1. integer overflow

2. integer underflow

3. Out of bound Read

4. Out of bound Write

5. Double Free

6. Use After Free

7. Memory leaks

file generate là 28 byte nghĩa là input sẽ là 28 byte

đọc 1 file ta thấy input sẽ bắt đầu với dr4g0n

dùng ida để phân tích file trong hàm main thì ta thấy có 1 hàm là start\_quest

đi vào hàm này ta thấy có các giá trị là secret được đưa vào vào vector

ta thấy giá trị đầu là 100 đó là giá trị ascii của ký tự "d" và nó cũng giống như giá trị mà ta đã fuzz ra được. Có vẻ như là AFL đã fuzz ra được flag.

và ta thấy có quy tắc đó là các giá trị được đưa vào vector sẽ là tổng tích lũy của các giá trị ascii của flag

ví dụ

giá trị đầu là giá trị ascii của "d" là 100 và ta cũng biết ký tự tiếp theo là "r" với mã ascii là 114 thì 100+114=214 và tương tự ký tự tiếp theo ta cũng biết là "4" với mã ascii là 52 thì 214+52=266 đó cũng là những giá trị được đưa vào vector