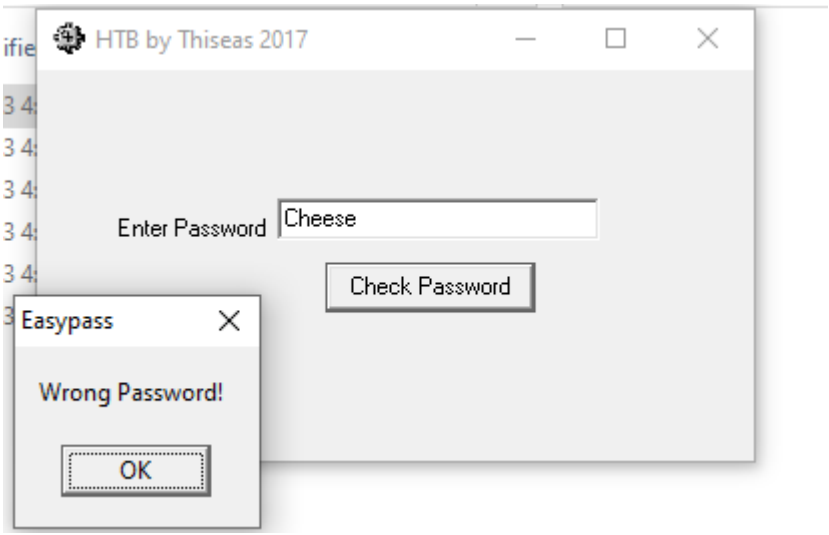
Find The Easy Pass

Function:

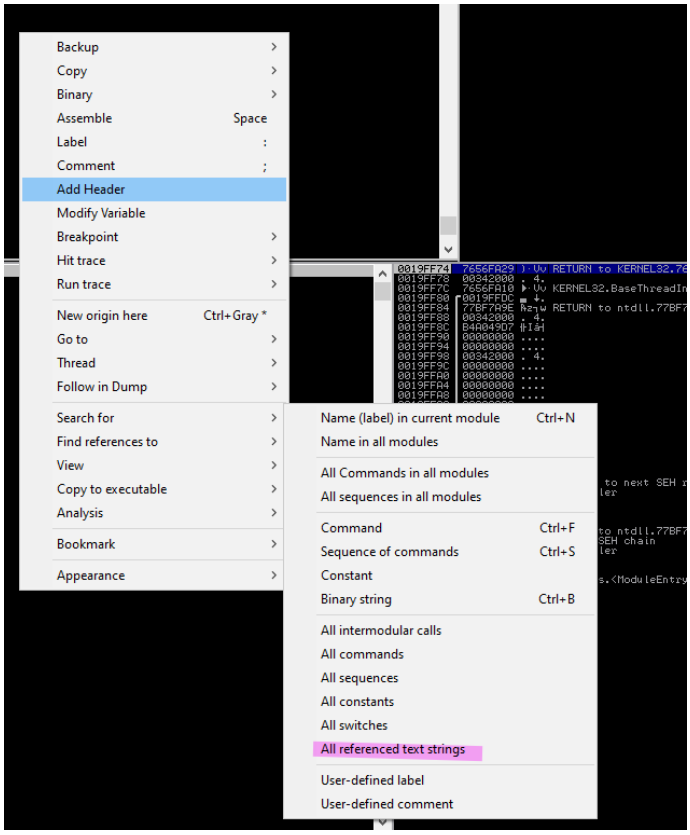


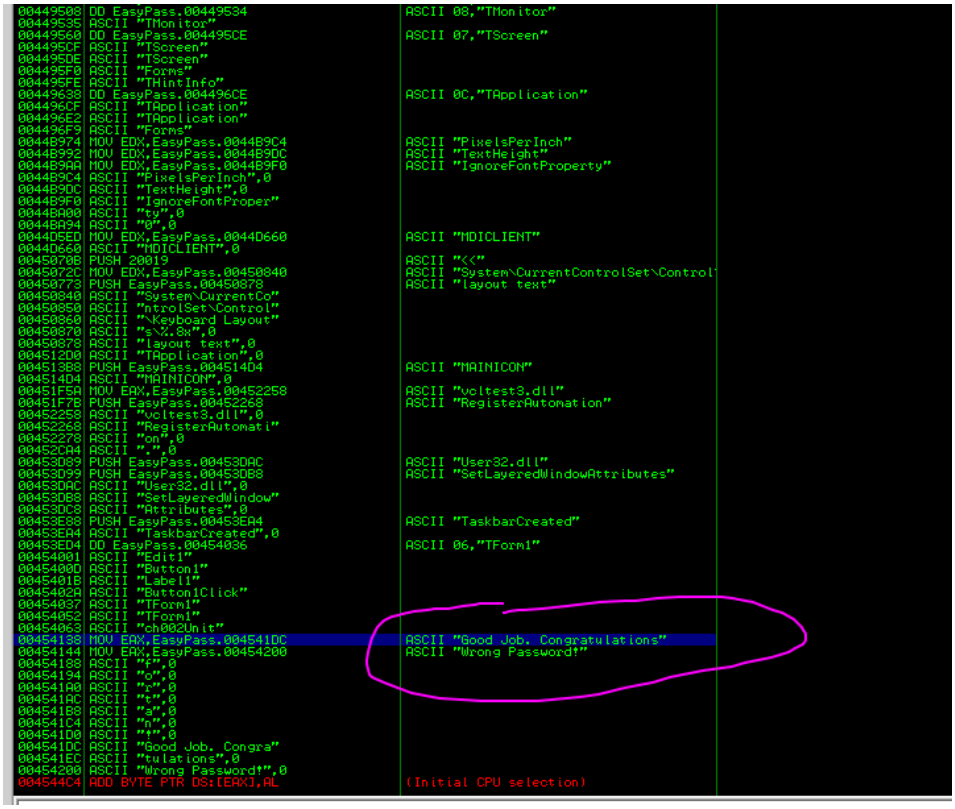
The disassembly in has way too many functions to manually look through and looks obfuscated so it's not plain to see what's going on using static analysis, so dynamic analysis is needed.

There it looks like [ebp+var_28] and [ebp+var_4] are being compared and if they are not equal then it jumps to wrong password.

Presumably the user input is pushed onto the stack after the string, but who knows

Using Immunity, search for the Wrong Password string so we can add a breakpoint at the jnz instruction to see what values are there and what is being compared:



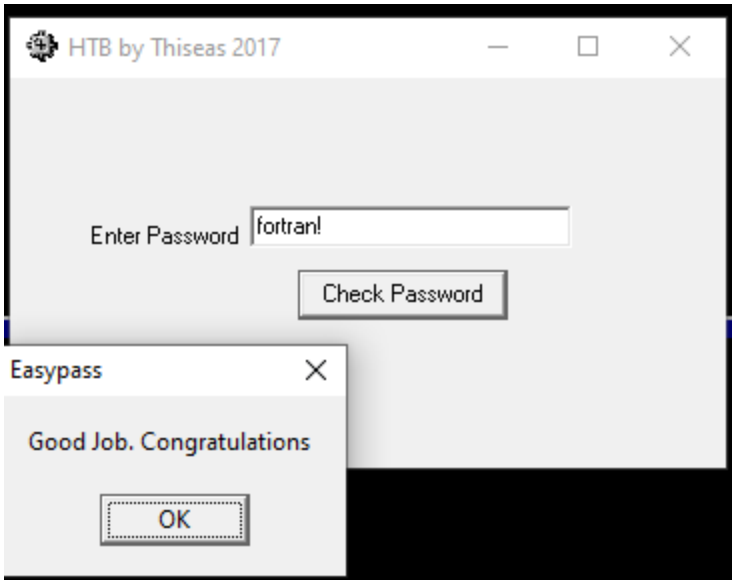


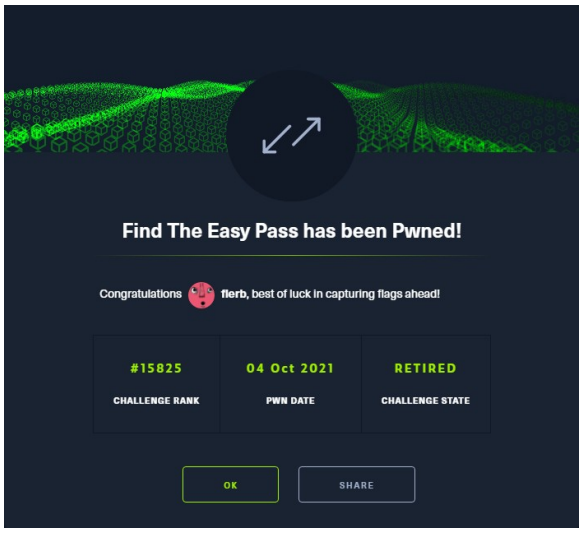
Clicking the Good Job, Congratulations takes us to where it's referenced in the program, set a breakpoint on the Call directly before the JNZ:

```
0045410D  . FF75 DC        PUSH DWORD PTR SS:[EBP-24]
00454110  . 8D45 FC        LEA EAX,DWORD PTR SS:[EBP-4]
00454113  . BA 08000000    MOV EDX,8
00454118  . E8 7F04FBFF    CALL EasyPass.0040459C
0045411D  . 8D55 D8        LEA EDX,DWORD PTR SS:[EBP-28]
00454120  . 8B83 F8020000  MOV EAX,DWORD PTR DS:[EBX+2F8]
00454126  . E8 E5EFFDFF    CALL EasyPass.00433110
0045412B  . 8B45 D8        MOV EAX,DWORD PTR SS:[EBP-28]
0045412E  . 8B55 FC        MOV EDX,DWORD PTR SS:[EBP-4]
00454131  . E8 F204FBFF    CALL EasyPass.00404628
00454136  . 75 0C          JNZ SHORT EasyPass.00454144
00454138  . B8 DC414500    MOV EAX,EasyPass.004541DC          ASCII "Good Job. Congratulations"
0045413D  . E8 EE38FDFF    CALL EasyPass.00427A30
00454142  . EB 0A          JMP SHORT EasyPass.0045414E
00454144  > B8 00424500    MOV EAX,EasyPass.00454200          ASCII "Wrong Password!"
00454149  . E8 E238FDFF    CALL EasyPass.00427A30
0045414E  > 33C0           XOR EAX,EAX
00454150  . 5A             POP EDX
00454151  . 59             POP ECX
00454152  . 59             POP ECX
```

After running the program and entering Cheese as a password the comparison appears to be [EBP-4], [EBP-28], aligning the stack window to EBP shows that [EBP-4] is "fortran!".

```
EBP-50    00672440 @$g. ASCII "Cheese"
EBP-4C    0043313B ;1C. EasyPass.0043313B
EBP-48    0019F568 hJ↓.
EBP-44    0042CC54 T╠B. EasyPass.0042CC54
EBP-40    00671E7C |▲g.
EBP-3C    0045412B +AE. EasyPass.0045412B
EBP-38    0019F71C ∟*↓. Pointer to next SEH record
EBP-34    00454171 qAE. SE handler
EBP-30    0019F3EC «≤↓.
EBP-2C    00673C80 Ç<g.
EBP-28    00672440 @$g. ASCII "Cheese"
EBP-24    004541D0 ╨AE. EasyPass.004541D0
EBP-20    004541C4 ─AE. EasyPass.004541C4
EBP-1C    004541B8 ╕AE. EasyPass.004541B8
EBP-18    004541A0 àAE. EasyPass.004541A0
EBP-14    004541AC ¼AE. EasyPass.004541AC
EBP-10    004541A0 àAE. EasyPass.004541A0
EBP-C     00454194 öAE. EasyPass.00454194
EBP-8     00454188 êAE. EasyPass.00454188
EBP-4     00673668 h6g. ASCII "fortran!"
EBP ==>   0019F52C ,J↓.
EBP+4     004346AA ¬FC. RETURN to EasyPass.004346AA
```




Find The Easy Pass has been Pwned!
Congratulations flerb, best of luck in capturing flags ahead!
#15825
CHALLENGE RANK
04 Oct 2021
PWN DATE
RETIRED
CHALLENGE STATE
OK
SHARE