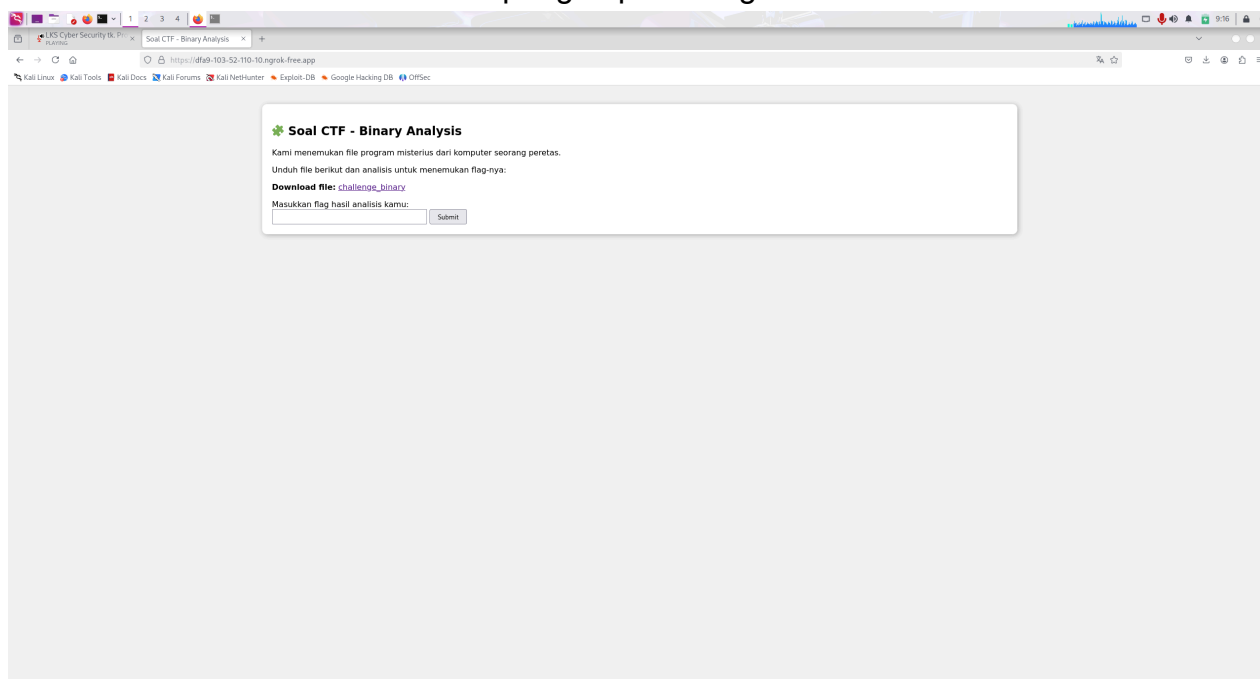


SMK_HARAPAN BANGSA_Depok_CTF_SOAL_6_CTF_Stabil

CTF Binary Exploite — challenge_binary

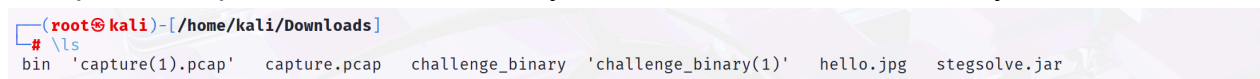
Deskripsi Soal

Oke pada soal ini kita disuruh untuk menemukan `flag{}` dari file `challenge_binary` dan memasukkan ke dalam kolom pengumpulan flag.



Tahap 1: Download & Cek File




Oke pada tahap ini kita download filenya lalu kita cek di terminal file-nya.



Tahap 2: Analisis Awal pakai file

Nah lanjut, jadi pada tahap ini kita akan mencari informasi tentang `challenge_binary` tersebut dengan tools yang bernama `file`.

Informasi yang didapatkannya itu seperti:

-  **Jenis File**
-  **Arsitektur File**
-  **Endianness:**
 - LSB: byte yang disimpan nilainya **paling kecil**
 - MSB: byte yang disimpan nilainya **paling besar**

```
(root@kali)-[/home/kali/Downloads]
# file challenge_binary
```

```
challenge_binary: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=1820ecac93ad75248c6677b95b720bd009a40017, for GNU/Linux 3.2.0, not stripped
```

Tahap 3: Ubah Permission

Nah di tahap ini kita ubah permission-nya menggunakan perintah:

```
chmod +x challenge_binary
```

Bertujuan agar file `challenge_binary` tersebut bisa dieksekusi, karena default-nya dia belum bisa.

```
(root@kali)-[/home/kali/Downloads]
# chmod +x challenge_binary
```

Tahap 4: Eksekusi & Coba Input Manual

Oke nah sampai pada tahap ini saya mencoba untuk menjalankan si file `challenge_binary` -nya lalu saya disuruh untuk memasukkan flag-nya.

Nah di sini saya coba masukkan input `abc` dan ternyata salah.

```
(root@kali)-[/home/kali/Downloads]
# ./challenge_binary
```

```
Masukkan flag: abc
X Jawaban salah!
```

Tahap 5: Gunakan `ltrace` untuk Reversing

Nah oke langkah terakhir: Ini **jalanin binary-nya dengan library tracing (`ltrace`)**:
Bisa ngintip **fungsi library C** apa aja yang dipanggil saat program jalan.

Dan inilah titik kuncinya dalam reversing **tanpa perlu bongkar kode source-nya langsung**.

★ **BOOM!** Sebuah kata yang diinginkan muncul yaitu si flagnya:

```
flag{reversing_is_fun}
```

```
(root@kali)-[/home/kali/Downloads]
# ltrace ./challenge_binary

printf("Masukkan flag: ")                                = 15
__isoc99_scanf(0x402014, 0x7ffc00713590, 0, 0Masukkan flag: abc
)                                                         = 1
strcmp("abc", "flag{reversing_is_fun}")                  = -5
puts("\342\235\214 Jawaban salah!"X Jawaban salah!
)                                                         = 19
+++ exited (status 0) +++

(root@kali)-[/home/kali/Downloads]
# strcmp("abc", "flag{reversing_is_fun}") = -5

zsh: number expected

(root@kali)-[/home/kali/Downloads]
#
```

✓ Tahap Akhir: Submit Flag

Oke dan terakhir kita submit , selesai.

