rop 문제풀이

basic_rop_x64	2024-03-05 오후 1:14	파일	9KB
basic_rop_x64.c	2024-03-05 오후 1:14	C 파일	1KB
Dockerfile	2024-03-05 오후 1:14	파일	1KB
flag	2024-03-05 오후 1:14	파일	1KB
libc.so.6	2024-03-05 오후 1:14	6 파일	2,165KB

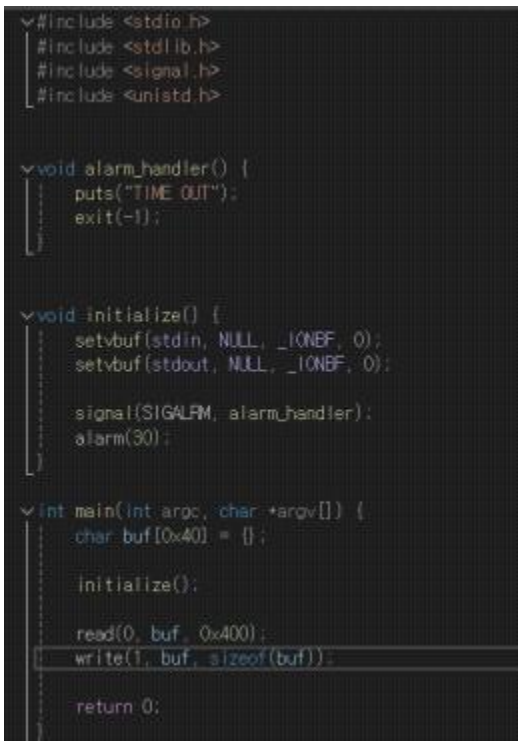
여러 가지 파일이 있었는데 xss 관련 문제에서도 도커 파일이 있었다.

도커 파일이 뭐지? ctf 문제에서 꽤 자주 나오는 파일 같아서 아주 열심히 찾아봤다.

구글링해서 찾아보는데 도커 파일은 어떻게 여는 건 지 친절하게 설명해주는 포스팅은 없었다.

Docker Desktop 이라는 프로그램을 깔아서 어떻게든 해보려고 했는데 프로그램 사용법을 잘 모르겠다.

그래서 c파일을 우선 열어봤다.



```c
#include <stdio.h>
#include <stdlib.h>
#include <signal.h>
#include <unistd.h>

void alarm_handler() {
    puts("TIME OUT");
    exit(-1);
}

void initialize() {
    setvbuf(stdin, NULL, _IONBF, 0);
    setvbuf(stdout, NULL, _IONBF, 0);

    signal(SIGALRM, alarm_handler);
    alarm(30);
}

int main(int argc, char *argv[]) {
    char buf[0x40] = {};

    initialize();

    read(0, buf, 0x400);
    write(1, buf, sizeof(buf));

    return 0;
}
```

코드에는 버퍼오버플로우의 취약점을 내포하고 있다고 한다.

buf 크기(64바이트)를 초과하는 데이터를 read 함수로 읽을 수 있어, 메모리 손상 및 잠재적인 코드 실행 공격이 가능하다고 한다.