# Brob

| | |
|---|---|
| 태그 | 포너블 |
| 상태 | 진행 중 |

문제설명: **bof + probability**

## BOF

버퍼 오버 플로우

→ 연속된 메모리 공간을 사용하는 프로그램에서 할당된 메모리 범위를 넘어선 위치에 자료를 읽거나 쓸 때 발생. 오작동 또는 악의적 코드 실행 가능

https://isc9511.tistory.com/119

*** C 언어 상 BOF 주요 함수**

| BOF 주요 함수 | 설명 |
|---|---|
| strcpy(char *dst, const char *src) | - src 문자열을 dst 버퍼에 저장<br>- src 문자열 길이를 체크하지 않아, dst 버퍼를 초과하는 BOF 가능 |
| strncpy(char *dst, const char *src, size_t len) | - src 문자열의 len 만큼을 dst 버퍼에 저장<br>- src 문자열 길이를 제한하여 BOF 방지 가능 |
| size_t strlen(const char *str) | - 문자열(str)의 null 문자를 제외한 바이트 수를 반환 |
| sizeof(피연산자) | - 피연산자의 크기를 반환 |

## probability

확률론?

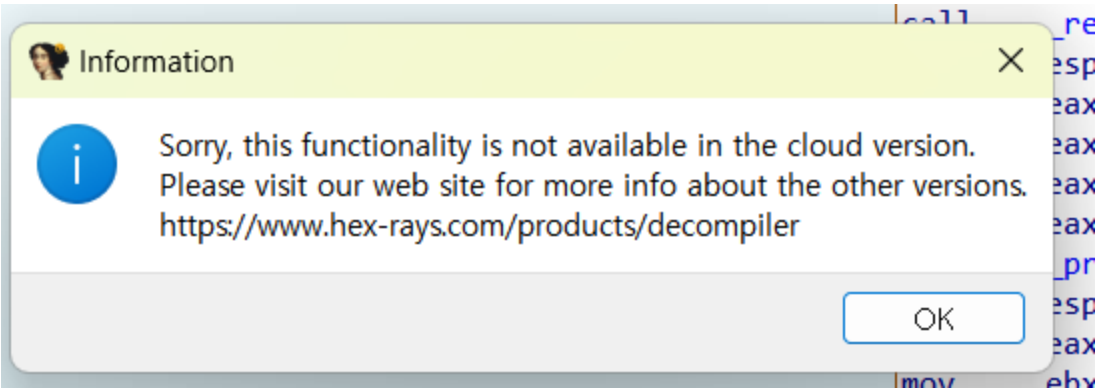
```
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x80490c0
  Start of program headers:          52 (bytes into file)
  Start of section headers:          10392 (bytes into file)
  Flags:                             0x0
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         10
  Size of section headers:           40 (bytes)
  Number of section headers:         29
  Section header string table index: 28
```

./brob 으로는 실행되지 않음.

elf 헤더 → 엔트리 포인트 체크(main or main 함수 호출 위치)

IDA로 디컴파일링 시도

→ 오류 발생




현재 구독하고 있는 요금제에서는 지원을 안 해준다는 뜻인가?

지금껏 잘 해주다가 왜....

검색해 보니 아이다 서버 연결 오류라고 한다. 기다려보면 해결되는 경우가 많다니 내일 다시 시도해보자.

+) 8.17.

여전히 같은 오류 발생.


입력값이 3개가 넘어가는 순간 버퍼오버플로우가 발생하는 것 같다.

https://isacacia.tistory.com/49

https://velog.io/@elfinsun/리버싱-핵심-원리-스택-프레임