CSAW - LLM

Suriya Prakash Jambunathan - sj3828
Krishnan Navadia - kn2501

pwn/target_practice

Observation:

The challenge provides us with a binary that asks for user input (address), and executes code at that address.

Approach:

1. Observe the binary using Ghidra.
2. Observe the main function for vulnerabilities in the script to exploit.
3. Identify the string that will result in executing the “cat_flag” function.
4. Extract the printed flag.

Solution:

1. Prompted ChatGPT to give a python code for steps 2-3 in the Approach.

```
0x00400717
```

Flag: *csawctf{y0ure_a_m4s7er4im3r}*
Chat: *CSAW LLM - target_practice (openai.com)*