Programmers' and Code Inspectors' Checklist:

Is every array index and pointer arithmetic operation…

- Okay given the preconditions and data assumptions?
- Checked for size before data is entered into the buffer?

Is every library function call…

- A safe library function call?
- Given the correct input in terms of number of characters or size of the buffer? Be careful of off-by-one errors.

Has all reused code…

- Been inspected for buffer overflow problems?
- Been checked for differences in data size such as the difference between ASCII and UNICODE?

Testers' Checklist:

Were all string inputs tested with a very long string to see if…
- The program crashes?
- Data is corrupted?

Were all non-string buffered inputs tested with too much data to see if…
- The program crashes?
- Data is corrupted?

Were all inputs that get reformatted into a buffer tested…
- With their maximum and minimum values?
- On the boundaries of all other partitions (i.e. you should test something with zeros in it like 4005 or 4000 for a program that converts decimal integers to ternary strings)?

Was all of the new code tested…
- On every platform that the software is intended to run on?
- With all possible settings that could affect it?

Was all of the old code tested…
- Under the new assumptions?
- With any changes in data size such as the difference between ASCII and UNICODE?
- On every platform that the software is intended to run on?

This Document was Funded by the National Science Foundation Federal Cyber Service Scholarship For Service Program: Grant No. 0113627

For more information, go to: http://nsfsecurity.pr.erau.edu
or contact Susan Gerhart, gerharts@erau.edu
Embry-Riddle Aeronautical University • Prescott, Arizona • USA

Also available are:

- Demonstrations of how buffer overflows occur (Java applets)
- PowerPoint lecture-style presentations on an introduction to buffer overflows, preventing buffer overflows (for C programmers), and a case study of Code Red
- Checklists and Points to Remember for C Programmers
- An interactive module and quiz set with alternative paths for journalists/analysts and IT managers as well as programmers and testers
- A scavenger hunt on implications of the buffer overflow vulnerability

Please complete a feedback form at http://nsfsecurity.pr.erau.edu/feedback.html to tell us how you used this material and to offer suggestions for improvements.