Noob oob

문제이름

noob oob

사용 된 취약점

out of bounds

풀이 과정

전체 코드

```
#include <stdio.h>
#include <string.h>
#include <unistd.h>
#include <stdlib.h>
#include <signal.h>
#include <time.h>

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

void initialize(char buffer[], int size) {
    signal(SIGALRM, alarm_handler);
    setvbuf(stdin, NULL, _IONBF, 0);
    setvbuf(stdout, NULL, _IONBF, 0);
    alarm(30);
    for (int i = 0; i < size; i++) {
        buffer[i] = rand() % 100;
    }
}

int calculateSecretKey(int buffer[], int size) {
    int secret_key;
```

```
    do {
        secret_key = 0;
        int randomCount = rand() % 16;
        for (int i = 0; i < randomCount; i++) {
            int randomIndex = rand() % size;
            secret_key += buffer[randomIndex];
        }
    } while (secret_key == 0);
    return secret_key;
}

void Shell() {
    char *cmd = "/bin/sh";
    char *args[] = {cmd, NULL};
    execve(cmd, args, NULL);
}

int main() {
    char buffer[0x10];
    int secret_key;
    int idx;

    srand(time(NULL));
    initialize(buffer, 0x10);
    secret_key = calculateSecretKey(buffer, 0x10);

    printf("Buffer idx: ");
    scanf("%d", &idx);

    if (idx >= 0 && idx < 0x10) {
        printf("%d\n", buffer[idx]);
    } else if (idx >= -0x10 && idx < 0) {
        printf("%d\n", *((int*)(buffer + idx)));
    } else {
        puts("Invalid index");
    }

    printf("secret_key address : %p\n", &secret_key);
```

```
    puts("Enter the key: ");
    scanf("%d", &idx);

    if (idx == secret_key) {
        Shell();
    } else {
        puts("Access denied");
    }

    return 0;
}
```

해당 문제에는 랜덤으로 생성되는 비밀 키를 알아내서 입력을 하면 Shell함수가 실행 되서 플래그를 알아낼수 있습니다.

비밀 키는 buffer에 저장되는데 현재 유저가 접근 가능한 곳에서 할 수 있는 것은 idx에 정수를 입력하여 buffer의 값을 출력하는 게 전부입니다.

제공된 소스 코드를 보면 buffer 변수가 먼저 선언되고, 그 다음에 secret_key 변수가 선언됩니다.

스택에서 로컬 변수는 선언된 역순으로 할당되므로, secret_key가 buffer보다 낮은 주소에 위치하고 buffer의 크기가 0x10 (16)바이트이므로, secret_key는 buffer의 8바이트 앞에 위치하게 됩니다.

입력값에 -8을 입력하고 출력되는 값을 입력하면 쉘이 실행됩니다.

FLAG : SOTI{Hmm..5uper_DupEr_34Sy_ri9HT?}