Embedded Systems Security (CS6898)

Assignment-1 (100 Marks)

Submission Guidelines

In this assignment we expect the following to be submitted :

- A single report that describes your approach taken for solving the assignment (PDF format)
  - The report should contain a snapshot of the stack binaries while they are executing (this can be a screenshot of a debugger like **gdb** or an illustration) with the *addresses* being visible.
  - Highlight why the binary could be exploited, what can be done to make it secure?
- Exploit string for the given binary (tested on the provided VM)
- All submission files should be zipped as one archive (Ex: `submission.zip`).

Files

```
lab_1
├── lab_1
├── lab_1.c
└── Makefile
```

- Students are provided a binary `lab_1` and the corresponding source file `lab_1.c`
- Students can view the source file and identify vulnerabilities in the program, they are also given the `Makefile` that contains the compilation flags that were used.
- Students need to come up with an exploit string `payload` such that they are able to call the function `exploit()` present in the program, when this payload is passed as input to the program.

Expected Output

```
sse@sse_vm:~/lab_1$ ./lab_1 $(cat payload)
Welcome group "something".
Exploit succesfull...
```