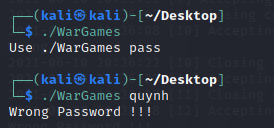
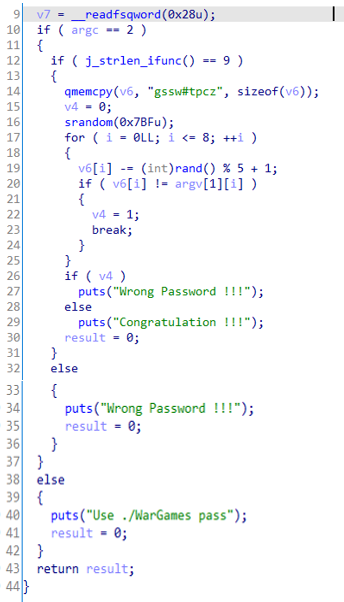
*Nguyễn Mỹ Quỳnh 19520241*

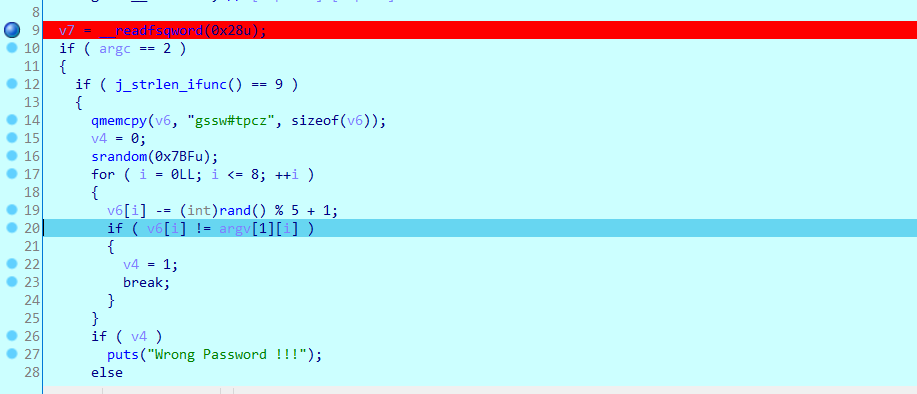
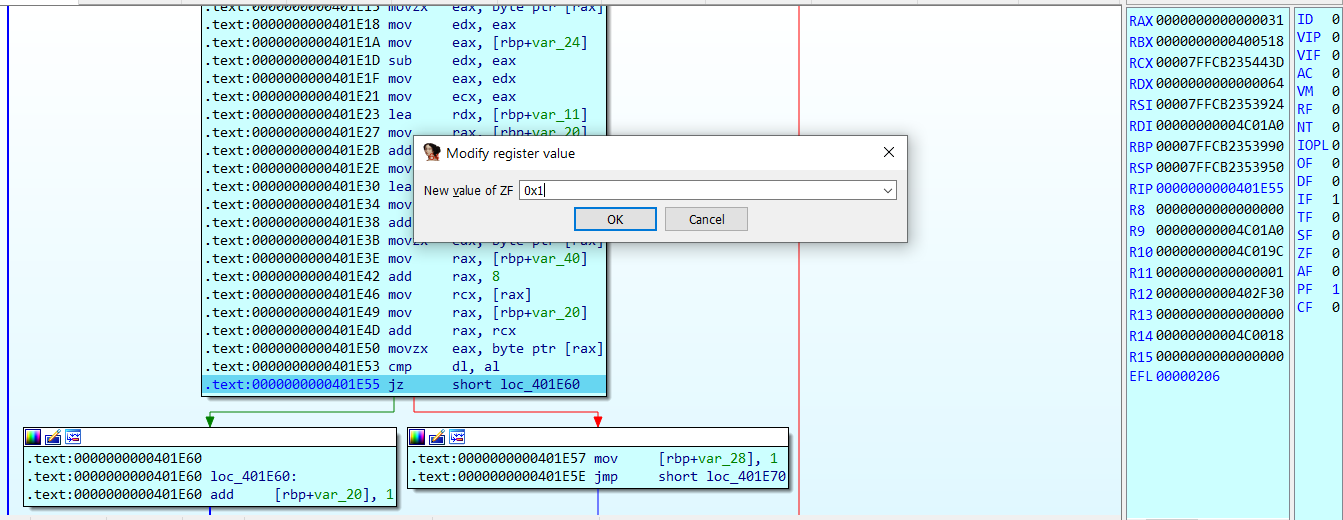
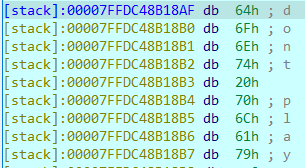
**WarGames**

Chạy thử chương trình

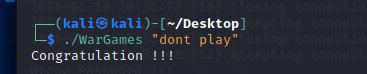
****

Đọc mã giả của chương trình ta thấy chuỗi ta mong muốn nằm ở dòng 29. Để đến được đó , cần vào được if ở dòng 10 (kiểm tra việc truyền tham số khi chạy chương trình, nếu không truyền in ra “Use ./WarGames pass”), cần vào được if ở dòng 12 (kiểm tra chuỗi nhập vào phải có độ dài là 9). Ta thấy ở dòng 26 v4 cần = 0 thì dòng 29 mới được thực hiện. Ban đầu dòng 15 gán v4=0. Từ dòng 17 đến dòng 25 thực hiện so sánh chuỗi v6 và chuỗi ta nhập vào, nếu khác kí tự nào thì v4 sẽ bằng 1 ngay. Vì vậy đặt breakpoint ngay dòng 9 để debug để tìm chuỗi v6.

****

****Ta nhập chuỗi input là “quynh” và tại dòng 20 ta sẽ sửa cờ ZF = 1 để chương trình không chạy vào dòng 22 (có thể xem mã assembly tương ứng khúc này khi debug để rõ hơn), làm tương tự cho 8 lần duyệt 8 kí tự còn lại, sau đó ta nhấp vào v6 để xem giá trị v6. 

Kiểm tra:

****