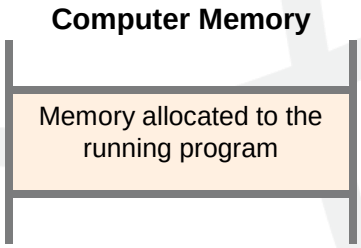
Buffer Overflow Exploit

Out in the real world, the `IndexError` you saw in the fish tank monitoring code is a not an error that would result in a security breach. A coding error that *could* cause a security breach is called a "buffer overflow" error. In computer science, *buffer* means stored memory, so this error has to do with the computer's memory.

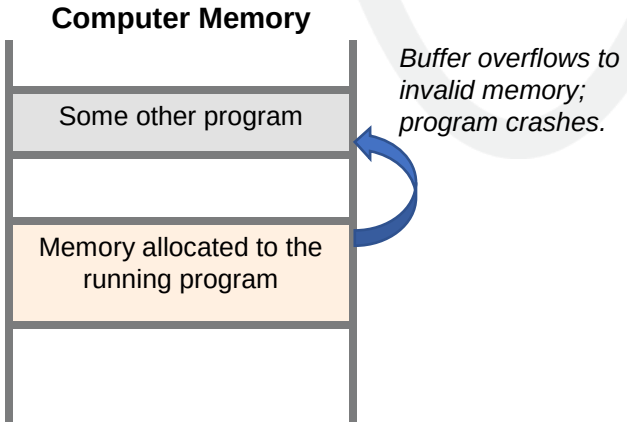
Error-free program

When any program runs on a computer, the operating system gives it memory, called its "program space", in which to run.



Buggy program

In some languages (but not *Python*®), if a program's memory usage is not managed correctly, the program will crash. For example, say you create a variable to store 1000 bytes. Then an error in the code or even some malware attempts to store more than what was allocated, say 1007 bytes. The program tries to access this memory where something else might be running and crashes with a *buffer overflow*.



Buggy program and malware

This is where malware can enter the scenario. A malicious user can install malware so that when the original program hits the buffer overflow, it accesses the malware program instead. The original program seems to be running, but in reality, the malware has taken over and is running on the system.