

# CKR

사진 속 실행파일을 복구하여 gdb를 통해 분석한다.

실행파일을 gdb로 열어보면 0x100003ebc값을 0x5a와 xor 연산을 통해 input과 비교한다.

```
0x100003ca6 <main+22> movl    $0x0,-0x54(%rbp)
0x100003cad <main+29> mov     0x208(%rip),%rax      # 0x100003ebc
0x100003cb4 <main+36> mov     %rax,-0x13(%rbp)
0x100003cb8 <main+40> mov     0x205(%rip),%ax       # 0x100003ec4
0x100003cbf <main+47> mov     %ax,-0xb(%rbp)
0x100003cc3 <main+51> mov     0x1fd(%rip),%al      # 0x100003ec6
0x100003cc9 <main+57> mov     %al,-0x9(%rbp)
0x100003ccc <main+60> lea     -0x30(%rbp),%rdi
0x100003cd0 <main+64> lea     -0x13(%rbp),%rsi
0x100003cd4 <main+68> mov     $0x14,%edx
0x100003cd9 <main+73> call    0x100003e10
0x100003cde <main+78> lea     -0x30(%rbp),%rdi
0x100003ce2 <main+82> mov     $0x5a,%esi
0x100003ce7 <main+87> call    0x100003c20 <xor_encrypt_decrypt>
0x100003cec <main+92> lea     -0x30(%rbp),%rax
0x100003cf0 <main+96> mov     %rax,-0x60(%rbp)
0x100003cf4 <main+100> lea     0x1cc(%rip),%rdi     # 0x100003ec7
0x100003cfb <main+107> mov     $0x0,%al
0x100003cfd <main+109> call    0x100003e28
0x100003d02 <main+114> lea     -0x50(%rbp),%rsi

exec No process (asm) In:                               L??  PC: ??
(gdb) x/s 0x100003ebc
0x100003ebc:      "**?(366;536"
```

만약 input과 encrypted\_answer = \*(366;536 ^ 0x5a와 같다면 “It's me, perillaoil!!!”이 담긴 flag.txt파일이 열린다.