# Tutorial 0x0008

## Task 1: Stack Based Buffer Overflow Analysis using gdb

Implement the code given below.

```c
#include <string.h>
#include <stdio.h>

int main(int argc, char** argv)

{
        argv[1] = (char*)"ABCDEFGHIJKLMNOPQRSTUVWXYZ";
        char buffer[8];
        strcpy(buffer, argv[1]);
        printf("Buffer Address :%p\n", buffer);
        return 0;
}
```

Save the code as “day8_ex1.c” and generate executable output and

`Compile: gcc -fno-stack-protector -z execstack day8_ex1.c -o day8_ex1`

I. Load the program to gdb-peda and analyse the code

II. What is the value expected to be in the RIP register at the end of the execution of this program?

III. Replace the vulnerable strcpy() with strncpy() and analyse how this will eliminate the buffer overflow vulnerability