## Abstract

*Cyber security is now one of the most important aspects of information technology. One of the important cyber security is the security of the application. However, the application's attack is still common until now it is no exception in the C programming language-based applications.  Applications with C programming languages are vulnerable to Buffer Overflow attacks. Buffer Overflow occurs when hackers provide excessive input to the program that is running, so the program is overloaded and memory cannot be able to allocate it. There are several methods that are done to detect a buffer overflow attack, one of which is by using Lexical analysis. By using lexical analysis the system can detect functions that are vulnerable to Buffer overflow attacks by utilizing the tokenizing process. Detecting using the Lexical Analysis method can be done that occurs with a Buffer Overflow attack with 90% accuracy with average system running time of 0.0177 seconds.*

**Keywords:** ***Buffer Overflow, Lexical Analysist, Tokenizing***