



Capture The Flags

NAMA TIM	SMKN 22 Jakarta
ANGGOTA	Muhammad Arsyah Al Bassam
	Sholahuddin Muhammad Athar

Reverse Engineering

Challenge : 🧒 Level 1 - Baby Steps

Halo, selamat datang di challenge Reverse Engineering Level 1!

Disini Anda diminta untuk memasukkan input sebuah **flag** dari suatu program biner ELF (File Executable dari distro OS Linux).

Dapatkah kamu mendapatkan **flag** yang tepat?

Author: Felix (aseng)

File: babyRE

Answer

saya langsung mencoba membukanya pada ghidra dan menemukan buffer pada function tersebut

```
char local_38 [48];
```

kemudian saya coba jalankan dengan ltrace dan mencoba melewati buffer tersebut dan muncul

```
(kali@kali)-[~/Desktop/CTF/dki]
└─$ ltrace ./babyRE
puts("Welcome to RE LKS 2023! Just wan"...Welcome to RE LKS 2023! Just want
to check your sanity, input the flag:
) = 73
__isoc99_scanf(0x5619b1771051, 0x7ffd82ba7b10, 0, 0x7ff6e5c0aad0aaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
) = 1
strlen("aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"...) = 48
strcmp("aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"... , "LKS{baby_r3_baby_ELF_just_str
ing"... ) = 21
puts("The flag is still incorrect :(."The flag is still incorrect :(."
) = 32
exit(0 <no return ... >
+++ exited (status 0) +++
```

kemudian saya jalankan dengan gdb line per line dan menemukan string lengkap

```
00:0000  rsp 0x7fffffffdd90 -> 0x7fffffffdf18 -> 0x7fffffff28f -> '/home/kali/Desktop/CTF/dki/babyRE'
01:0008  0x7fffffffdd98 -> 0x100000000
02:0010  0x7fffffffdda0 -> 'LKS{baby_r3_baby_ELF_just_strings}'
03:0018  0x7fffffffdda8 -> '_r3_baby_ELF_just_strings}'
04:0020  0x7fffffffddb0 -> '_ELF_just_strings}'
05:0028  0x7fffffffddb8 -> 't_strings}'
06:0030  0x7fffffffddc0 -> 0x7d73 /* 's}' */
07:0038  0x7fffffffddc8 -> 0x0

[ BACKTRACE ]
▶ 0 0x555555551ce main+85
1 0x7ffff7deb6ca __libc_start_call_main+122
2 0x7ffff7deb785 __libc_start_main+133
3 0x555555550b1 _start+33

pwndbg> █
```

langsung saja saya mendapatkan flag lengkap
flag = LKS{baby_r3_baby_ELF_just_strings}

Binary Exploitation

Challenge : 🐣 Step 2

CTRL+C -> CTRL+V

nc 52.221.234.73 11102

Author: Stanley (enryuzz)

View Hint

bagaimana cara merubah file elf kedalam code c ? walaupun gak persis tetapi bisa dibaca

View Hint

bener bener melihat semua code

file = chall

Answer

sesuai dengan hint saya langsung me-decompile dengan ghidra dan menemukan call function yang aneh pada opsi 6 / exit

```
    case 6:
        puts("Exiting the program.");
LAB_00101850:
        secret();
    }
```

kemudian saya langsung melihat pada function secret dan terdapat strcmp

```
printf("Input password : ");
getss(local_58);
iVar1 = strcmp(passw,local_58);
if (iVar1 == 0) {
    local_c = 0;
```

langsung saya jalankan file chall pada local dengan ltrace dan mendapatkan string yang hendak di compare

```
printf("Input password : "Input password : )
fgets(awdawdwd
"awdawdwd\n", 60, 0x7f8519871aa0)
strlen("awdawdwd\n")
strcmp("E2haASL0v9qAY7D", "awdawdwd")
puts("Invalid choice. Please select a "...Invalid choice. Please select a valid option.
```

dan ketika saya lakukan netcat dengan menginputkan string comparison yang telah didapat saya mendapatkan hasil

```
(kali@kali)-[~/Desktop/CTF/dki]
└─$ nc 52.221.234.73 11102
) while( true );
Linked List Operations:
1. Push Back
2. Push Front
3. Pop Back
4. Pop Front
5. Print List
6. Exit
Enter your choice: 6
Exiting the program.
Input password : E2haASL0v9qAY7D
lsk{step-2_flag_jchyhnfudshfu3734}Invalid choice. Please select a valid option.
```

dan mendapatkan string flag

flag = lsk{step-2_flag_jchyhnfudshfu3734}