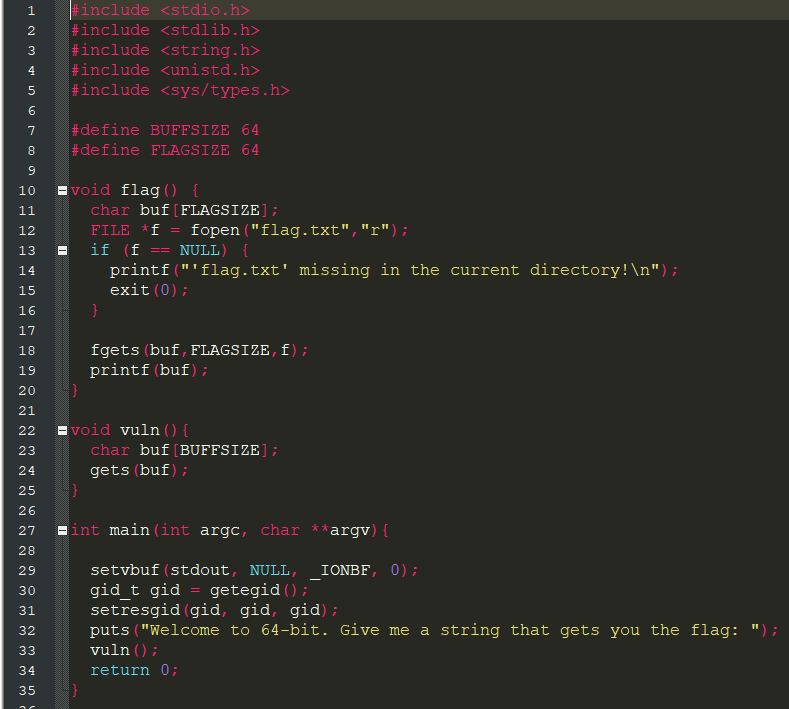
NewOverflow 1

1. Đọc hiểu source code:



Đề bài cho gồm 3 hàm chính:

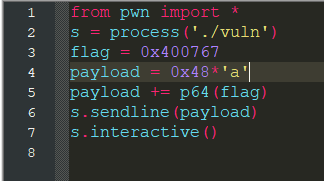
* Flag ( ) : dùng để lấy flag
* Vuln( ) : cho nhập vào 1 mảng kí tự có len = 64
* Main( ) : gọi hàm vuln.

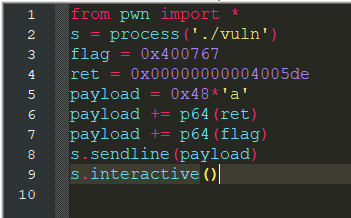
Rất đơn giản, không có gì nhiều để phân tích.

1. Tìm lỗi và khai thác:
   1. Tìm lỗi:

* Để ý trong hàm vuln, gets( ) cho nhập vào buf mà không check độ dài của chuỗi nhập vào, xảy ra lỗi buffer overflow.
  1. Khai thác:
* Ý tưởng:

Chúng ta có hàm flag, như bài overflow-1, chúng ta có thể ghi đè địa chỉ return thành địa chỉ hàm flag để lấy flag.

* Khai thác:
  + Tìm khoảng cách ( offset) và địa chỉ hàm flag rất đơn giản, các bạn tự tìm. Ở đây mình tìm ra offset = 0x48 và flag\_address = 0x400767
  + Code :
  + 
  + Vì một lí do nào đó mà code ở trên dù đúng và mình chạy local thành công nhưng lên server thì lại không được. Nên mình đã dùng thêm 1 chuỗi ROP thì lại chính xác và lấy được flag.



1. Flag:

