**Reversing**



Opened docker container.

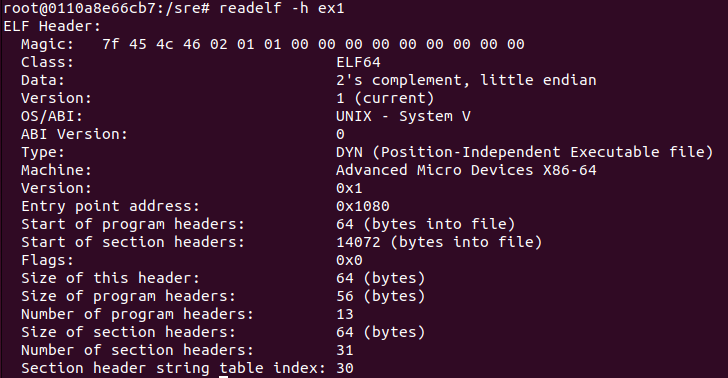


Navigated to /sre directory where I unzipped the files.



Ran gcc to compile and produce executable ex1.

Problem 1



1. Ran readelf to show all ELF sections of ex1.
2. The difference between an object file and an executable is that an object file contains machine code that is not directly executable. It requires linking to libraries in order for it to become an executable. An executable contains instructions which the computer (CPU) directly runs.
3. Text is the section which holds the code & instructions for the executable to run. Data is where global and static variables that have been initialized are stored. Rodata means read-only data, which is used to store constants. Bss stands for block start by symbol and is the space for uninitialized variables in the code.

Problem 2

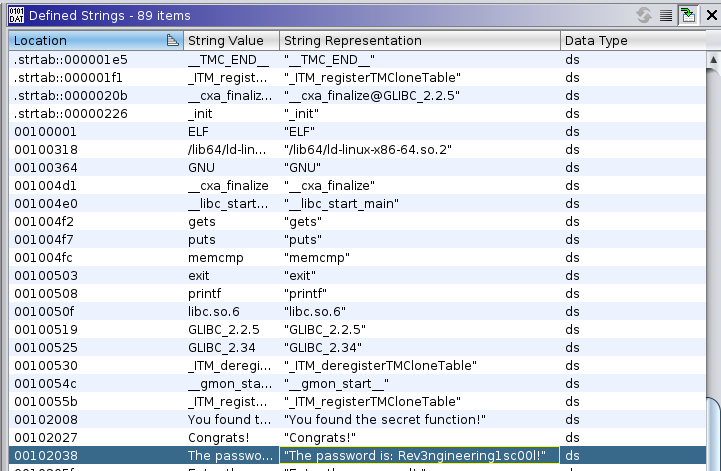
1. A more optimized solution would be to start the program with LD\_PRELOAD
2. “strcmp” can always succeed by doing export LD\_PRELOAD
3. There is much lower security by making it always succeed, since all users regardless of permissions can bypass this check.

Problem 3

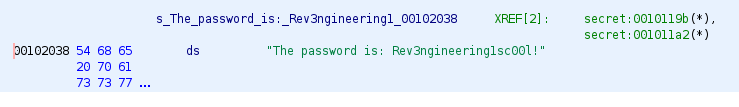
To Harden a system against interposing, always unset the PRELOAD variable before compilation. Alternatively, you can implement checks to see if PRELOAD has been initialized and prevent its usage.

Problem 4

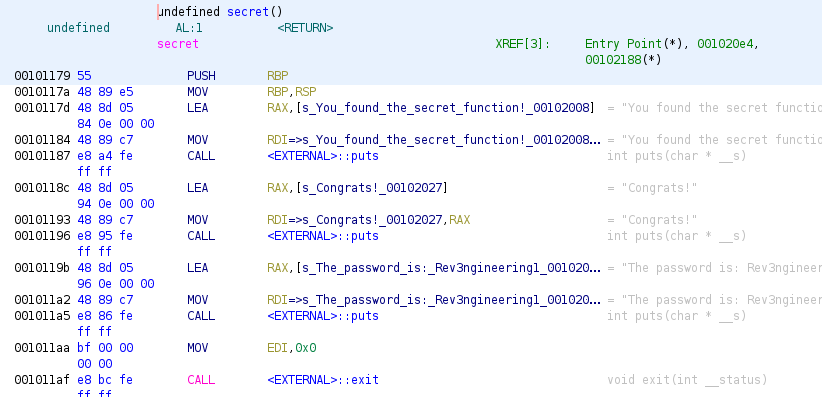
We first open the program in Ghidra.



By going to Window>DefinedStrings, we can find a string which contains the password.



Under the Program Trees > .rodata section, we can also find a mention of the password.



From the Symbol Tree > Exports there is a file suspiciously named secret. In there we can again discover a mention of the password.

References

<https://pediaa.com/what-is-the-difference-between-object-file-and-executable-file/>

<https://blog.katastros.com/a?ID=00750-f28db8b2-67f6-4a3b-b10c-1495756e3c58>

<https://medium.com/iqube-kct/know-what-is-bss-text-data-memory-segments-of-an-executable-file-in-embedded-systems-6158d92aa519>