JASMINE C. OMANDAM
[picoCTF - picoGym Challenges]

Reverse

Medium | Reverse Engineering | picoCTF 2023

AUTHOR: MUBARAK MIKAIL

Description

Try reversing this file? Can ya?

I forgot the password to this file. Please find it for me?

Hints

(None)

16,376 users solved

72% Liked

picoCTF{FLAG}

Submit Flag

Write-Up: REVERSE

I started by running the binary, but instead of just interacting with it blindly, I wanted to peek inside. The first clue came from simply inspecting the file with `strings`. Right away, I saw familiar phrases:

“Enter the password to unlock this file” and “Password correct, please see flag.” That told me the program was checking user input against some hidden value.

Curious, I dug deeper. I opened the binary in a disassembler and followed the execution flow. The program used `scanf` to read my input, then compared it with a hardcoded string using `strcmp`. That was the key moment I realized the correct password wasn’t something I had to guess; it was already embedded inside the binary.

Scrolling through the disassembly, I noticed chunks of ASCII characters being moved into registers. Piece by piece, they formed something recognizable. And then it hit me: the flag was right there, spelled out in the instructions.

The binary wasn’t trying to hide it very well it was just waiting for me to notice. The full flag appeared as:

picoCTF{3lf_r3v3r5ing_succe55ful_7851ef7d}

I tested it by running the program and entering that exact string. Sure enough, the program confirmed: “Password correct, please see flag.”

Reflection

In the end, the challenge wasn’t about brute-forcing or guessing it was about looking inside the binary and realizing the answer was already there. By tracing the logic and spotting the embedded string, I unlocked the flag. It felt like uncovering a secret message hidden in plain sight.Honestyly this is my easiest challenge that I’d encounter.