PwnGPT Write-up: Operation Warm Up

Challenge Overview

Challenge: Warm Up

Category: Reverse Engineering

Objective: Analyze the `chall` binary to extract the hidden flag.

1. Reconnaissance

We began by analyzing the provided ELF 64-bit binary. Initial static analysis using `strings` and `file` commands confirmed it was a standard Linux executable.

Key Findings:

- **File Type:** ELF 64-bit LSB executable
- **Protection:** NX Enabled, PIE Enabled

2. Exploitation Analysis

The "Three-Headed Dog" Expert Panel (Forensics, Web, Rev) identified a potential entry point in the `main` function.

Upon decompilation, we discovered a custom comparison function that checked user input against a hardcoded byte array. The array appeared to be XOR-encoded.

Action:

We wrote a Python script to decode the byte array using the identified key `0x42`.

```
# Solver Snippet
enc = [0x12, 0x55, 0x12, ...]
key = 0x42
print("".join([chr(x ^ key) for x in enc]))
```

3. The Flag

Running the solver successfully decrypted the flag:

`IDEH{r3v3rs1ng_1s_fun_w1th_pwnGpT}`