**MIS 6330: IT Security**

**Prof. A. Lahiri**

**Individual Homework 5**

1. Based on what we have learned about software vulnerability and injection/ overflow attacks, what do you think is the major difference between *testing programs for functionalit*y vis-à-vis *testing them for vulnerability*?
2. Consider the C procedure below.

void hello(char \*tag)

{

char inp[16];

printf(“Enter value for your %s: ”, tag);

gets(inp);

printf(“Hello your %s is %s\n”, tag, inp);

}

**hello(“message”) produces an output of this form:**

Enter a value for your message: *test* (🡸 input from user)

*Hello your message is test* (🡸 output from hello)

* 1. Explain *the main vulnerability* of this piece of code.

* 1. Modify the code above in order to address the vulnerability.

**Hint:** search the Internet for the C function “fgets,” and find out how it can help.

1. Check the vulnerability <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2208>. What are some of the broader lessons that can be learned from this particular vulnerability? (Avoid technical details and provide an executive-level synopsis of key takeaways.)