Jesse Kniss

CS-405

Module 2 Buffer Overflow

A buffer overflow is a coding vulnerability that can be exploited by hackers to gain unauthorized access to a computer system. (Fortinet, 2022) This exploit is one of the best-known software vulnerabilities, and one of the most common attacks due to the various ways the vulnerability can be exploited. A buffer overflow attack typically happens when a hacker overwrites the bounds of a buffer by manipulating memory addresses. It most commonly occurs when a program relies on external input to control the behavior.

For this assignment, the buffer overflow is triggered when the hacker sends more data than the buffer is assigned to handle. To prevent this type of attack, it’s important to validate all user input, making sure it conforms the bounds of the array. A variable which acts as a flag is created, which will notify the system if the user input is greater than the allowed buffer size. By validating the user input, we can stop attacks by exiting the program and returning a message to the console that an overflow was detected.

# Works Cited

Fortinet. (2022, Mar 14). *Buffer Overflow*. Retrieved from Fortinet Resources: https://www.fortinet.com/resources/cyberglossary/buffer-overflow#:~:text=Also%20known%20as%20a%20buffer,the%20data%20in%20those%20locations.

Text

Description automatically generated