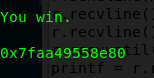
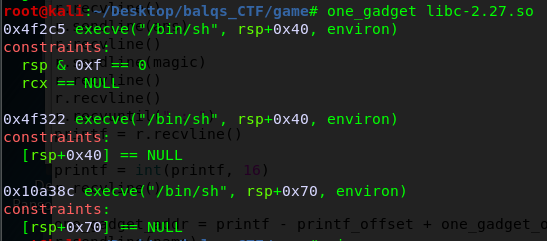
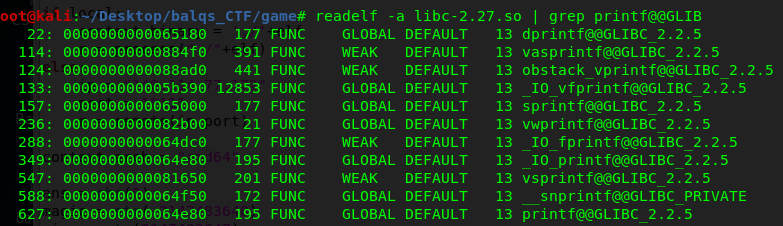
**game**

Account : stanleymusic

Writeup :

* Step 1
  + The third argument of strncmp is strlen(ans), while ans is the input. That means we can decide the length that we need to compare.
  + Use NULL to pass the strncmp by sending chr(0)
* Step 2
  + Since abs() function use 2’s complement to calculate absolute, abs(-2147483648) = -2147483648. Thus, magic = -2147483648
* Step 3
  + Get the address of printf
  + 
  + Use one-gadget to calculate the offset
  + 
  + Since we cannot meet the first condition, we use 0x4f322
  + Then use readelf to get the offset of printf
  + 
* Step 4
  + Use IDA to find out the size of payload
  + 
  + 
  + It needs 0x3F0 + 0x08(rbp) to overflow return address
  + Thus send ‘A’\*1016 + p64(printf\_addr – print\_offset + gadget\_offset)
* Step 6
  + Get the flag
  + 