BabyRE:

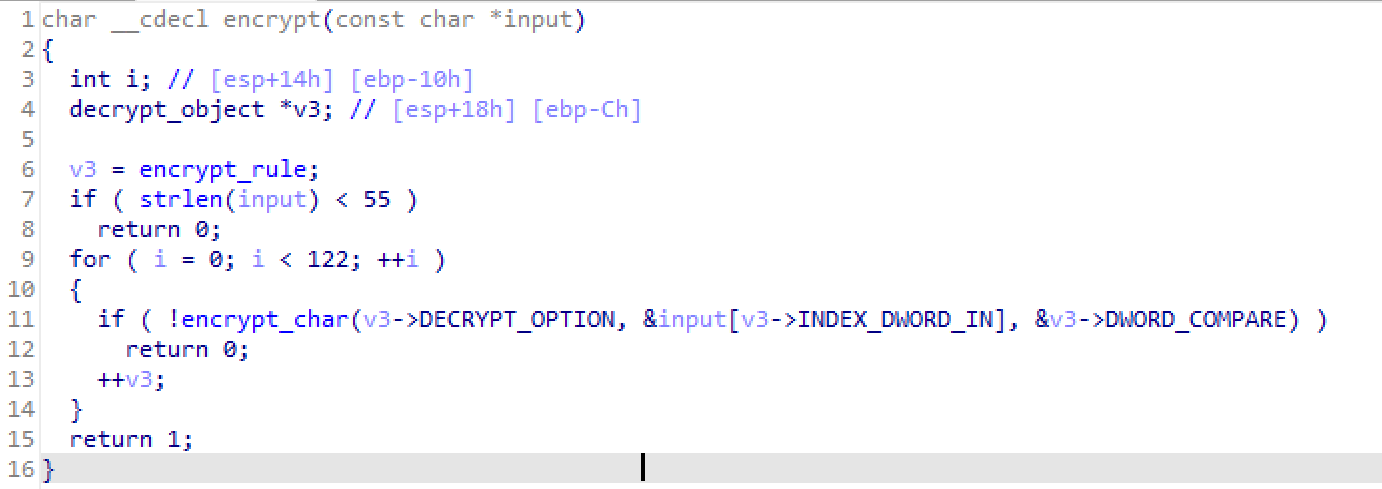
Đây là file thực thi window 32 bit.

Graphical user interface, text

Description automatically generated

Đầu tiên, chương trình khởi tạo một vùng nhớ 300 bytes, set về zero (dòng 20). Vùng nhớ này được sử dụng để chứa userinput (dòng 31 scanf với %300[^\n]s – nhập vào tối đa 300 kí tự )

Dòng 41 kiểm tra xem độ dài của userinput có lớn hơn 294 hay không. Nếu đúng thì tiếp tục gọi hàm encrypt.

Hàm encrypt: 

Ở đây, ta chú ý tới một vùng nhớ đặc biệt là encrypt\_rule. Đây là 1 vùng nhớ đã chứa dữ liệu sẵn (fix cứng, không phải là dump ra lúc chương trình chạy, cũng không phụ thuộc vào user input). Cấu trúc vùng nhớ này là 1 array 122 object, 1 object có kích thước 12byte (3 dword). DWORD thứ nhất chứa option để encrypt, DWORD thứ hai chứa vị trí trên userinput được sử dụng để encrypt. DWORD thứ ba chính là payload để so sánh, nếu sau khi encrypt output đúng với DWORD thứ ba thì return 0, user input là chính xác.



Hàm encrypt\_char: Encrypt option được pass vào từ hàm encrypt, dựa vào option này thì chương trình sẽ dump ra 1 trong 4 đoạn op-code vào lpAddress (được set quyền read/write/execute), sau đó lpAddress sẽ được call với tham số là in và compare để thực hiện mã hóa và check.

Text

Description automatically generated

Để biết 4 đoạn shell code trên, ta breakpoint và inspect memory bằng ida.

Shell code 1: Xor

Graphical user interface, text, application

Description automatically generated

Shell code 2: Bit shift

Graphical user interface, text, application

Description automatically generated

Shell code 3: Base64

A picture containing table

Description automatically generatedText

Description automatically generated

Shell code 4: RC4 với key là susan (tác giả là fan susan0175? =)))

Text

Description automatically generated

Dựa vào 4 đoạn shellcode trên, ta có thể decode ngược ra được userinput:

ThiS 1s A rIdiCuLously l0ng\_Lon9\_l0ng\_loNg\_lOng strIng. The most difficult thing is the decision to act, the rest is merely tenacity. The fears are paper tigers. You can do anything you decide to do. You can act to change and control your life; and the procedure, the process is its own reward.

Nhập input trên vào chạy chương trình ta thu được flag: vcstraining{Aw3s0me\_D4ta\_tran5Form4t1oN\_Kak4}

Text

Description automatically generated

WAILA!