# **fatBoy**

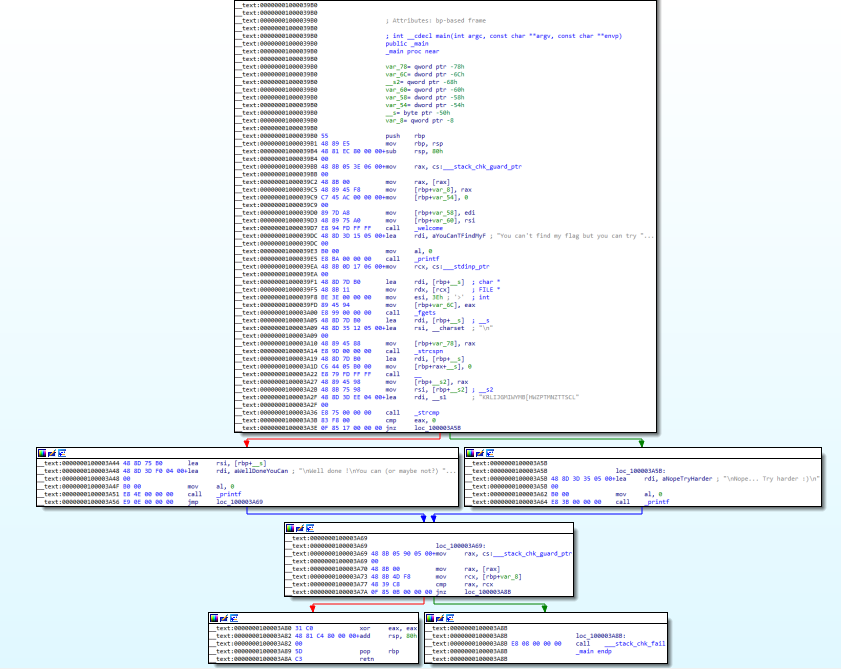
You'll never find my flag.

Format : Hero{}

Author : SoEasY

Đây là một challenge của [Heroctf](https://www.heroctf.fr/) ,các bạn có thể tải các challenge khác ở đây [githup](https://github.com/HeroCTF/HeroCTF_v3) của BTC heroctf

Load file fatBoy vào IDA thì có 2 arch cho mình lựa chọn đó là x86\_64 và Arm64,mình sẽ chọn x86\_\_64 bởi vì intel assembly is the best ^^ : 

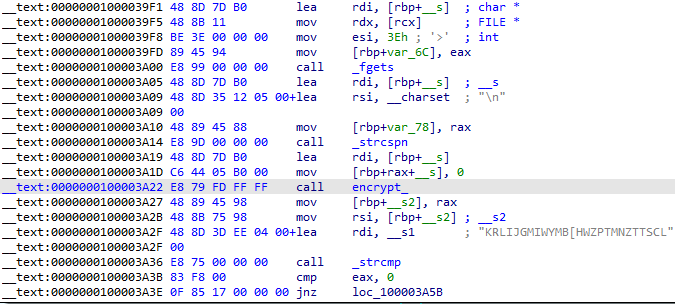


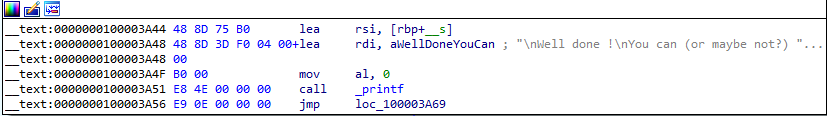
Bài này cũng không có gì quá nhiều nó thực hiện đọc file và lưu fake flag vào [rbp+\_s].

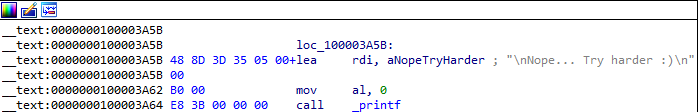
Tiếp theo tính độ dài fake flag trừ kí tự xuống dòng “\n” bằng hàm strcspn() kí tự “\n” được thay thế 0.

Tiếp tục thực hiện encypt fake flagencypt tại hàm encrypt\_() rồi so sánh với real flag đã bị encrypt ”KRLIJGMIWYMB[HWZPTMNZTTSCL” .

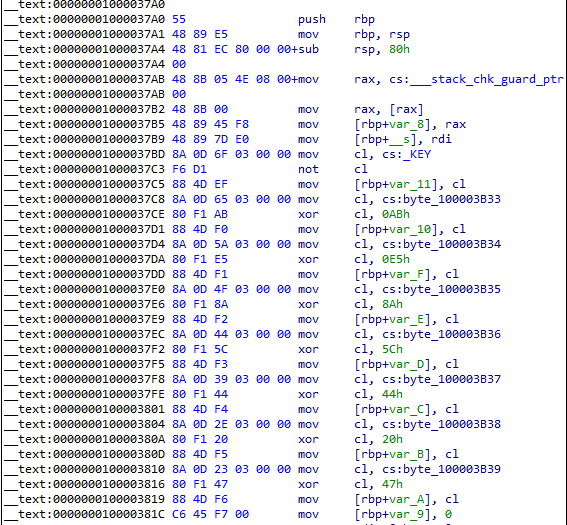
Vậy nếu bằng nhau thì các bạn biết nó làm gì rồi đấy và ngược lại nó in dòng “Nope... Try harder :)”.





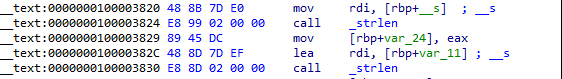


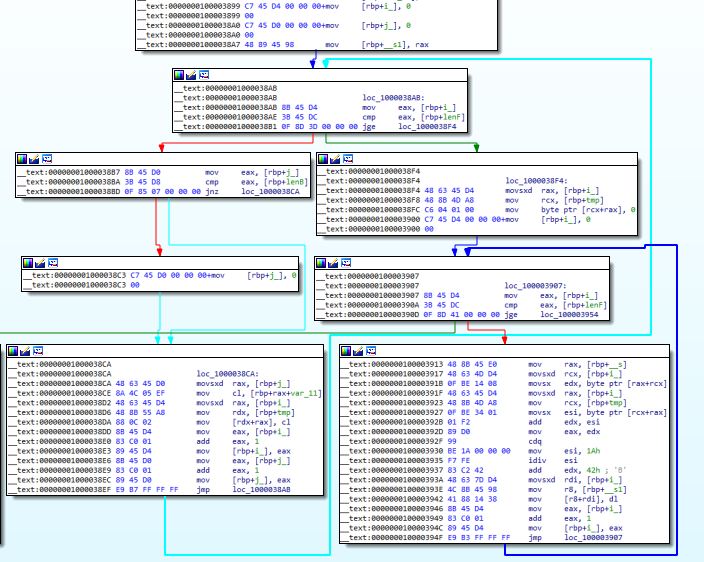
Tiếp tục phân tích hàm encrypt\_() , đoạn này lấy từng giá trị từ \_KEY để thực hiện tính toán riêng kí tự đầu thực hiện NOT còn các kí tự tiếp theo thực hiện xor theo thứ tự:0xAB,0xE5,0x8A,0x5C,0x44,0x20,0x47 các byte sau khi được tính toán được lưu từ [rbp+var\_11] đến [rbp-var\_A] sau một lúc tính tay thì ra được chuỗi “BESTRONG”.

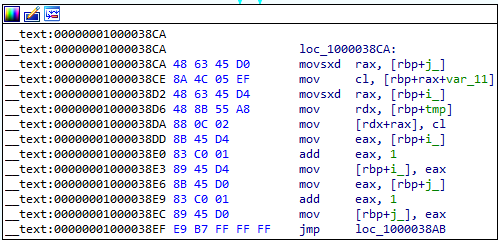




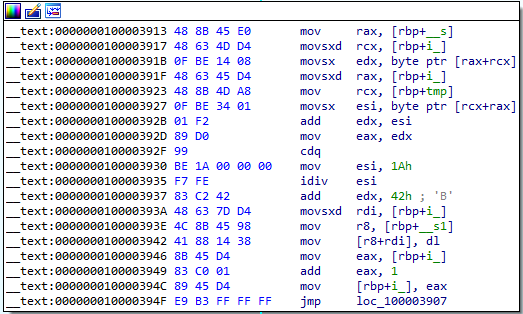
Thực hiện tính độ dài chuỗi fake flag và “BESTRONG”



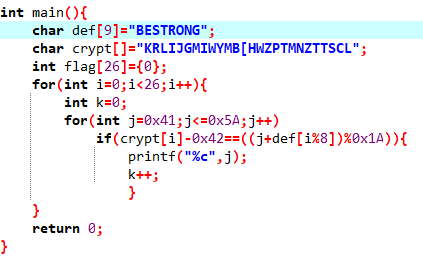
Đây là đoạn nó thực hiên encrypt fake flag.Mình sẽ nói sơ qua nhánh bên trái mà thật ra cũng không có gì nhiều, nó thực hiện việc gán từng char của chuỗi “BESTRONG” vào biến [rbp+tmp] bằng với độ dài của chuỗi fake flag:



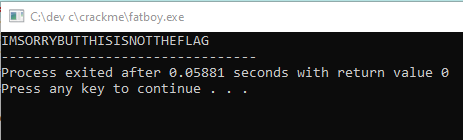
Nó thực hiện encrypt chuỗi cũng khá đơn giản.s1[i]=[(\_s[i]+tmp[i])%0x1A]+0x42 nó thực hiện encrypt từng kí tự như trên,s1 lưu chuỗi encrypt, \_s và tmp thì mình có nói ở trên:



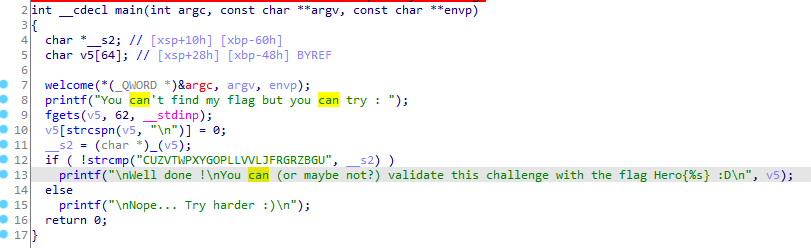
Vậy mình đã có đầy đủ thông tin,giờ mình sẽ code để lấy real flag và đây là code của mình:

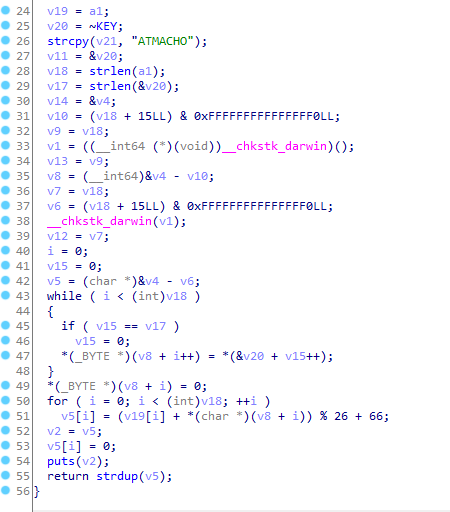


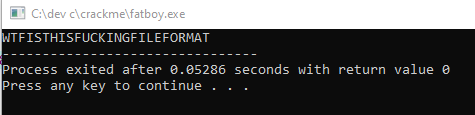
Cái này không phải flag nhưng còn arm64 binary mình chưa load:



Lần này mình sẽ dùng Hex-ray chức năng của IDA bởi vì mình chưa học ARM, tới đây thì biết 2 chuỗi "BESTRONG" và "KRLIJGMIWYMB[HWZPTMNZTTSCL" thay đổi thành "FATMACHO" và "CUZVTWPXYGOPLLVVLJFRGRZBGU" ,F của chuỗi "FATMACHO" được lưu ở v20:







Flag: Hero{WTFISTHISFUCKINGFILEFORMAT}

Script với file fatBoy:<https://github.com/MinhHy23343/Heroctf>