# Why doesn't "*gets()*" get it?

*Or more formally:*

An investigation into the use of the buffer overflow vulnerability in the C function *gets()*.

# Scope of research

Compare *gets()* function with *strcpy()* function, looking for area(s) where differences in code may contribute to differences in exploit behavior.

# Research plan

1. Compare C code of *strcpy()* & *gets()*
2. Compare assembly code of *strcpy()* & *gets()*
3. Find suspicious areas that might explain difference in exploit behavior between *strcpy()* & *gets()*
4. Determine how this difference might be used to exploit *gets()* in a new way