Assignment 10, Fall 2018
CS4630, Defense Against the Dark Arts
Format String Attack:
Incursus Format Sententiam Curse

Purpose

In this assignment, you will learn how format string vulnerabilities can be exploited.

Due

This assignment is due on **Thursday, 29-NOV-2018 at 11:59 pm**

Assignment Prerequisites

1. Review the format string vulnerability slides.

Assignment Details

1. This assignment must be completed using the **64-bit Ubuntu 18.04.1 LTS OS** you installed on your VM for Assignment #1. This environment is where we will test your submitted code. It is possible, due to the sensitivity of vulnerabilities to the operating environment, that exploit code developed for one environment will work not correctly in a slightly different environment.

2. Download the code `format_string_vulnerability.exe` and `format_string_vulnerability.c` from the class Collab site. You must attack the supplied version of `format_string_vulnerability.exe`. **Do not recompile and use a different version.**

3. `format_string_vulnerability.c` has a format string vulnerability that you can exploit to give yourself a better grade than the default, which is a "D". Your goal is to give yourself a grade of "A."

4. You should write a program that generates the malicious input. The input that you generate should have the program print your name in addition to giving you a grade of "A." This program should be written using C. Below is a sample C program.

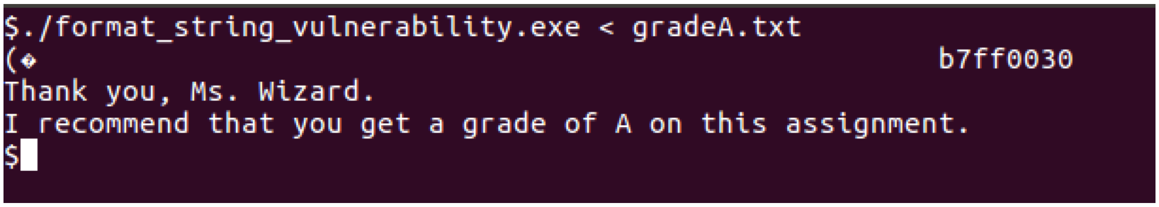
```
#include <stdio.h>
#include <string.h>
char attackString[] = "Bill Smith\n";
int main() {
 int i;
 char *p = attackString;
 for (i = 0; i < sizeof(attackString); i++) {
 putchar(*p);
 p++;
 }
 return 1;
}
```

Your code should contain comments with your name, UVA ID and a detailed explanation of how you figured out the pieces of information you needed to craft your attack string. Your explanation will be graded in addition to your attack input.

Here are two sample runs that demonstrate the sample runs of the program. **Benign Input.** Assume the file name.txt contains two lines where each line has the name Hermione Granger.

```
$ ./format_string_vulnerability.exe < name.txt
Hermione Granger
Thank you, Hermione Granger.
I recommend that you get a grade of D on this assignment.
```

Attack Input. The following sample run shows the output when giving the attack string generated by the attack input generator program to the vulnerable `format_string_vulnerability.exe` program.



```
$./format_string_vulnerability.exe < gradeA.txt
(�                                                      b7ff0030
Thank you, Ms. Wizard.
I recommend that you get a grade of A on this assignment.
$
```

Figure 1: Result of giving attack input to `format_string_vulnerability.exe`

Requirements

1. Submit your attack generation code via the Collab. It must be named `format_string_attack.c`. Your attack generator code must be commented to contain the following:
   - Your name and UVA computing ID
   - A detailed explanation of the process you used to determine the content of your attack string input. Include a description of all the pieces of information you needed to gather.
2. This assignment is pledged.

Items to Submit

This assignment is due on **Thursday, 29-NOV-2018 at 11:59 pm** .

1. Upload your `format_string_attack.c` file.

It is mandatory that you use the file names given and adhere to the given API to ease the task of grading multiple different student submissions of this assignment. Throughout the semester, you will be given file names and sample execution output. All assignments will be submitted using the class Collab Website.