Challenge: Wide

Challenge Description :

We've received reports that Draeger has stashed a huge arsenal in the pocket dimension Flaggle Alpha. You've managed to smuggle a discarded access terminal to the Widely Inflated Dimension Editor from his headquarters, but the entry for the dimension has been encrypted. Can you make it inside and take control?

Context :

- We are given a compiled file, when we run the file it pops up with a weird TUI interface . Going on one of the options by inputting the names in as a numeric list, e.g Primus = 1 and Cheagaz = 2. . Selecting the Option six asks for a password as it is shown as “Encrypted”.

Notes :

- Tools:
    - Text editor - To open the bash script / downloaded files.
    - You can choose your way to decoding the base64 string for simplicity im going to use a website, “www.base64decode.org”

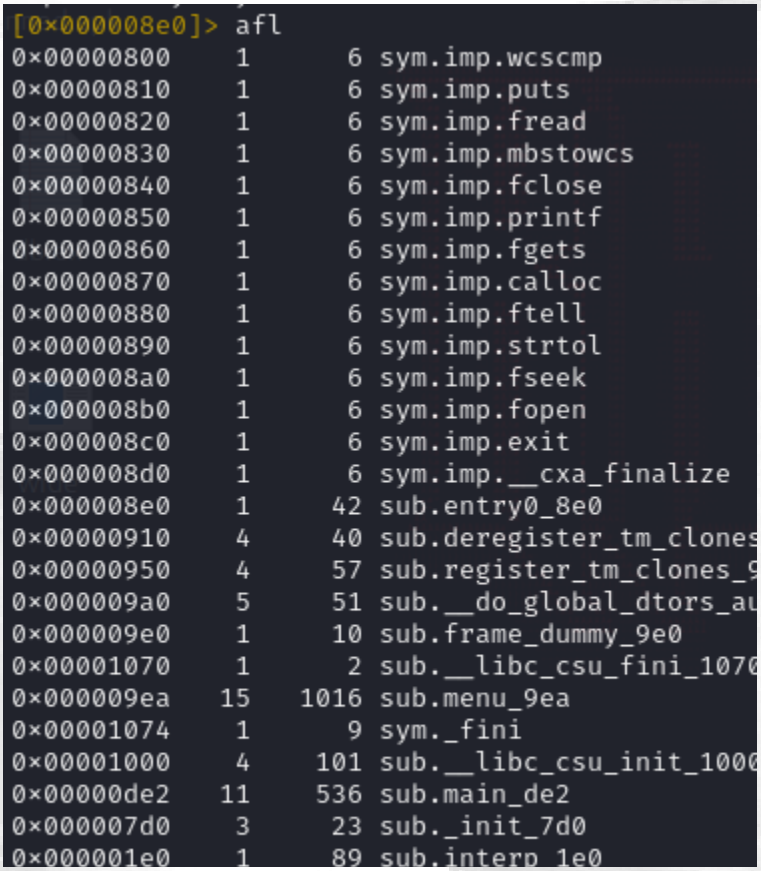
Flag :

- Download the file and run it. I started doing some basic static analysis on the file using Strace , Ltrace, objdump and some other tools. I couldn't find anything interesting or anything linking to a password.

```
birdo@DESKTOP-0ENQDDA:/mnt/d/HackTBox/Wide/rev_wide$ ./wide db.ex
[*] Welcome user: kr4eq4L2$12xb, to the Widely Inflated Dimension Editor [*]
[*]    Serving your pocket dimension storage needs since 14,012.5 B      [*]
[*]                        Displaying Dimensions....                     [*]
[*]       Name        |              Code                |   Encrypted    [*]
[X] Primus            | people breathe variety practice  |                [*]
[X] Cheagaz           | scene control river importance   |                [*]
[X] Byenoovia         | fighting cast it parallel        |                [*]
[X] Cloteprea         | facing motor unusual heavy       |                [*]
[X] Maraqa            | stomach motion sale valuable     |                [*]
[X] Aidor             | feathers stream sides gate       |                [*]
[X] Flaggle Alpha     | admin secret power hidden        |       *        [*]
Which dimension would you like to examine?
```

- When that fails, when I did some dynamic analysis on the file starting with IDA freeware, I got nothing from extracting strings or from just reading the binary.
- Instead I went to run it against another tool called Radare2, using this I got a better analysis and found something interesting. Using Radare2 was weird to start off with but finally got a slight handle.
- Opening it, i ran a command, [AFL] to show a bunch of Entries to enter as well as how the file was structured, i can enter the entries and print the binary of them entering the command : [pdf@(data_entry_name)]

  E.g [pdf@sym.imp.fread]

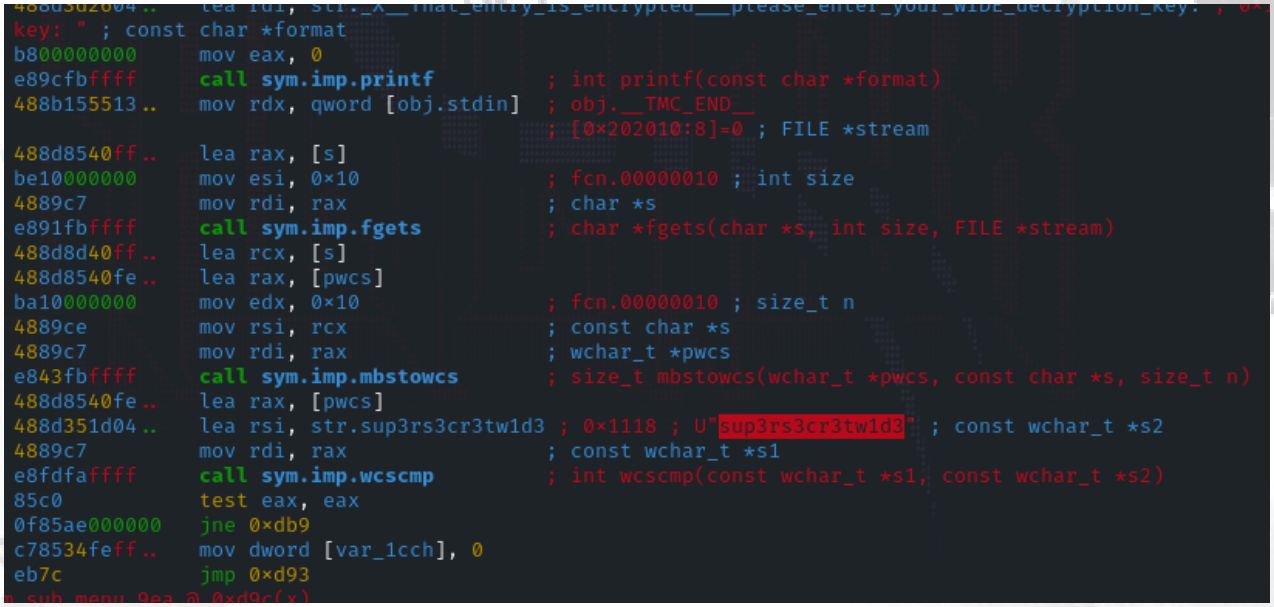


- Using this i opened the main entry, got nothing, same with some sub files, i Finally opened a entries that gave me the password for the application :

  [pdf@sym.menu]

- Either short for system menu or something else It should have been one of the first things to check based on what we are checking out.

- The Password is placed at the bottom of the result of the [sym.menu] Command i gave, the password in question being : sup3rs3cr3tw1d3



- Running the file again and going to the six option to prompt in the password gave us the flag : HTB{som3_str1ng5_4r3_w1d3}