COSC 647

Homework 3 – Due Nov 11, 2015 by 11:59PM

1. Write a program with a race condition, either in threads, processes or signals. (The flaw need not be exploitable) Explain the software defect, and why it forms a race condition.

2. Write a program with a race condition in the file system. Demonstrate how to exploit the flaw. You may modify the code somewhat to allow for control of the program's timing.

3. Write a program that has a format string flaw. Make the program SUID root, and exploit it to obtain a root shell. Overwrite the .dtors section to start the execution of the shellcode.

4. Write a program that demonstrates the use of format strings for output functions. It should be a suitable example for an introductory programming course.

5. Create a web application that uses a MySQL database backend. Demonstrate it.

6. Create a web application that uses a MySQL database backend that suffers from a SQL injection vulnerability. Demonstrate it.

7. Correct the flaw in the previous problem by correctly sanitizing the input.