VishwaCTF

CHALLENGE NAME : [SANDESE AATE HAI]

DEV : [YOHAAN DHURI & PUSHKAR DEORE]

CATEGORY : [REVERSE ENGINEERING]

LEVEL : [MEDIUM]

2024

Description:

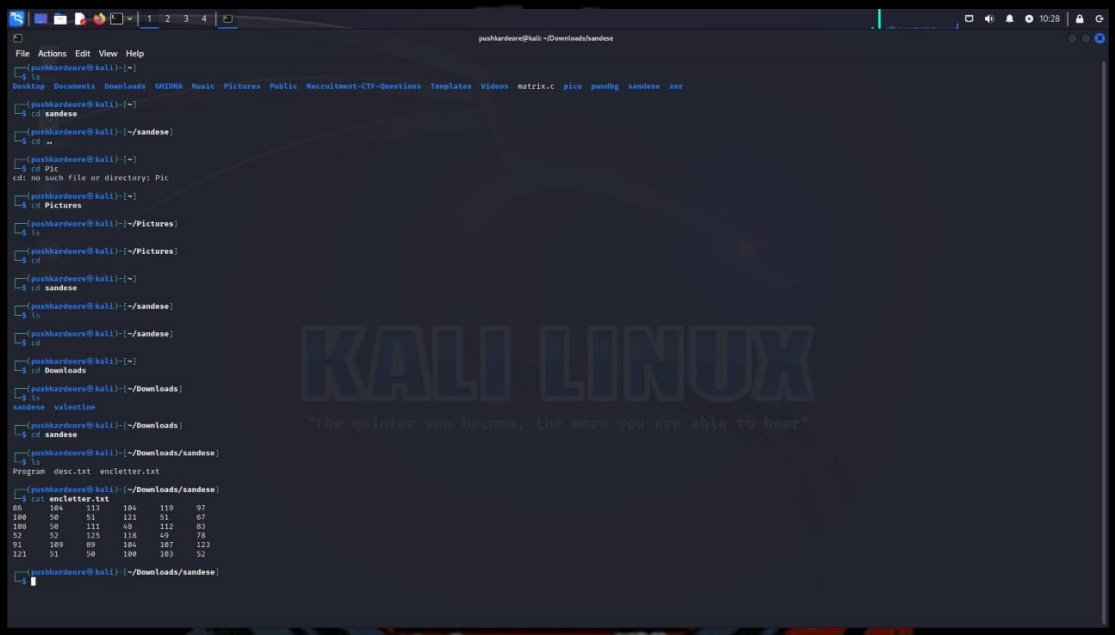
A friend pranked me by encrypting my letter but gave me the program by which he encrypted it. Can you help me decrypt it?

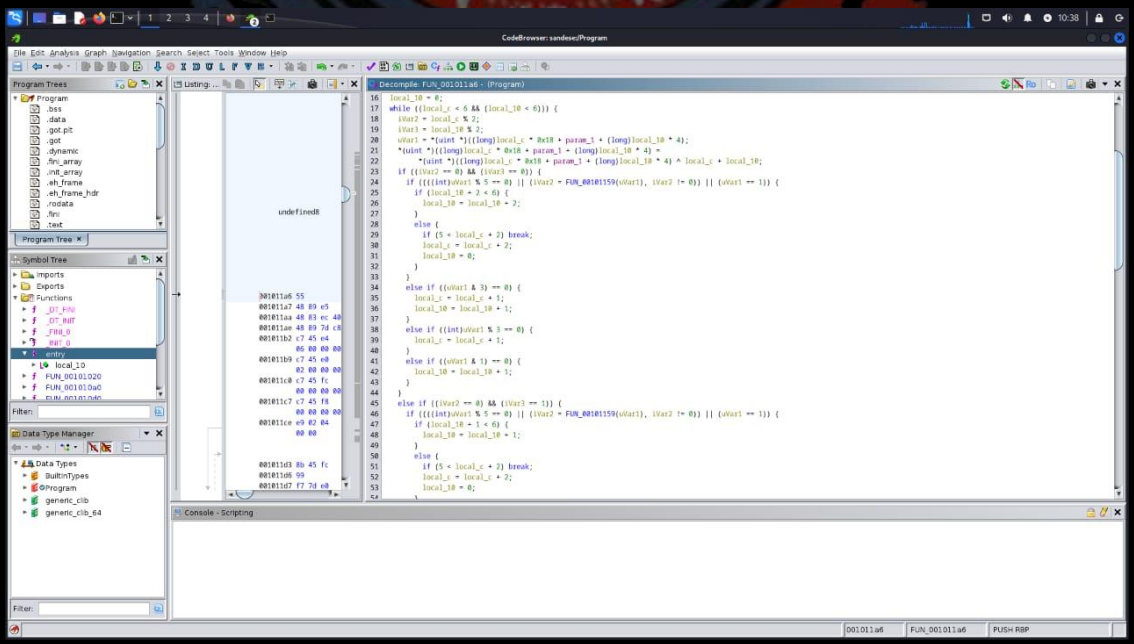
Flag:

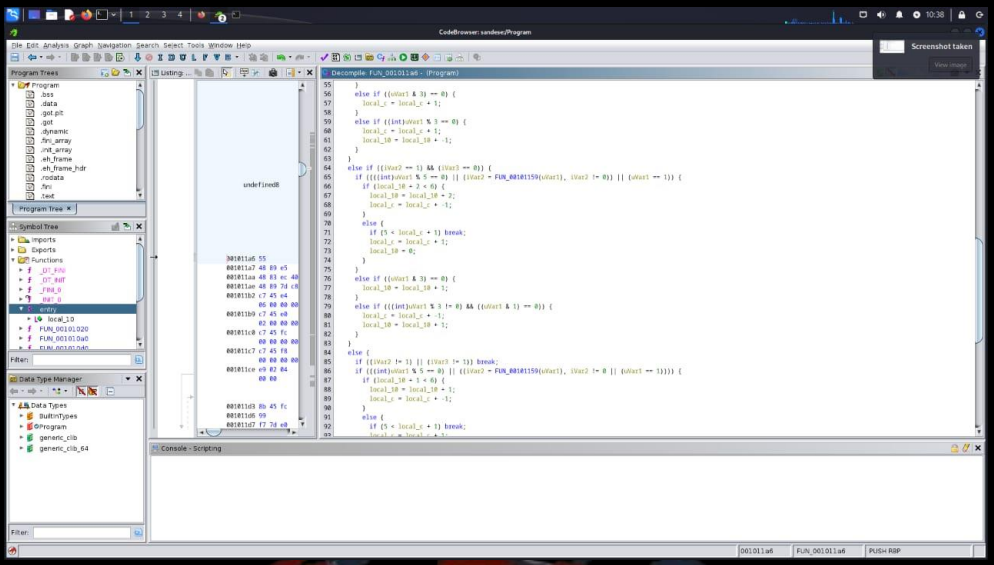
VishwaCTF{4nd23y_4nd23y3v1ch_m42k0v}

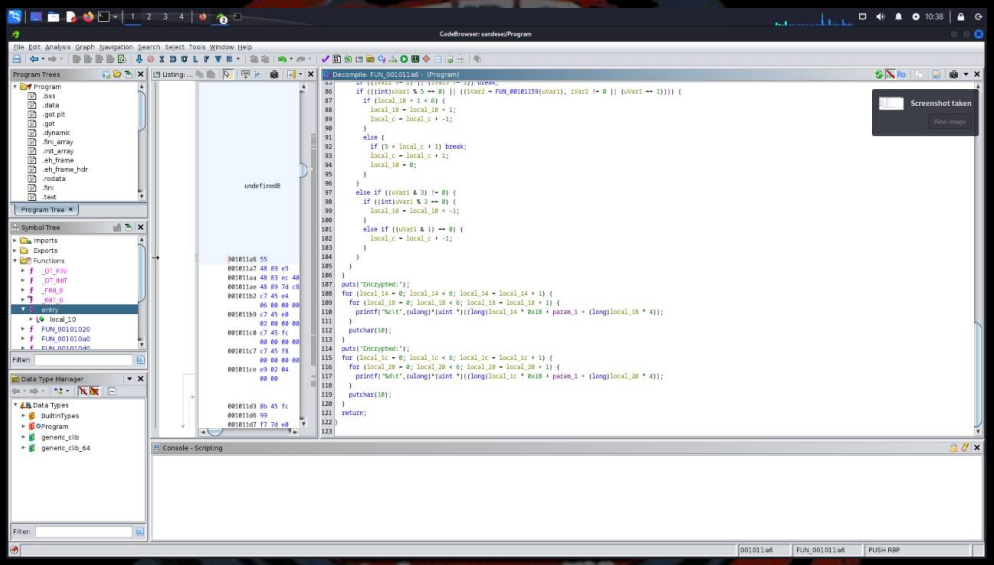
Solution:

In this challenge we are given an encrypted txt file in the form of a 2D square array. We are also given a program by which the encryption happened. We have to understand the code and reverse it to decrypt the encrypted file to get original txt and possibly our flag.









When you open the code in Ghidra, you will find a lot of if else statements. These were the if else statements which were used to encrypt the file.

When we understand the code, we realise that this code depends on whether the given element is prime, divisible by 2, 3, 5. This is a form of Markov chain which decides its next state depending on divisibility of current elements. Once we reverse the code, we get the decrypted 2D matrix in spiral form and fortunately our flag.

This is what we obtain in the last step: