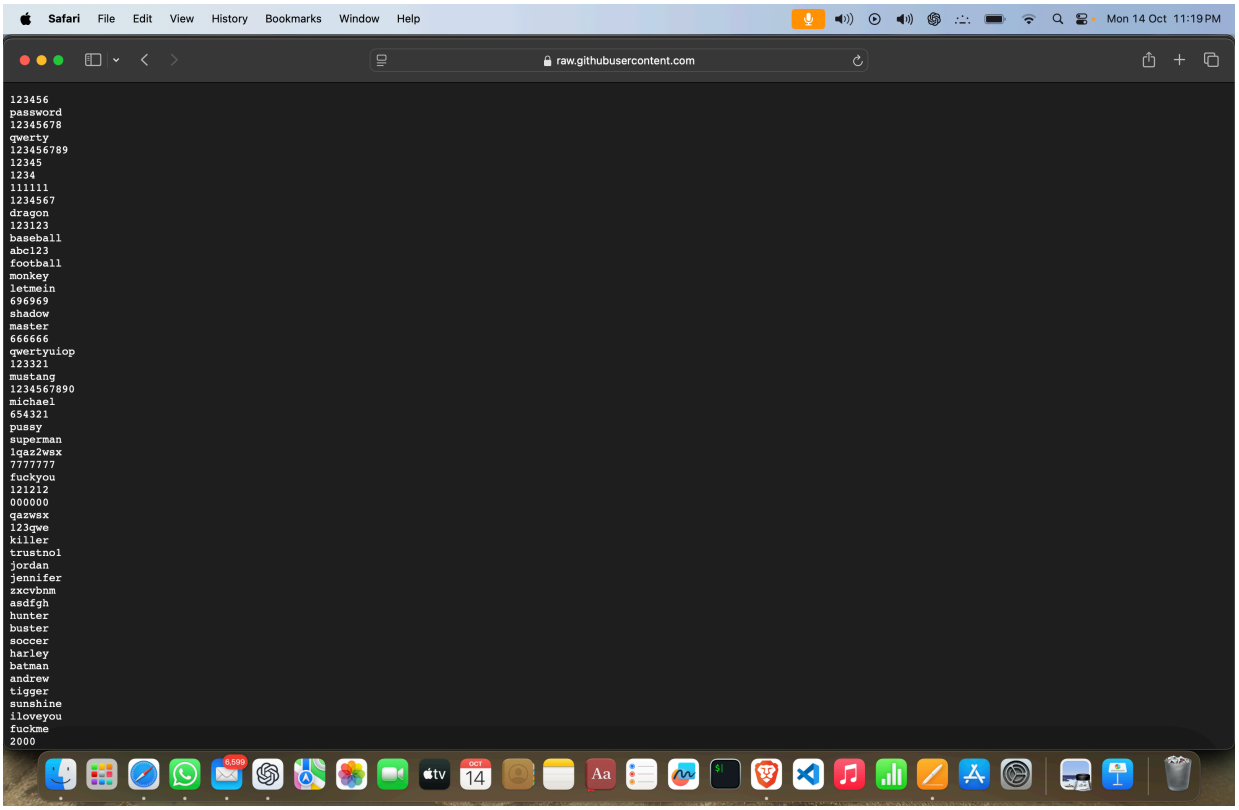
SHA1 Password Exploitation in Python



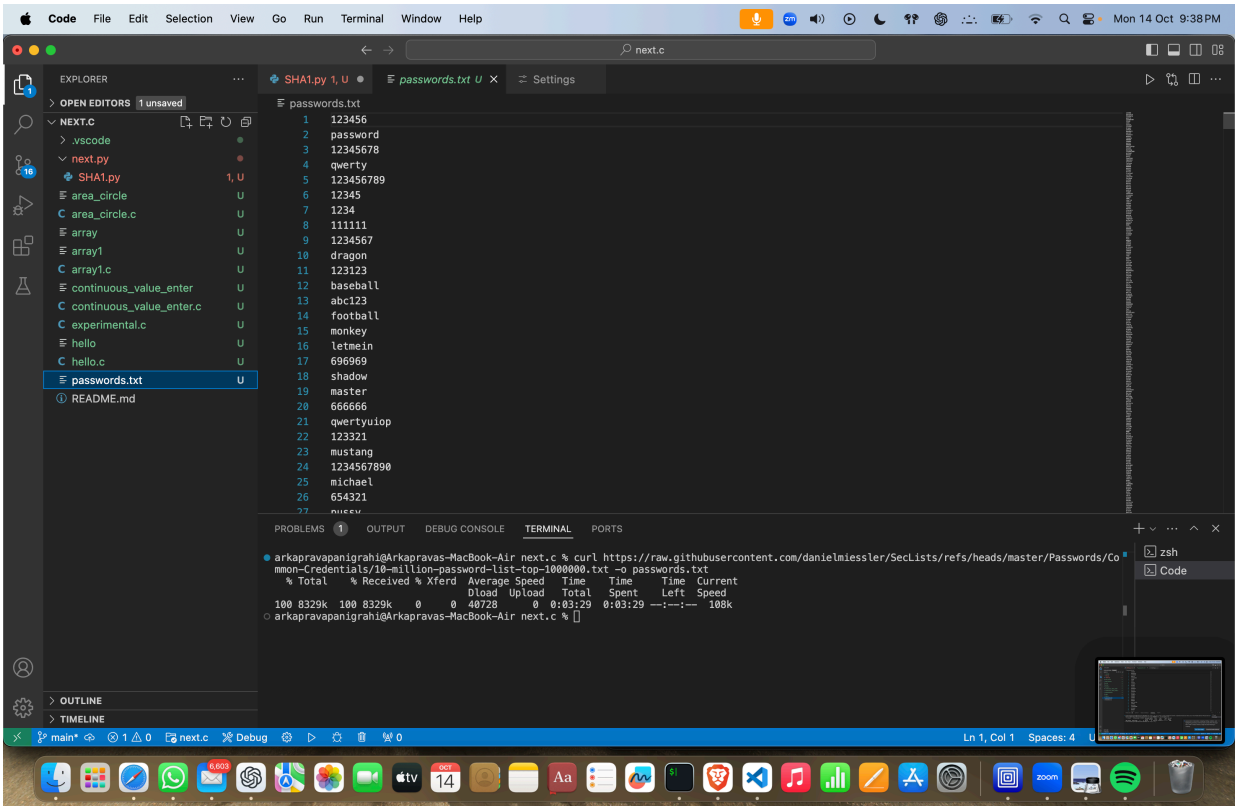
1. To exploit SHA-1 hash vulnerabilities in passwords using Python , first we have to write a code that is a SHA-1 hash cracker that takes a user-provided SHA-1 hash and compares it against the SHA-1 hashes of passwords in a file (passwords.txt). It reads each password from the file, hashes it, and checks if it matches the given hash. If a match is found, it prints the corresponding password; otherwise, it reports that the password could not be found.



2. We search for a password file in the internet that contains many passwords for testing



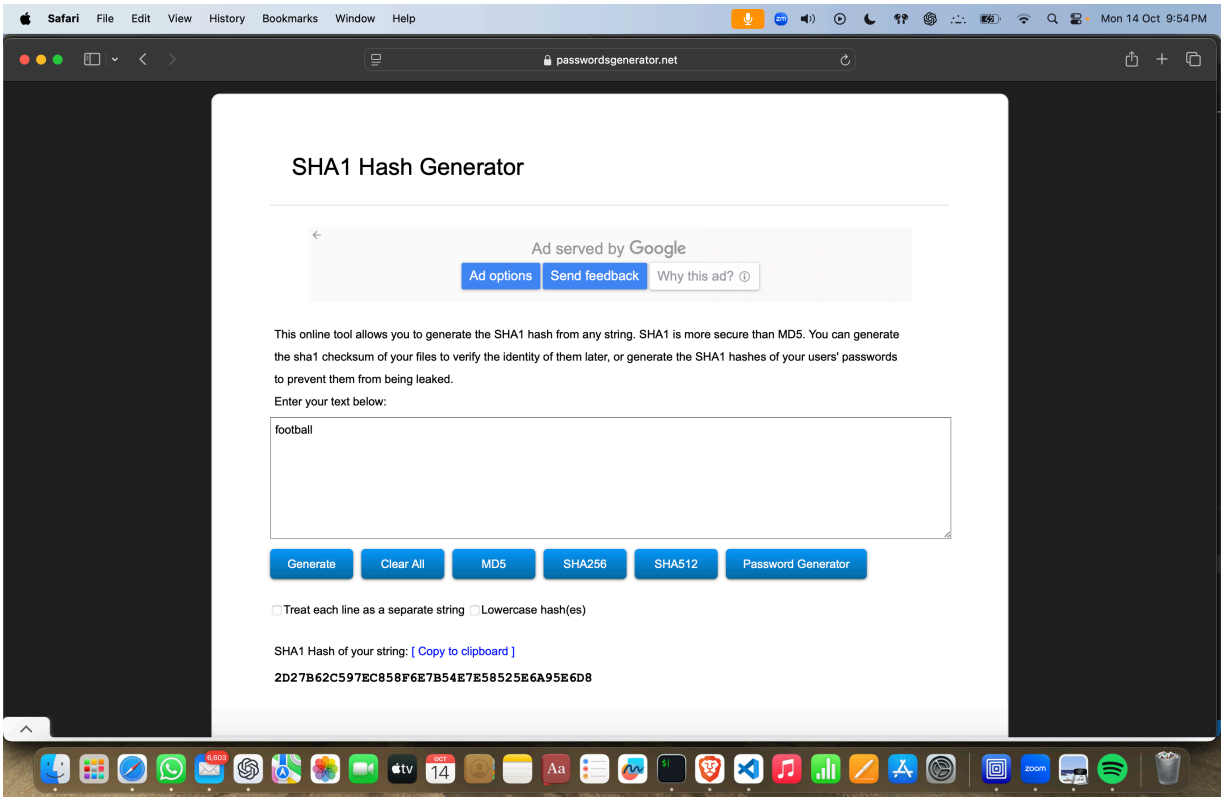
3. We can select any one password from the password list , here we select password football for the testing purpose.



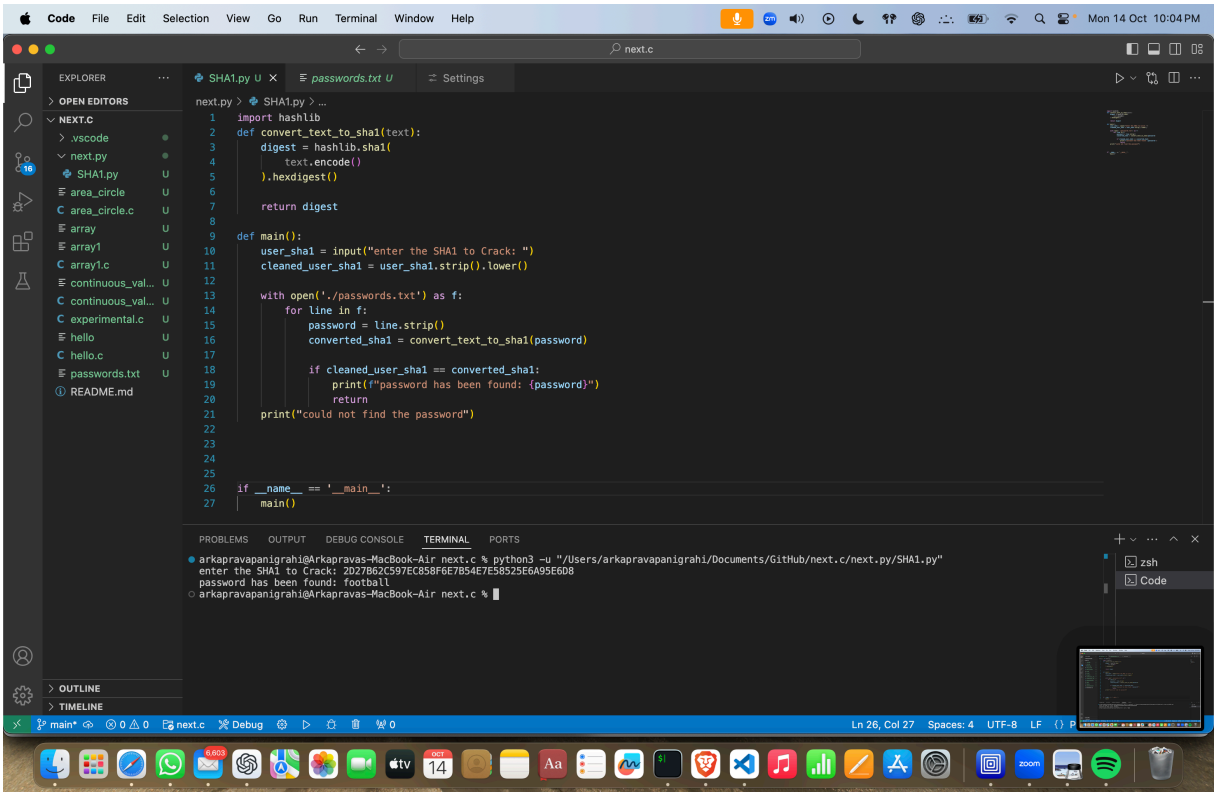
4. Then we download the password list by using curl command in the terminal of VS code

The command used - curl https://raw.githubusercontent.com/danielmiessler/SecLists/refs/heads/master/Passwords/Common-Credentials/10-million-password-list-top-1000000.txt -0 passwords.txt

Here we use -o command to rename the file as password.txt



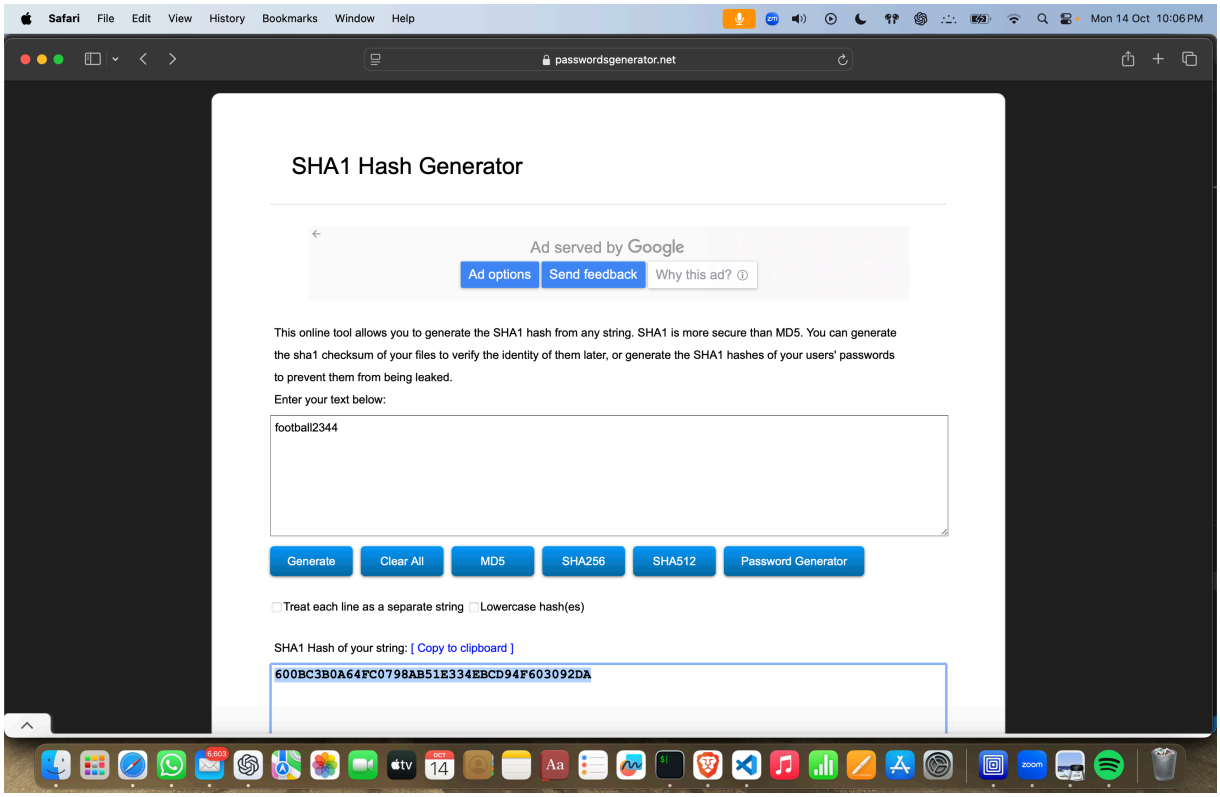
5. We go to the hash generator to generate a SHA1 hash for the selected password- football for verification purpose



6. Next we run the code and we input the SHA1 hash of football that we got from the hash generator website

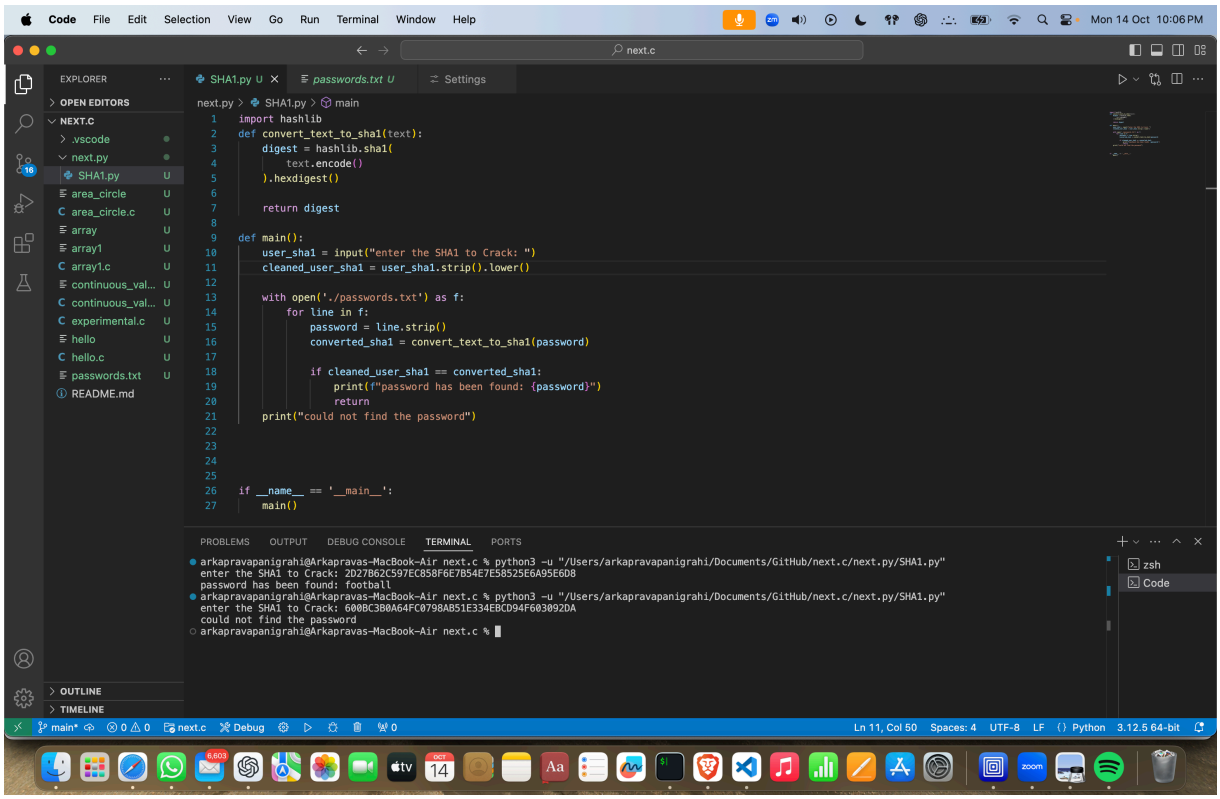
The hash is verified with all the passwords present in the password list and finally the hash matches with password- football

This signifies that out code is working properly



7. Now we are going to reverse verify it , we are going to generate SHA1 hash of a password that is not present in the password list

Hare it is football2344 , this password is not present in password list



8. We are going to run the python code again and we are going to enter the SHA1 hash of the password football2234. The code gives a output “could not find the password” , as the particular password football2344 is not present in the password list

This proves that our code for SHA1 password exploration in python is working properly.