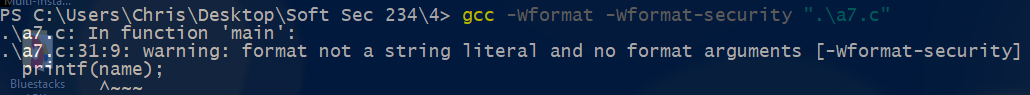
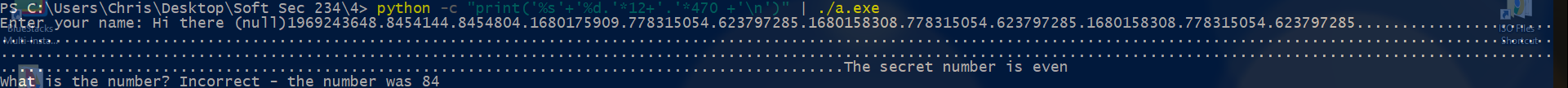
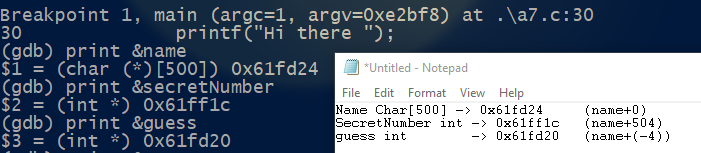
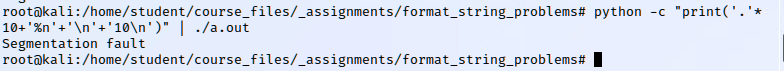
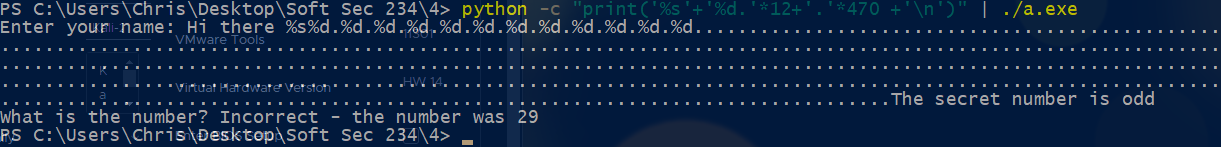
**Discovery**save time looking through the code.  
  
  
this printf() interperets the user controlled variable “name” without feeding it into a format string literal.

**proof of vulnerability:**  
printing garbage from the stack, no idea what’s what  
pulling up debug info to identify offsets of target variables  
  
I was not able to gain control of the program, however I understand that secretNumber can be written to by accessing the particular offset in the stack using the argument specifier “$” paired with %n, to write a known value. I didn’t compile it with all the fancy flags to remove security features though – so maybe that’s the reason I can’t.  
  
Whenever I fed the command line a “$” the script would break down, or I would get a segfault if I was typing it in manually to the program prompts.



**Fix:**  
  
substituting a string literal which interprets the variable as a string prevents interpretation of format specifiers in the user-provided string itself.