**郭又嘉**

**AosoraKuo**

**B06705020**

[**IDAmudamudamuda**](https://edu-ctf.csie.org/problems/8)

首先將執行檔用IDA PRO反編譯

簡單看過一遍之後發現function 4012F0是最主要的

而他底下有三個function 401000，401070，401270

401000用靜態看出來是取出dll內各種函式的function

再來輸入seed然後打它丟進一個長長的function

最後輸入flag再把它丟進401270裡面

然後發現401270其實是把flag丟到記憶體裡的4058的function裡面

用動態慢慢跑發現seed可以將4058開始的值加上自己

而根據opcode，function最後一個值應該要是c3也就是ret

再用原本在40A8上的值b3推算出seed = 16

再繼續用動態跑轉換出來的function之後發現

輸入的flag加上23再xor 66之後要等於4018上開始的32個值

經過運算之後便得到FLAG