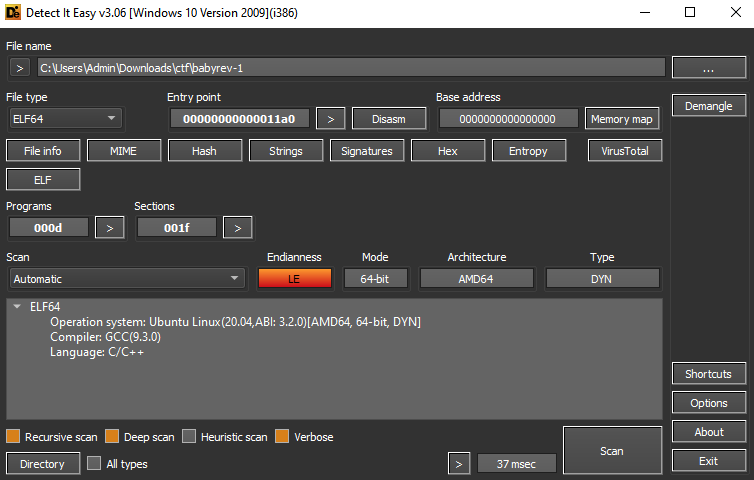
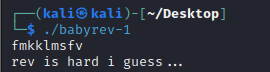
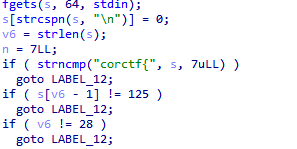
**­babyrev-1**

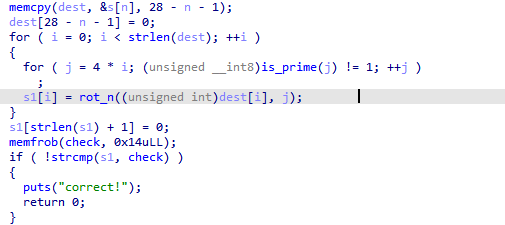
Cho file vào Detect It Easy thì cho biết đây là file ELF64 và chạy trên Linux.

Thử chạy trên chương trình trên Linux

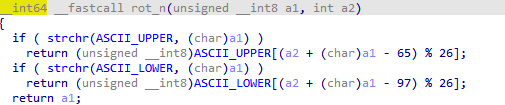


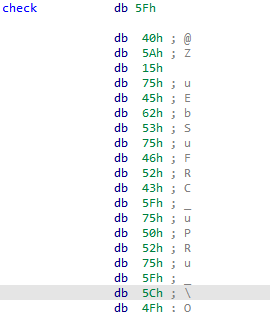
Cho file vào IDA64 ta thấy đoạn đầu là check format input là 28 ký tự: “corctf{…}”

 Chúng ta cần phải tìm “…” là 20 ký tự trong đoạn code này:

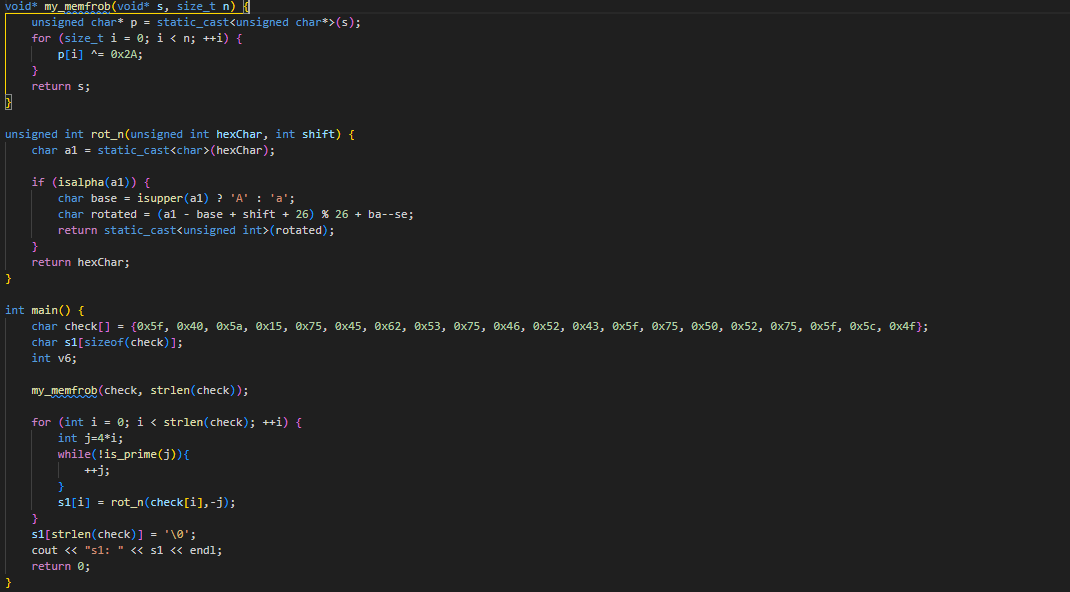
Đọc sơ qua thì chủ yếu là ở hàm rot\_n làm dịch chuyển input tạo ra s1 và so sánh với check trong hàm memfrob

rot\_n là một hàm dịch chuyển các ký tự như bình thường:

memfrob là hàm xor trong Linux cụ thể ở đây là check xor với 0x2A, lấy data của check ta có:



Thử code ngược lại chương trình:

Có vẻ kết quả hơi bất ổn =]]

Flag: corctf{see?\_rEv\_aiTZ\_YU\_HaJ4}