**郭又嘉**

**AosoraKuo**

**B06705020**

**Open my backdoor**

打開門之後發現一個d00r.php

看完程式碼之後算出 $c = #

然後要GET的東西必須是四個字母

四個字母在php要呼叫shell的只有exec

於是透過計算與d00r的XOR算出要GET的東西是 %01HU%11

在網址後面加 ?87=%01HU%11 之後把他丟到postman裡

再開一個requestbin接傳出去的東西

於是在 # 裡面丟各種不同的指令

最後用在指令裡面丟cd ~ 在根目錄找到flag\_is\_here

Cd進去之後得到FLAG

**M4chine**

先在一串emu.e\_start裡面的動作前加上b讓他變成bytes的狀態

開弄一個檔案print出每一行self.op[i[0]](i[1])裡的i[0]、i[1]

在讀完上面程式碼之後從第一個開始用手算

用很多變數加減得到一串數字

最後經過ASCII比對之後得到FLAG

**Encrypt**

看懂程式碼之後寫一個反向解密的程式碼

Stage0的部分因為之中會回傳的值是經過XOR的而XOR對同一個數字做兩次會恢復原狀所以不用重寫

Stage1的部分op2也是一樣XOR所以不用重寫

op3和op4則用數列模擬然後推著寫回去

然後把所有可能的key丟進去跑

就可以在亂碼海之中得到FLAG