Security Injections @Towson

Welcome, Marilyn Soyars!

Security Injections, Java CS1 - Buffer Overflow

1. Background | 2. Code Responsibly | 3. Laboratory Assignment | 4. Discussion Questions

Discussion Questions

(Note: You may want to refer Background and Code Responsibly sections to answer the Discussion Questions.)

Question 1

Describe the buffer overflow problem.

A buffer overflow happens when a program attempts to access a value that is outside of the specified data buffer. ✓

Question 2

What happens if you exceed the size of an array in Java? Do you consider this robust behavior?

Question 3

List three ways you could potentially overflow a buffer or exceed the size of an array in your program.

Using user input value to index an array without verifying that it has an appropriate value
Having a loop counter that increments an index variable so it goes beyond the end of a data array.
Copy multiple items from one array to another without verifying that they can fit ✓

Question 4

How could you prevent a buffer overflow from occurring in your program?

Make sure you have enough space
Check index values
Beware of code that copies items from one array to another ✓

Question 5

Give three real life examples of buffer overflow attacks (research on the web).

The 1998 Morris Internet Worm
2001 Code Red Worm – Microsoft Internet Information Services
2003 SQL Slammer – Microsoft SQL Server 2000 ✓

Question 6

What can result from a buffer overflow

The potential impact of a buffer overflow will largely depend on the programming language. Some languages, such as Java, automatically identify situations that would lead to buffer overflows. These languages will generally indicate an error by throwing an exception, which the program should handle appropriately. If exceptions are not handled, the program will terminate. ✓

Question 7

Buffer overflows can be troublesome if they are used by attackers to run their own code. What sort of things might an attacker try to do if he or she were able to run any code they wanted on a computer?

Directly malicious attackers might destory data or otherwise render the computer unusable. Criminals in search of useful information might try to read files, looking for credit card numbers, social security numbers, and other information that can be useful for theft, fraud, and identity theft. Others might use an attacked computer to run software that will be used to attack still other computers, creating an army of ✓

Complete! Finish

This project is supported by the National Science Foundation under grants DUE-1241738 and DUE -0817267. Any opinions, findings, conclusions, or recommendations expressed are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Powered by a modified version of Class2Go