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.

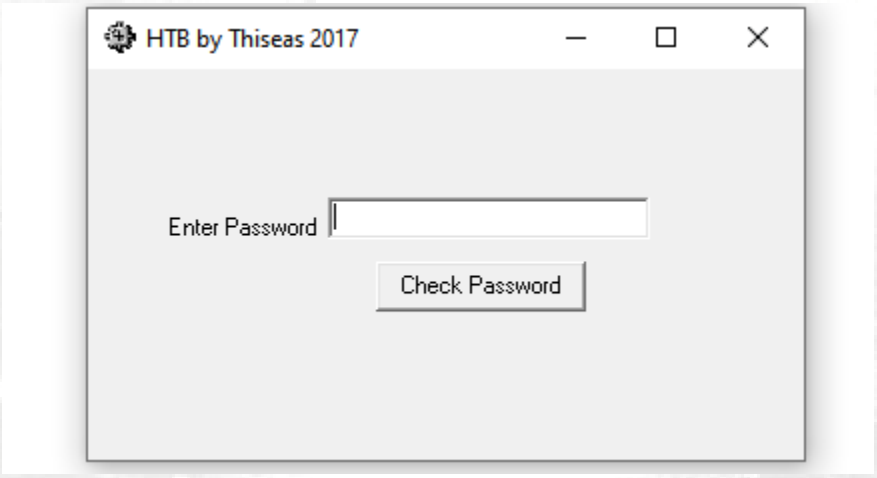
Notes:

- 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".

```
00454118  call    sub_40459c
0045411d  lea     edx, [ebp-0x28]
00454120  mov     eax, dword [ebx+0x2f8]
00454126  call    sub_433110
0045412b  mov     eax, dword [ebp-0x28]
0045412e  mov     edx, dword [ebp-0x4]
00454131  call    do_check
00454136  jne     0x454144

00454138  mov     eax, congrats  {"Good Job. Congratulations"}
0045413d  call    showmsgbox
00454142  jmp     0x45414e

00454144  mov     eax, password  {"Wrong Password!"}
00454149  call    showmsgbox
```

Flag:

- After Seeing this we set a breakpoint before the do_check function is called.

```
gef➤  b *0x0454131
Breakpoint 1 at 0x454131
gef➤  c
Continuing.
```

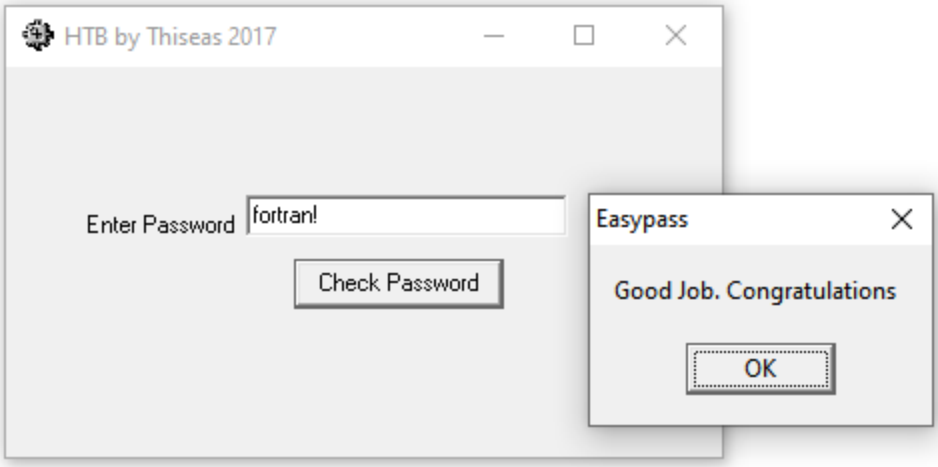
- After setting the breakpoint, run it, hoping that the $eax and $edx have passed the value into the function in the program so we can inspect it.

```
gef➤  x/s $eax
0x1772470:  "password"
gef➤  x/s $edx
0x1773698:  "fortran!"
```

- 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!}


HTB by Thiseas 2017
Enter Password
fortran!
Check Password
Easypass
Good Job. Congratulations
OK

From Birdo