Lecture 4

Friday, 25 November 2022 15:35

in C: a 'string' of length 10 is an array of length 10, containing 9 characters + 1 terminating character

1. buffer overflow is possible
2. overwrite return address does not raise alarms
3. malicious code must be executable
4. return address must map to malicious code

Common weaknesses:

out-of-bound write

improper input validation

out-of-bounds read

use after free

NULL pointer dereference

integer overflow

improper restriction of operations within the bounds of a memory buffer

Uncontrolled resource consumption