**CSE 410/510 Software Security**

**Final CTF**

**Fall 2022**

**Total 200 Points**

**Your full name:**

**Your CSE410/510 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.**

**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.**

1. [50] Exploit challenge-1 to capture the flag.

a. [5] Is this a 32bit or 64-bit program?

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

b. [5] Describe your high-level idea on how to exploit this challenge.

1. [50] Exploit challenge-2 to capture the flag. Source code of this challenge is available.

a. [5] Is this a 32bit or 64-bit program?

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

b. [5] Describe your high-level idea on how to exploit this challenge.

1. [50] Exploit challenge-3 to capture the flag. Source code of this challenge is available.

a. [5] Is this a 32bit or 64-bit program?

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

b. [5] Describe your high-level idea on how to exploit this challenge.

1. [50] Exploit challenge-4 to capture the flag.

a. [5] Is this a 32bit or 64-bit program?

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

b. [5] Describe your high-level idea on how to exploit this challenge.