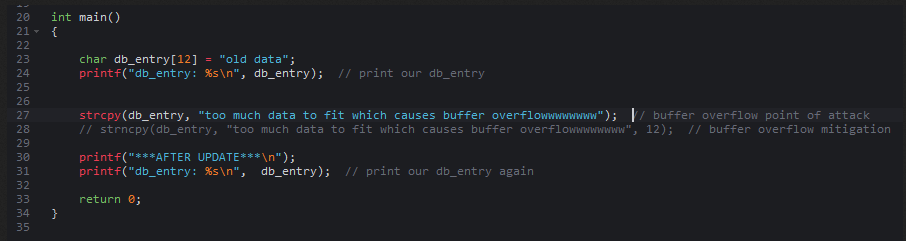
**Buffer overflow**

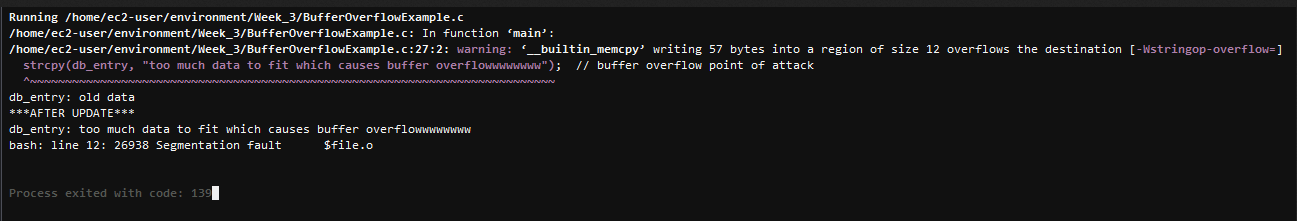
What is a buffer overflow? According to the Common Weaknesses Enumeration (CWE) documentation, a buffer overflow occurs "when a program attempts to put more data in a buffer than it can hold, or when a program attempts to put data in a memory area outside of the boundaries of a buffer" (CWE, 2006). When a buffer overflow occurs, it usually just makes the program crash without any serious damage occurring. However, a sophisticated attacker could cause the program to enter an infinite loop or run arbitrary, malicious code (OWASP, 2021).

I chose to focus on Example 2 (CWE, 2006) which uses the strcpy() function to create a local copy of a buffer. In this example the function is vulnerable to buffer overflow attacks because a user could enter more characters in the string than is expected from the program and C does not automatically check the length of the string to be copied (OWASP, 2021). In the example below, the program (written in C) takes a variable 'db\_entry', and attempts to copy new data into the variable using strcpy() (line 27). However, 'db\_entry' is defined to only allow 12 characters (line 23), causing a buffer overflow.

Code:



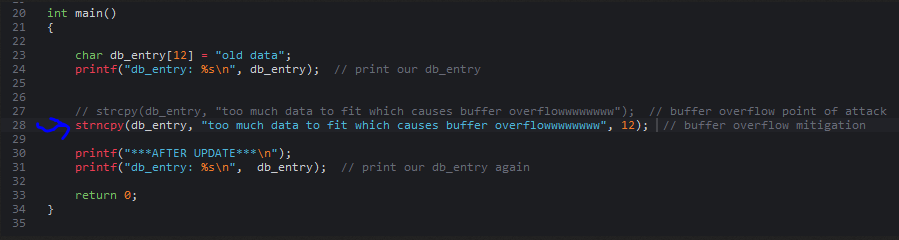
Output:



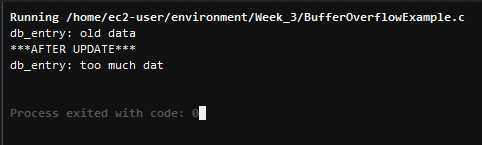
As can be seen in the error message, the program attempted to write 57 bytes into a region size of 12 bytes.

I mitigated this vulnerability by using the strncpy() function rather than the strcpy() function. The strncpy() function takes a third parameter, length of the string being copied, so that the program does not attempt to copy a buffer that is longer than is allotted. The code below uses strncpy() and limits the length to 12 bytes (line 28).

Code:



Output:



Rather than causing a buffer overflow and crashing, the program copies over the first 12 characters and then stops. Ideally, you would also want to implement some additional input validation such as checking the type of the input, the length, checking against a list of acceptable inputs, and so on.

**References**

Common Weaknesses Enumeration (CWE). (2006, July 19). CWE - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow’) (4.4). CWE. Retrieved from <https://cwe.mitre.org/data/definitions/120.html#Demonstrative%20Examples>

Open Web Application Security Project (OWASP). (2021). Buffer Overflow | OWASP. OWASP Foundation. <https://owasp.org/www-community/vulnerabilities/Buffer_Overflow>