Impossible

Author : wayneOuO | 吳崇維 | B06902058

Problem Description

程式首先會讀入一個將要讀入的長度，若是小於0則取用絕對值，接著若是大於0x100則強制改為0x100，藉此來控制read的長度。

Solution

洞在於如果我們輸入 0x80000000 這個數字，則進入abs之後，出來的數值依然一樣(因為找不到相應的正值)，此時他是負數，不大於0x100，也可以繞過，最後的read讀進去的參數又是unsigned的型態，所以可以達到 stack overflow，有了overflow之後就簡單的ROP就結束了。