Challenge:

Find The Easy Pass

# Challenge Description:

Spying time. Check what all users have been up to with this Challenge recently.

# Context:

## Decompile a Wine Windows Application

* + - We will be dynamically analyzing the file as we need to

Be able to execute the program to better find the password.

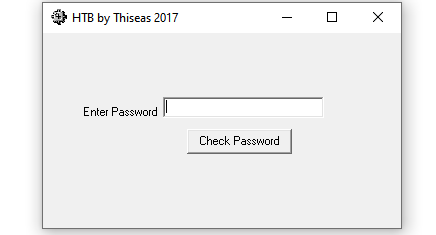
# Notes:

* Using Winedbg for the binary of the application.
  + - Try to cross reference the Binary for a password

# Challenge:

* First we download the files, and unzip them with the HTB password given. Hint it the same password till you do sherlocks or machines.
* We then run the wine application to see what we are dealing with,

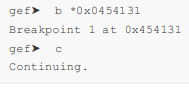
It seems to be a window prompting us to enter a password.



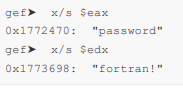
* We then run it with winedbg to find any cross-references with the strings from the Windows box’s either ”Correct Password“ or “Wrong Password”.

# Flag:

* After Seeing this we set a breakpoint before the do\_check function is called.



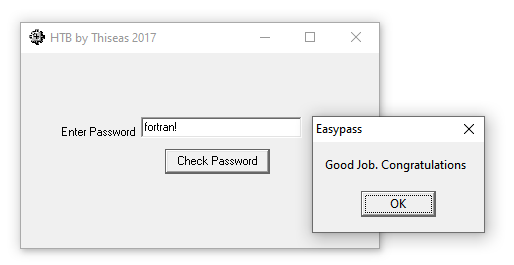
* After setting the breakpoint, run it, hoping that the $eax and $edx have passed the value into the function in the program so we can inspect it.



* We can now suggest that ‘fortran!’ is the password for the application.

When we enter the password it just responds with Good Job, We can now just assume that the password is the flag without the flag format.

We get the flag : HTB{fortran!}



From Birdo