Buffer overflow practice

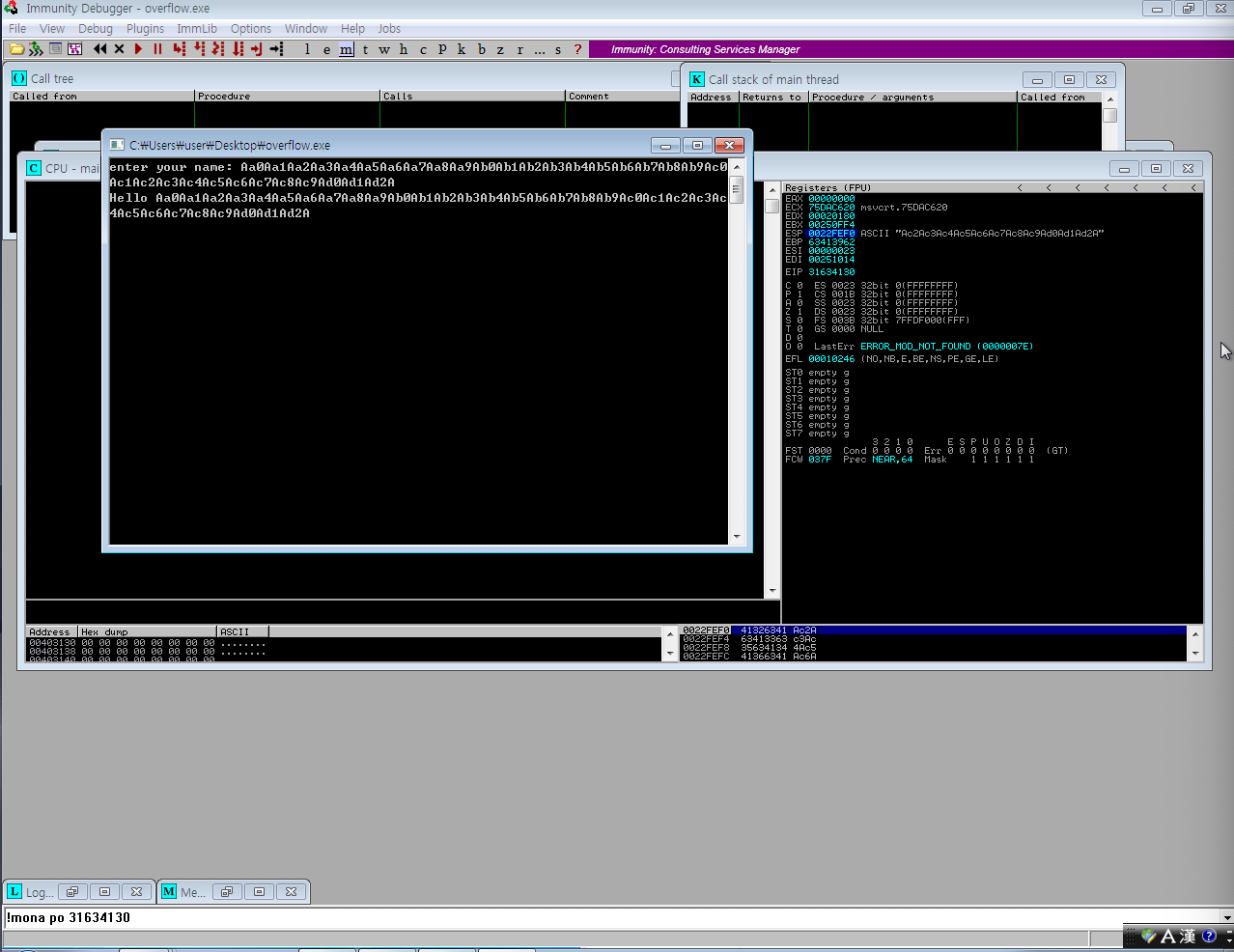
Scanf buffer overflow

사용된 함수 – gets

Cmd gcc 컴파일러 이용.

Cmd -> setx %”path”% ……. <- desktop 에 gcc 컴파일러 생성

Cmd -> gcc overflow.c -> exe 파일 생성 -> immunityDebugger 에서 분석



C 언어 사용

#include<stdio.h>

Int main()

{

Char str[50];

Printf(“enter your name:”);

Gets(str);

Printf(“Hello %s”,str);

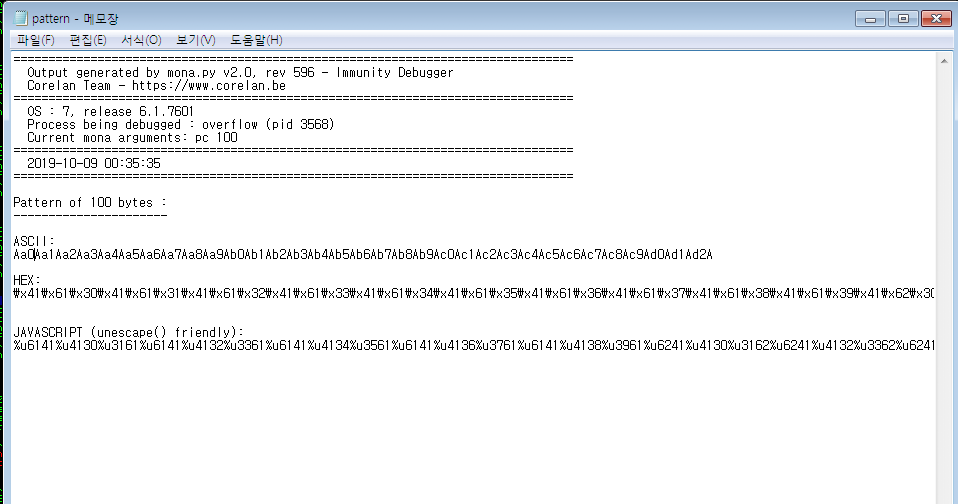
}

이후 발생된 오버플로로 인한 파일중지(오류)

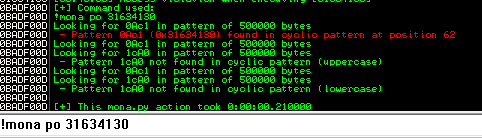
실행중지된 파일을 mona 를 이용해서 분석

!mona workingfolder c:\mona\%p

.exe 파일에 관한 Pattern 생성



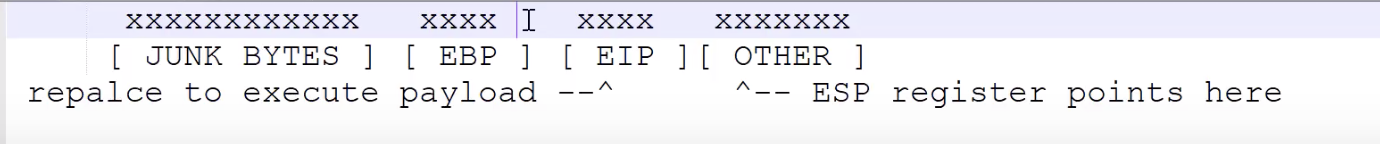
Askii 코드를 그대로 복사해서 gets 에 입력시키면





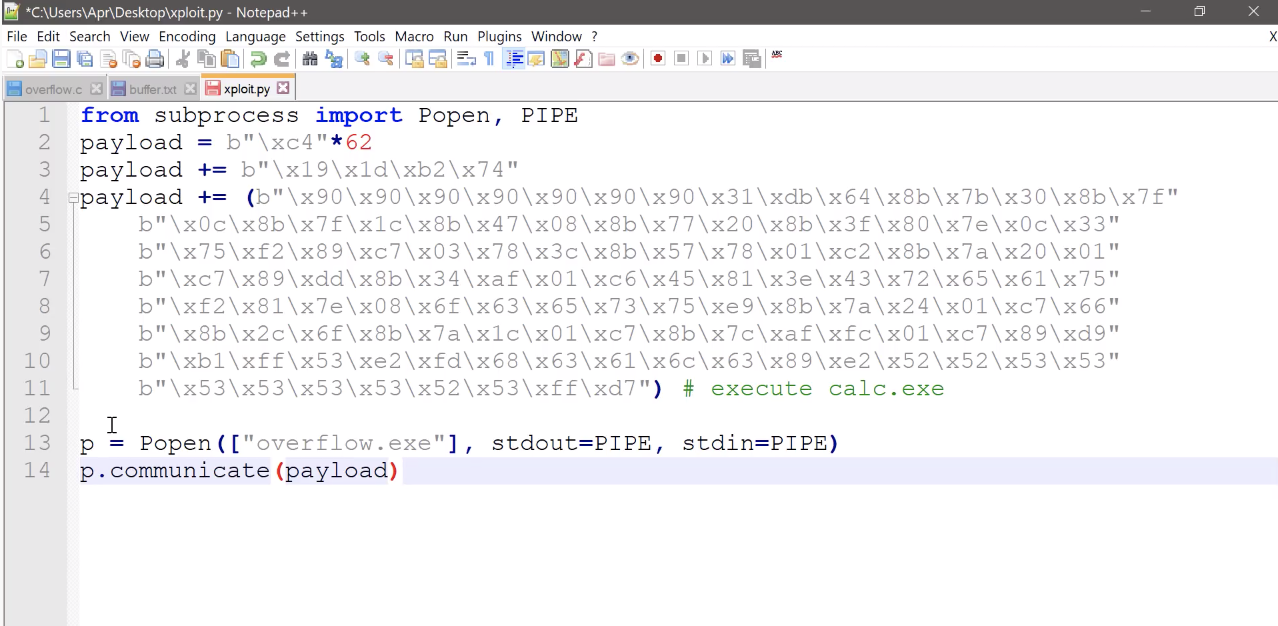
취약점 발견.

정크데이터 크기 62로 발견됨



EIP 를 exploit 하는 페이로드 작성 with py,,,,

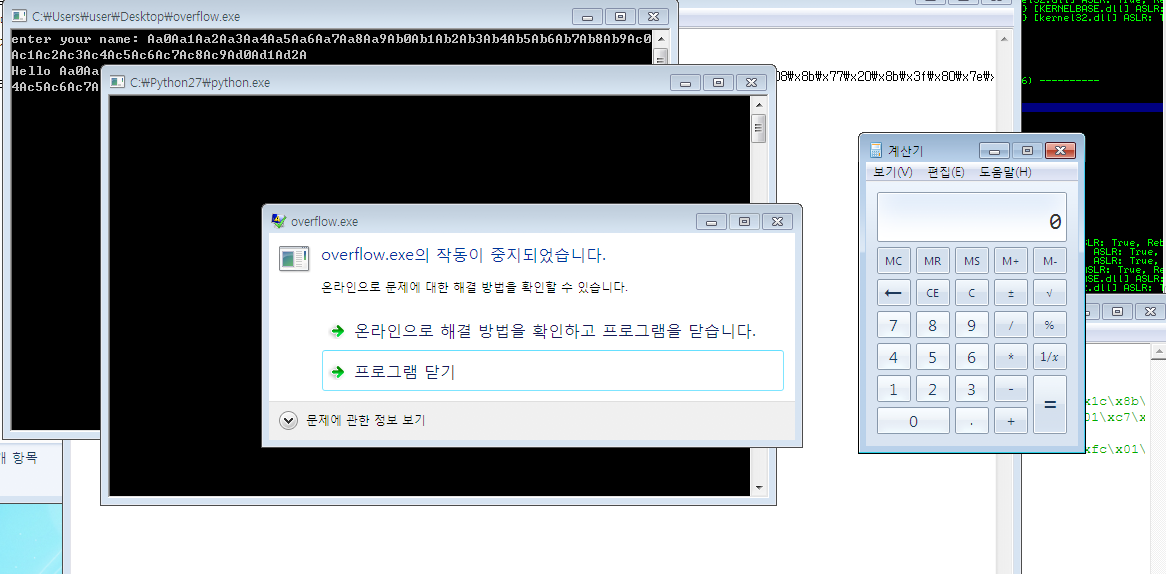






Exploit.py 실행시키면

Overflow.exe 는 작동중지 되며 calc.exe 실행



EIP 조작으로, Overflow.exe 리턴 값이 calc.exe 실행 값으로 변경