SP Coursework Part 1
Task 2

1. The vulnerability is Heap-based Buffer Overflow. CWE-122
3. The buffer is allocated on the heap and the adversary can exploit the vulnerability by overwriting adjacent memory to the buffer. The attacker could redirect the program's execution to the attacker's code or arbitrary code (somewhere in the memory) and execute with the permissions of the program. The exploit is called remote code execution and a CVE is CVE-2023-38545.
4. Poor input sanitization gives rise to the double free vulnerability, which is when the free() method is called twice on the same memory address argument. CWE-415
6. Calling the free() method twice with the same argument twice can lead to the heap to become corrupted and a malicious user could overwrite particular registers or memory spaces, and trick the program into executing code of its own choosing. The code could be for a shell with elevated privileges. This was seen in CVE-2023-33952 where a lack of validation of the existence of an object can lead to free operations on it, and a local privileged user could escalate privileges and execute code in the kernel.