Memory Disclosure Vulnerability

- read/leak memory contents
  (ideally arbitrary)

vs.

Memory Corruption Vulnerability

- write/alter memory contents
  (ideally arbitrary)
Memory Disclosure Vuln.

- read/leak memory contents
  (ideally arbitrary)

vs.

Memory Corruption Vuln.

- write/alter memory contents
  (ideally arbitrary)

(can be abused to construct mem. disclosure vulns.)
Format String

La format specifications

"Hello world.\n" → Hello world!

"Hello world %d\n", ω → Hello world %d

unsigned int → string/char[]

"Hello %s\n", Ω → Hello %s

unsigned int → string/char[]

printf("%d\n", 1, 2, 3)

% N $ x