[hw0x02] writeup

莊翔旭, woolninesun, b04902083

simplebox

先觀察 data，發現 data 後段有 = 符號，猜測是 base64 後的結果，拿去 encode，發現是一段神祕文字。之後在用 gdb trace code 的時候發現在 401978 位置上的 switch 有對應到左移、右移、輸入、輸出這些動作，判斷神祕文字是 brainfuck 的程式碼，簡單地判斷後依據下列對應關係轉換

```
a => 0x401768 => '<'
m => 0x401788 => '+'
b => 0x4017a8 => '-'
x => 0x401863 => ']'
B => 0x401748 => '>'
F => 0x401808 => '['
O => 0x4017e8 => ','
o => 0x4017c8 => '.'
```

將轉換出來的 brainfuck code 丟到 https://copy.sh/brainfuck/ 執行看看發現可以 work (印出 try hard!)，之後就將 brainfuck code 轉成 c code，將一樣的 code 整理，會發現每讀入一個字就會去比對，所以就將比對數字算出來，算出來的數字(dec)都轉成 ascii，就拿到 flag 了