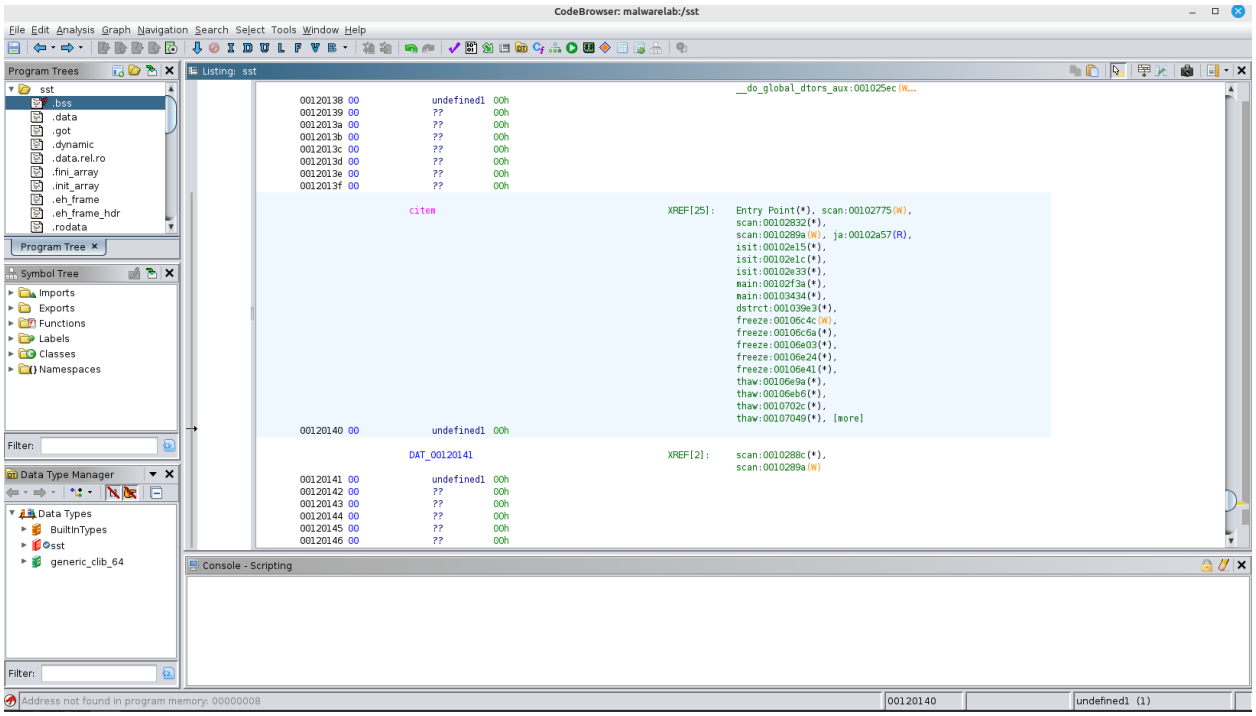
Mark Garcia 018019103
5/15/2023

LAB 3: Malware

Searching for the self destruct function:

I opened sst in ghidra and scrolled through the .bss file and towards the bottom, after all the dialogue options, i saw the dstrct function.



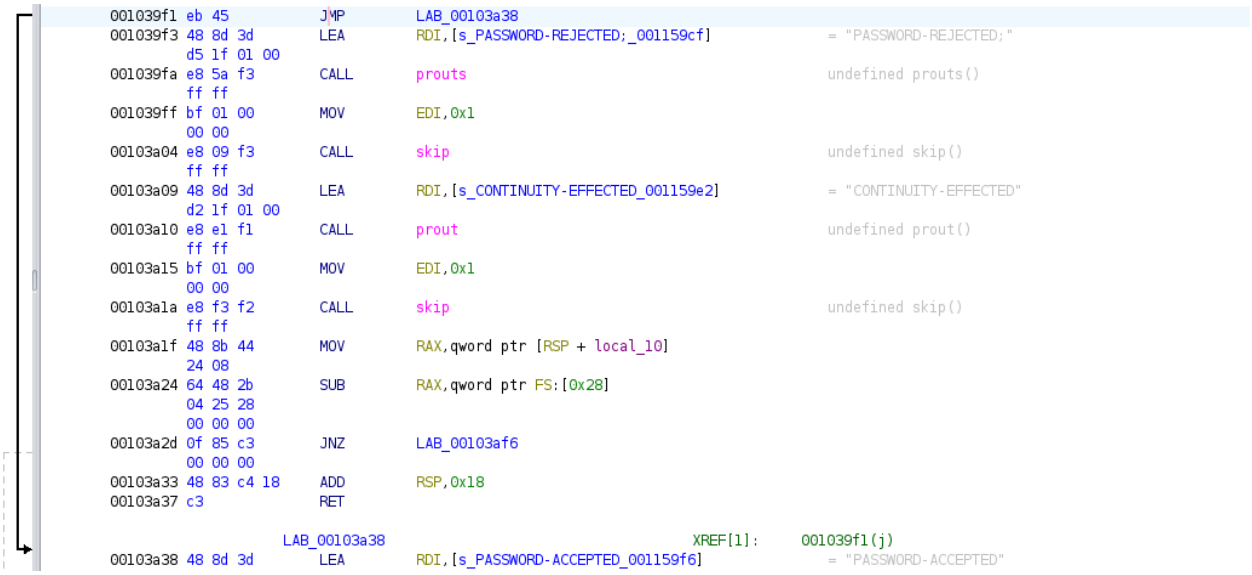
Double clicking it brought me to this page where i am assuming checks the password for the self destruct function

```
001039bc 48 8d 3d        LEA        RDI,[s_SELF-DESTRUCT-SEQUENCE-WILL-BE-A_00115e...  = "SELF-DESTRUCT-SEQUENCE-WILL-B...
         45 24 01 00
001039c3 e8 2e f2        CALL       prout                                              undefined prout()
         ff ff
001039c8 e8 75 ed        CALL       scan                                               undefined scan()
         ff ff
001039cd e8 28 ed        CALL       chew                                               undefined chew()
         ff ff
001039d2 48 b8 21        MOV        RAX,0x7470677461686321
         63 68 61
         74 67 70 74
001039dc 48 89 04 24     MOV        qword ptr [RSP]=>local_18,RAX
001039e0 48 89 e7        MOV        RDI,RSP
001039e3 48 8d 35        LEA        RSI,[citem]
         56 c7 01 00
001039ea e8 01 ea        CALL       <EXTERNAL>::strcmp                                 int strcmp(char * __s1, char * _...
         ff ff
001039ef 85 c0           TEST       EAX,EAX
001039f1 74 45           JZ         LAB_00103a38
001039f3 48 8d 3d        LEA        RDI,[s_PASSWORD-REJECTED;_001159cf]                = "PASSWORD-REJECTED;"
         d5 1f 01 00
001039fa e8 5a f3        CALL       prouts                                             undefined prouts()
         ff ff
001039ff bf 01 00        MOV        EDI,0x1
         00 00
00103a04 e8 09 f3        CALL       skip                                               undefined skip()
         ff ff
00103a09 48 8d 3d        LEA        RDI,[s_CONTINUITY-EFFECTED_001159e2]               = "CONTINUITY-EFFECTED"
         d2 1f 01 00
00103a10 e8 e1 f1        CALL       prout                                              undefined prout()
         ff ff
00103a15 bf 01 00        MOV        EDI,0x1
         00 00
00103a1a e8 f3 f2        CALL       skip                                               undefined skip()
         ff ff
```

Now all i have to do is bypass the strcmp or make it so the result of strcmp goes to the password accepted option, bypassing the self destruct password check. First I located the self destruct function in the symbol tree and then click “ctrl + e” to open the C psudocode that represents the assembly. The line

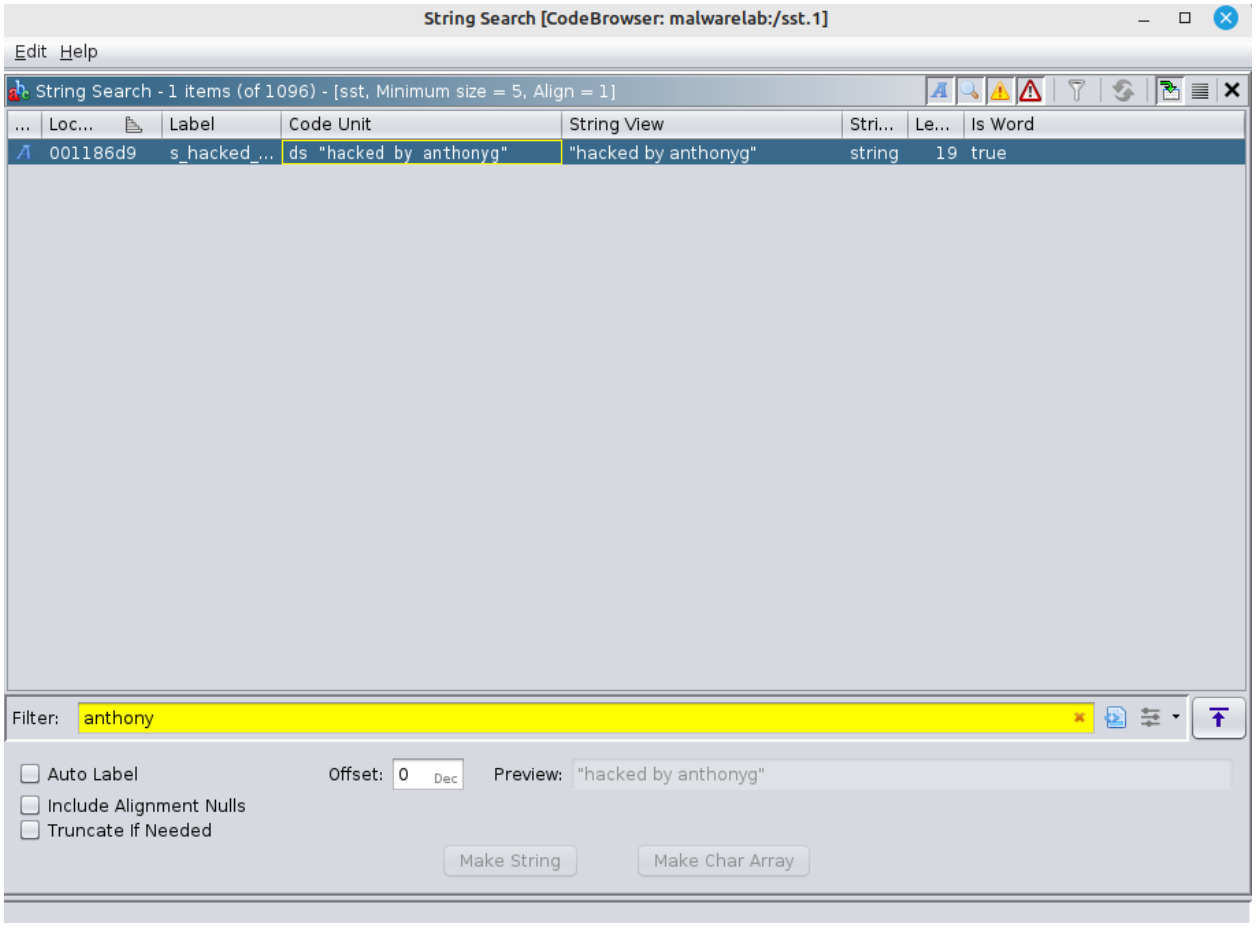
if (iVar1 == 0) {.....}

is what checks if the password matches the self destruct password. If I make this check result in true all the time then it doesnt matter what the password is or instead of having a conditional *JZ* jump, what if I were to just use an unconditional *JMP* jump instead to go straight to password accepted.



Adding name to hacking credits:

I used the search for string function in ghidra and applied the filter to search for “anthony”. Only one location popped up, so I’ll just include myself in the credits here.



Adding my name to the very end says it was too long to i just adjusted the string to be:

```
                        s_hackbymark&anthonyg_001186d9
001186d9 68 61 63           ds          "hackbymark&anthonyg"
         6b 62 79
         6d 61 72 ...
```

For some reason the release of ghidra I was using did not have the option to export sst as a binary file, so I am unable to test if my changes were correct but in theory, The change from JZ to JMP will result in an unconditional jump to call the *password accepted* sequence. And adding my name to the hacker credits was done by altering the hex values in the screenshot above.