This is examining strings in C/C++.

What are some different string vulnerabilities?

* Improperly bounded strings
* Copying and Concatenating Strings
* Printing strings
* Off-by-one errors
* Truncation

How could someone exploit these vulnerabilities?

* Command line arguments
* Environment Variables
* Console input
* Text/Configuration/Data files
* Network connections

How could someone find these vulnerabilities?

* Examining source code
* Accidently crashing program
* Reverse Engineering in x64dbg for crashes – fuzz with python scripts

We also don’t want to forget that someone could find hard coded string credentials if examining with x64dbg.

# Improperly bounded strings

See “outofbounds.exe” in ".\outofbounds\Debug\” for the code. Essentially, the user is prompted for the password, which is of a preset size, and compared to a static string. An exploit can be found in this same directory labled “outofbounds.py”. The fixed c++ code is labled “inbounds.cpp”.

I first put the program into x64dbg. I found where the comparison was, put a breakpoint on it, and found the hard coded password.

I can see the size of the buffer that stores my password.

I can see all of my after code gets dumped to:

I generate the payload to pop the calculator with: