Untuk challenge babyrop1.0, saya langsung mencoba menjalankan programnya untuk menemukan clue yang diberikan. Ketika program sudah dijalankan, program memberikan informasi clue berupaya berapa padding yang harus dibuat untuk melakukan buffer overflow dan juga return address yang mau di overwrite untuk memanggil fungsi yang memberikan flag jawaban. Setelah itu, saya membuat file input berupa padding dan juga return address fungsi win. Tujuan pembuat hal tersebut adalah membuat program memanggil fungsi win secara paksa dengan mengoverwrite return address fungsi mainnya sehingga program menjalankan fungsi win dan memberikan flagnya. Dengan memanfaatkan file “hex2raw.py” yang pernah diberikan ketika praktikum orkom, input hex tadi dapat diubah menjadi raw untuk dimasukan ke dalam stdout program challenge dengan memasukan command “python hew2raw.py | /challenge/babyrop\_level1.0” pada terminal workspace. Flag pun berhasil didapatkan.

Untuk challenge babyrop2.0 ada sedikit tambahan usaha, yaitu menggunakan gdb dan melakukan disas kepada fungsi-fungsi yang memberikan flag karena ketika program dijalankan clue yang diberikan hanya berupa jumlah padding yang harus dibuat untuk melakukan buffer overflow. Karena flag terbagi kedalam dua fungsi, proses pencarian flag dilakukan dengan cara melakukan eksekusi dua kali, yaitu untuk memperoleh flag dari fungsi win\_stage\_1 (overwrite return address fungsi diisikan return address fungsi win\_stage\_1) dan fungsi win\_stage\_2. Setelah itu, kedua potongan flag hanya perlu disatukan menjadi sebuah fla