TECH CLUB

Code Crack Conquest- Mains

Answer any Five Questions

1. Take a password string as input and returns its SHA-256 hashed representation as a hexadecimal string.

2. Generate random passwords of a specified length. The function takes an optional parameter length, which is set to 8 by default. If no length is specified by the user, the password will have 8 characters.

3. Check if a password meets the following criteria:
    a. Atleast 8 characters long and contains at least one uppercase letter, one lowercase letter, one digit, and one special character (!, @, #, $, %, or &).
    b. If the password meets the criteria, print a message that says "Valid Password." If it doesn't meet the criteria, print a message that says "Password does not meet requirements."

4. Creates a password strength meter. The program should prompt the user to enter a password and check its strength based on criteria such as length, complexity, and randomness. Afterwards, the program should provide suggestions for improving the password's strength.

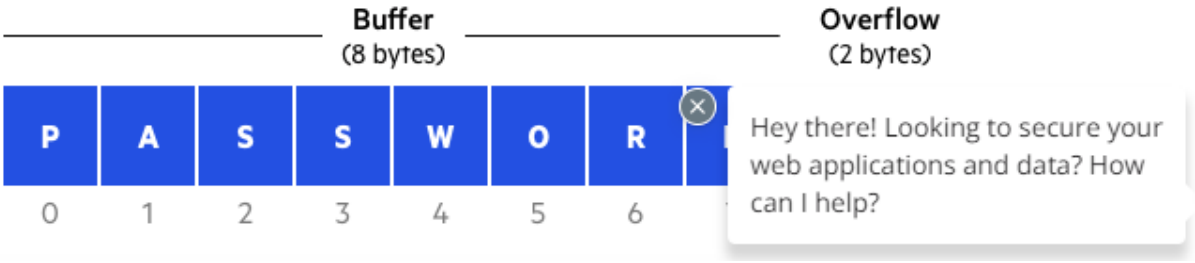
5. Perform encryption for a given input text using the substitution techniques Ceaser cipher and to perform **brute force attack to** decode the encoded data don't use decryption Ceaser cipher.

6. Write a script which reads a four digit integer entered by the user in a prompt dialog and encrypt it as, replace each digit by the sum of that digit plus 7 modulus 10 and then swap the first digit with the third, and second digit with the fourth. Then output the encrypted one time pad data.

   Write a separate script that inputs an encrypted integer and decrypts it to from the original number.

   (Note only one time is used and it is never used after one minute time is expired please show all these validations also)

7. Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.



The programming languages **C ,C++, JAVA, Python** Which are buffer overflow attack/Buffer overrun exploits generated can you validate with specified fragment of code and how to prevented buffer overflow attack/Buffer overrun. Please specify the defense mechanism program code and validate it.