楊力行 b06705001 b06705001

用 ida pro 打開看，發現他在接收完第一個的輸入後，會先呼叫 sub_401070 做一些事，接著接收到第 2 個的輸入後會呼叫 sub_4012F0 函數，而在這個函數中會 call 記憶體位置 404058，也就是把由 404058 開始的當作是 shellcode 執行，並且是把 404018 之後 32 個值作為參數傳入，並回傳結果，接著我用 X64DBG 進行動態偵錯，首先先隨意輸入數字，發現在 sub_401070 中，他會先把 404018 的值進行變動，變動的值為固定的與輸入的數字無關，之後，他會從 404058 開始，把之後的每個記憶體位置中的數值都加上所輸入的數值，找到被最後修改的值原本是 B3，而在這個 shellcode 裡，最後的值應該是 ret 的機器碼也就是 C3，因此第一個輸入的數值應為 16，接著重新開始，先輸入 16，接著在輸入 32 個字元，因為他會檢查輸入的長度，接著，進入 call 記憶體位置 404058 裡面，發現他是把我的輸入的 32 個字的 ascii 值分別加上 0x23 再和 0x66 XOR 後再跟記憶體位置為 404018 開始的 32 個值進行比較，不一樣就 break，全部一樣的話就會 print 出得到了 flag，因此我直接把記憶體位置為 404018 開始的 32 個值取出來，寫一個 XOR_sub.py 檔將他們各自先和 0x66 XOR 後再減掉 0x23 接著 print 出來，即可得到 flag。