IMMERSIVE LEARNING ENVIRONMENT

LAB: BUFFER OVERFLOW

LEARNING OBJECTIVE

The objective of this lab is for students to gain knowledge on buffer overflows and dangers they pose to your applications and what techniques attackers use to successfully exploit these vulnerabilities.

DESCRIPTION

A buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers. A buffer overflow, or buffer overrun, occurs when more data is put into a fixed-length buffer than the buffer can handle. The extra information, which has to go somewhere, can overflow into adjacent memory space, corrupting or overwriting the data held in that space. This overflow usually results in a system crash, but it also creates the opportunity for an attacker to run arbitrary code or manipulate the coding errors to prompt malicious actions.

Many programming languages are prone to buffer overflow attacks. However, the extent of such attacks varies depending on the language used to write the vulnerable program. For instance, code written in Perl and JavaScript is generally not susceptible to buffer overflows. However, a buffer overflow in a program written in C, C++, Fortran or Assembly could allow the attacker to fully compromise the targeted system.

COMPONENT SECTIONS

- Game file/folder name: Game
- Movie file name: movie
- Power Point file name: Buffer Overflow.ppt
- Assessment file name: Buffer Overflow Quiz.doc

WHAT TO SUBMIT

Submit the quiz document by answering all the questions.