Under the sea

문제 이름

Under the sea

사용 된 취약점

정수 오버플로우

풀이 과정

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <signal.h>
void timeout_handler(int signum) {
    printf("Time out!\n");
    exit(1);
}
int main() {
    int value;
    signal(SIGALRM, timeout_handler);
    alarm(30);
    scanf("%d",&value);
    if (value < 0){
        value-=1004;
        if (value > 0) {
            system("/bin/sh");
        } else {
            printf("Value: %d\n", value);
        }
    }
```

```
    return 0;
}
```

해당 코드에서 쉘을 실행시키려면 value에 입력값은 음수면서 1004를 빼면 양수인 수를 입력해야 한다.

int형 변수의 최솟값은 -2147483648이고, 여기에 1004를 빼면 2147482644가 된다.

따라서 value에 int형의 최솟값인 -2147483648을 입력하면 -2147483648 < 0 이므로 첫 번째 if문의 조건을 만족하고,
-2147483648 - 1004 = 2147482644 > 0 이므로 두 번째 if문의 조건도 만족하여 system("/bin/sh")가 실행되어 쉘을 획득할 수 있다.

이는 정수 오버플로우를 이용한 것으로, int형 변수가 표현할 수 있는 범위를 넘어서는 연산을 수행하면 의도치 않은 값이 나오는 취약점이다.

SOTI{in7_vA1u3_I5_lOw_bu7_u_r_1N7_NOt_1Ow}