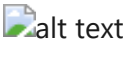
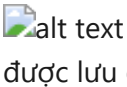
Generated: 2025-11-01 20:51

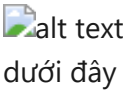
Kiểm tả file

 alt text

Dùng IDA để biên dịch sang ASM

 alt text - Ở đây ta có thể biết chắc rằng enc_flag là flag ta cần tìm. - Chuỗi của ta nhập và sẽ được lưu ở esi, còn chuỗi flag được lưu về esi.

Truy cập vào hàm check_password

 alt text - Khúc này đã quá rõ để tìm password, ta sẽ làm ngược lại các bước trên bằng đoạn code dưới đây

Ta có đoạn code decrypt như sau

```
enc_flag = [0x74, 0x78, 0x4B, 0x65, 0x77, 0x48, 0x5C, 0x69, 0x68, 0x7E, 0x5C,

len = 48

key = [0] * len
tmp = ""

for i in range(len):
    key[i] = enc_flag[i] ^ len
    tmp = tmp + chr(key[i])

print(tmp)
```

–> Flag: DH{UGxlYXNlIGRvIG5vdCBiYXNlNjQgZGVjb2RlIGl0Lg==}