**CSE 410/510 Software Security**

**Midterm CTF Part 2**

**March 16, 2022**

**Total 80 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.**

**Multiple choice questions. Highlight the correct answer. 5 points for each.**

1. When a process is created, the environment variables and command line arguments are placed at \_\_\_\_.
2. Stack
3. Heap
4. .data section
5. .rodata section

2. Which one of the following descriptions about the Data Execution Prevention (DEP) is CORRECT.

* 1. With DEP, an attacker cannot overwrite the RET address on stack
  2. With DEP, an attacker cannot overwrite the Saved EBP/RBP on stack
  3. With DEP, an attacker cannot execute code on the stack
  4. With DEP, an attacker cannot copy shellcode onto the stack

**CTF Challenges.**

**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.**

3. [35] Exploit challenge-1 to capture the flag.

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

[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)

[4] Where does this program take input?

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

4. [40] Exploit challenge-2 to capture the flag.

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

[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)

[4] Where does this program take input?

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