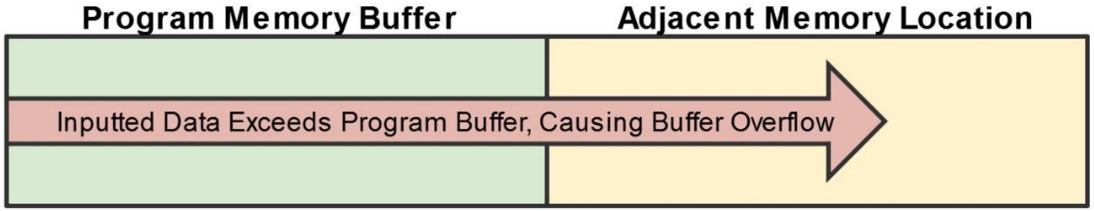
Buffer Overflows

- A **buffer overflow** is a programming error that occurs when a program (or system process) attempts to write more data to a fixed length block of memory (buffer) than the buffer is allocated to store.
- The overflow is then written to adjacent memory locations, which can be exploited with malicious code with the intent to cause an application or system crash or to introduce malware to the system.
- Buffer overflow protections include data input validation, Windows run-time protections, and secure development practices.


Program Memory Buffer
Adjacent Memory Location
Inputted Data Exceeds Program Buffer, Causing Buffer Overflow