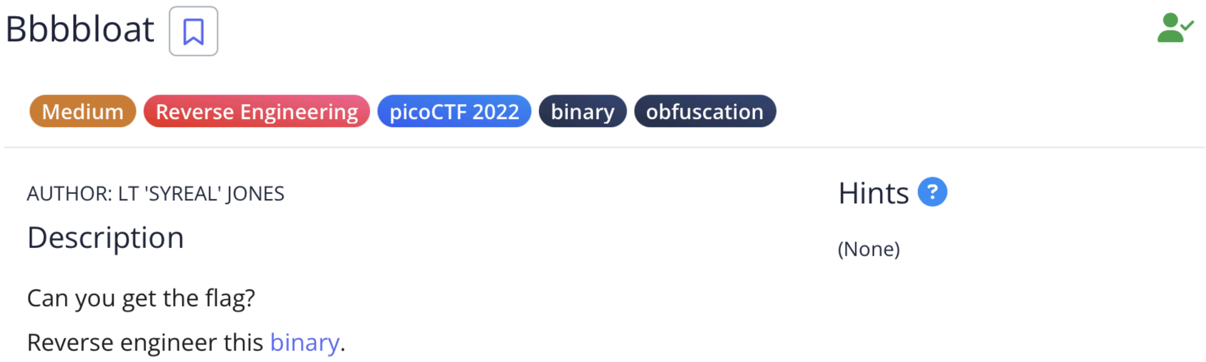


Bbbbloat

Medium | Reverse Engineering | picoCTF 2022 | binary | obfuscation

AUTHOR: LT 'SYREAL' JONES

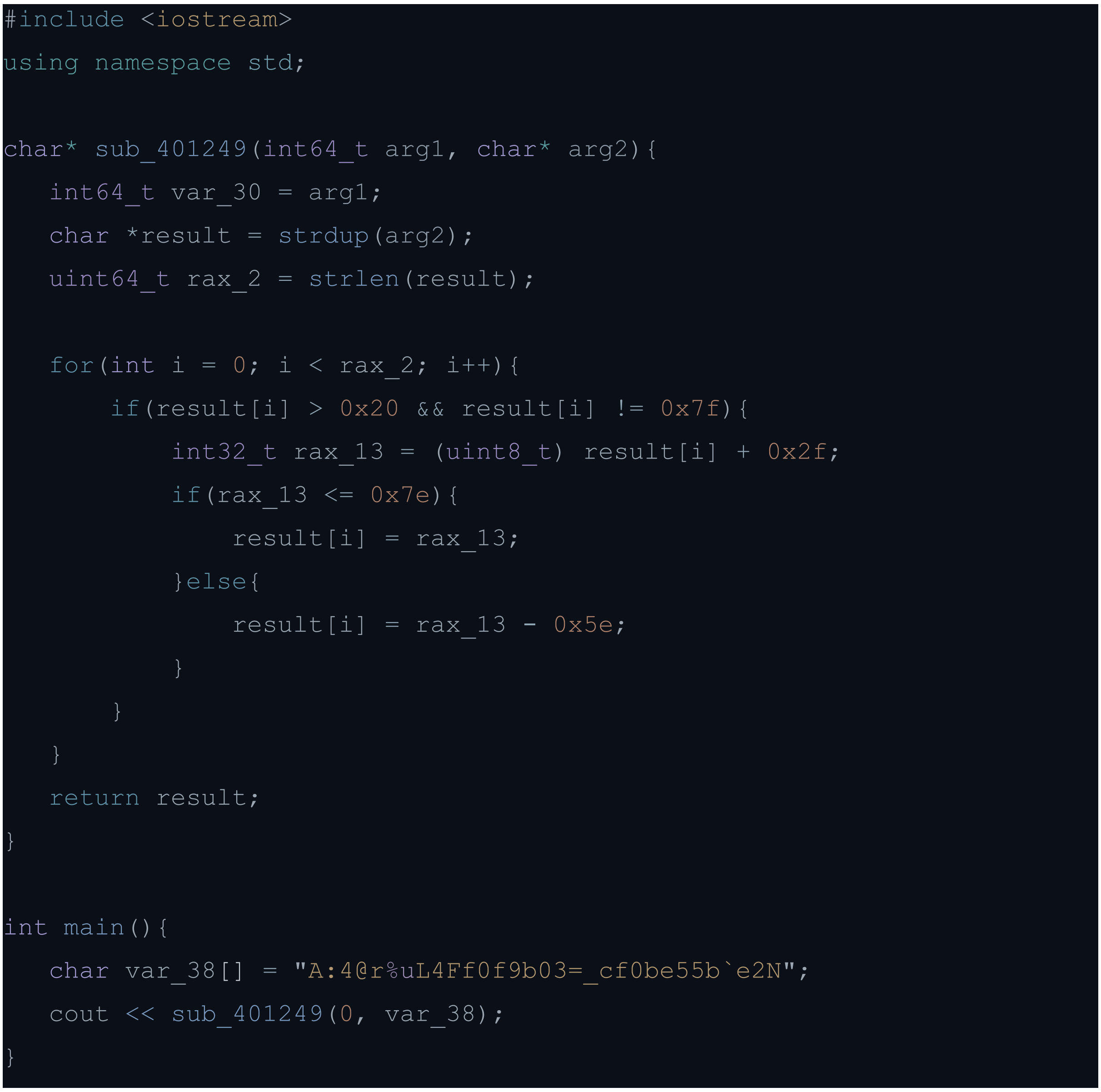
Description

Can you get the flag?

Reverse engineer this binary.

Hints

(None)



```
#include <iostream>
using namespace std;

char* sub_401249(int64_t arg1, char* arg2){
    int64_t var_30 = arg1;
    char *result = strdup(arg2);
    uint64_t rax_2 = strlen(result);

    for(int i = 0; i < rax_2; i++){
        if(result[i] > 0x20 && result[i] != 0x7f){
            int32_t rax_13 = (uint8_t) result[i] + 0x2f;
            if(rax_13 <= 0x7e){
                result[i] = rax_13;
            }else{
                result[i] = rax_13 - 0x5e;
            }
        }
    }
    return result;
}

int main(){
    char var_38[] = "A:4@r%uL4Ff0f9b03=_cf0be55b`e2N";
    cout << sub_401249(0, var_38);
}
```

Flag : picoCTF{cu7_7h3_bl047_36dd316a}