LKS SMK

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)

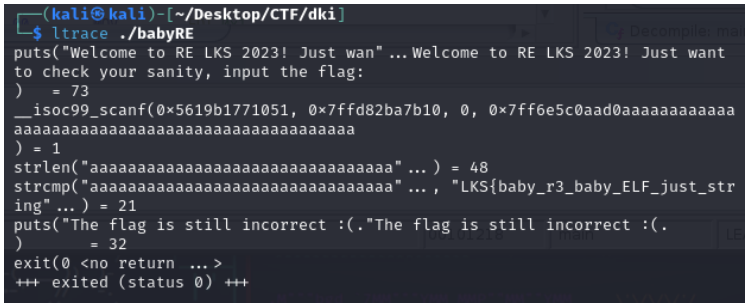
File: babyRE

Answer

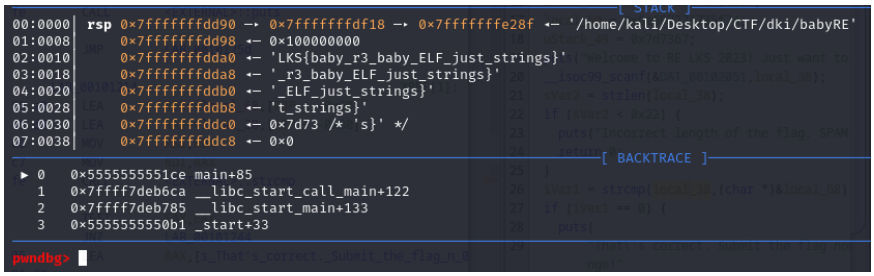
saya langsung mencoba membukanya pada ghidra dan menemukan buffer pada function tersebut

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

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



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



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(awdawdawd
"awdawdawd\n", 60, 0x7f8519871aa0)
strlen("awdawdawd\n")
strcmp("E2haASL0v9qAY7D", "awdawdawd")
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

dan mendapatkan string flag

flag = lsk{step-2_flag_jchyhnfudshfu3734}