

Homework 3 for CMPSC 447: Format String Attack

Yanling Wang

February 10, 2020

Due date: 11pm Wednesday February 19th, 2020.

1 Introduction

In this assignment, you will be given a C program and its corresponding x86-64 binary code compiled from the C program. Your job is to figure out proper input for the program so that your program prints out: "Congratulations, it is your lucky day today!".

2 Source code

```
#include <stdio.h>

int c = 'n';

int goodPassword() {
    // allocate buf and set them all to zero.
    char buf[100] = {};
    fgets(buf, 100, stdin);
    printf(buf);
    return c;
}

int main() {
    if (goodPassword() == 'y') {
        printf("\nCongratulations, it is your lucky day today!\n");
    }
    else {
```

```

    printf("\nWrong password, try again.\n");
}
return 0;
}

```

Try to figure out a proper input so that your program will print out at the end:
Congratulations, it is your lucky day today!

Save your input into the file input.txt

Explain in details how you find out the values needed for input.txt in hw3writeup.pdf.
 In particular your write up should answer the following questions:

1. Which variable's value your solution tries to corrupt? What is its memory address?
2. How do you get to this address? In other words, where do you place this address?
3. What value will you put in this variable? How do you obtain this value?
4. Please list the string you have in input.txt, use \x?? for characters with ascii's hexadecimal value being ??. Also list how many format descriptors your input has and why you need these many.

3 Requirement

Please submit "input.txt", "hw3writeup.pdf" to gradescope. You should have received an email about being enrolled in CMPSC 447 on gradescope in your psu school email.