**CSE 410/518 Software Security**

**Midterm CTF**

**Oct 23, 2023**

**Total 160 Points + Bonus Points**

**Your full name:**

**Your CSE410/518 CTF platform username:**

**You are allowed to use google, or refer to lecture slides, homework, code during the exam. But, you cannot communicate with anyone in or outside of the class. You cannot use LLM, e.g., ChatGPT, either.**

**For each challenge, you should clearly show your exploit, screenshot of successful exploitation, and a very brief description of how you did it. Even if you fail to capture the flag, you may get some points for documenting your steps.**

**Some hints: Use “file” to check if the executable is 32-bit or 64-bit. Use “./checksec --file executable-name” to see if the stack is executable or if stack cookie is inserted. Use “strace” to see what system calls a program makes.**

**All four challenges are under the MidTerm23Fall category.**

**The first person to capture each flag receives a 10-point ‘first blood’ bonus.**

1. [40] Capture the flag of ***re\_2\_64***.

a. [5] Where does this program take input?

1. [40] Capture the flag of ***overflowret9\_32***.

a. [4] Is this a 32bit or 64-bit program?

b. [4] Is stack executable? Can you overwrite RET address on stack? Is there a canary to protect the stack? (You can use checksec.sh, objdump, etc., to find out)

c. [4] Where does this program take input?

d. [4] Describe your high-level idea on how to exploit this challenge.

1. [40] Capture the flag of ***overflow7\_32***.

a. [4] Is this a 32bit or 64-bit program?

b. [4] Is stack executable? Can you overwrite RET address on stack? Is there a canary to protect the stack? (You can use checksec.sh, objdump, etc., to find out)

c. [4] Where does this program take input?

d. [4] Describe your high-level idea on how to exploit this challenge.

1. [40] Capture the flag of ***overflowret7\_32***. The source code of this challenge is in /code

a. [4] Is this a 32bit or 64-bit program?

b. [4] Is stack executable? Can you overwrite RET address on stack? Is there a canary to protect the stack? (You can use checksec.sh, objdump, etc., to find out)

c. [4] Where does this program take input?

d. [4] Describe your high-level idea on how to exploit this challenge.