Reversing.kr Music Player 4 풀이

리버싱 문제풀이 / Wonlf / 2022. 5. 13. 23:10


```
00404556   50              push eax
00404557   FF15 3C104000   call dword ptr ds:[<&__vbaHresultCheckObj>]
0040455D   8B85 5CFFFFFF   mov eax,dword ptr ss:[ebp-A4]
00404563   3D 60EA0000     cmp eax,EA60
00404568   8945 E8         mov dword ptr ss:[ebp-18],eax
0040456B   0F8C 8D000000   jl music_player.4045FE
00404571   8B0E            mov ecx,dword ptr ds:[esi]          esi:"pt@"
00404573   56              push esi                            esi:"pt@"
00404574   FF91 08070000   call dword ptr ds:[ecx+708]
0040457A   3BC3            cmp eax,ebx
0040457C   7D 12           jge music_player.404590
0040457E   68 08070000     push 708
00404583   68 C0254000     push music_player.4025C0
00404588   56              push esi                            esi:"pt@"
00404589   50              push eax
0040458A   FF15 3C104000   call dword ptr ds:[<&__vbaHresultCheckObj>]
00404590   B9 04000280     mov ecx,80020004
00404595   B8 0A000000     mov eax,A                           A:'\n'
0040459A   894D A8         mov dword ptr ss:[ebp-58],ecx
0040459D   894D B8         mov dword ptr ss:[ebp-48],ecx
004045A0   894D C8         mov dword ptr ss:[ebp-38],ecx
004045A3   8D55 90         lea edx,dword ptr ss:[ebp-70]
004045A6   8D4D D0         lea ecx,dword ptr ss:[ebp-30]
004045A9   8945 A0         mov dword ptr ss:[ebp-60],eax
004045AC   8945 B0         mov dword ptr ss:[ebp-50],eax
004045AF   8945 C0         mov dword ptr ss:[ebp-40],eax
004045B2   C745 98 AC2B4000 mov dword ptr ss:[ebp-68],music_player.402BAC  402BAC:L"1분 미리듣기만 가능합니다."
```

압축 해제를 하고 보니, ReadMe.txt가 있다 읽어보겠다.

```
This MP3 Player is limited to 1 minutes.
You have to play more than one minute.

There are exist several 1-minute-check-routine.
After bypassing every check routine, you will see the perfect flag.
```

해석해보면

"이 음악 플레이어는 재생 시간이 1분으로 정해져 있다. 1분보다 더 재생할 수 있게 만들어야 한다."

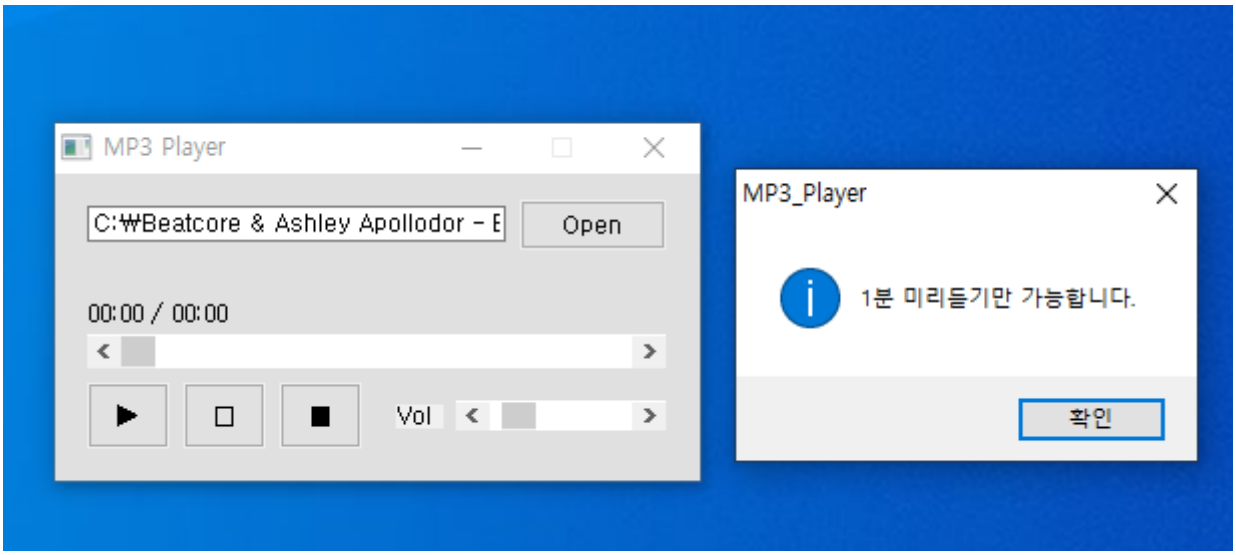
"1분 체크 루틴은 여러개 있다. 루틴을 우회하고 나면 플래그를 보게 될 것이다."

라고 한다.

Die로 열어보자.

Visual Basic으로 짜여있는 프로그램이고 특이사항은 보이지 않는다.

프로그램을 실행시켜보자.



음악 재생 플레이어이고, 1분이 지나자 특정 메시지가 출력 되었다.

디버거로 열어본다.

```
00404556    50              push eax
00404557    FF15 3C104000   call dword ptr ds:[<&__vbaHresultCheckObj>]
0040455D    8B85 5CFFFFFF   mov eax,dword ptr ss:[ebp-A4]
00404563    3D 60EA0000     cmp eax,EA60
00404568    8945 E8         mov dword ptr ss:[ebp-18],eax
0040456B    0F8C 8D000000   jl music_player.4045FE
00404571    8B0E            mov ecx,dword ptr ds:[esi]                  esi:"pt@"
00404573    56              push esi                                    esi:"pt@"
00404574    FF91 08070000   call dword ptr ds:[ecx+708]
0040457A    3BC3            cmp eax,ebx
0040457C    7D 12           jge music_player.404590
0040457E    68 08070000     push 708
00404583    68 C0254000     push music_player.4025C0
00404588    56              push esi                                    esi:"pt@"
00404589    50              push eax
0040458A    FF15 3C104000   call dword ptr ds:[<&__vbaHresultCheckObj>]
00404590    B9 04000280     mov ecx,80020004
00404595    B8 0A000000     mov eax,A                                   A:'\n'
0040459A    894D A8         mov dword ptr ss:[ebp-58],ecx
0040459D    894D B8         mov dword ptr ss:[ebp-48],ecx
004045A0    894D C8         mov dword ptr ss:[ebp-38],ecx
004045A3    8D55 90         lea edx,dword ptr ss:[ebp-70]
004045A6    8D4D D0         lea ecx,dword ptr ss:[ebp-30]
004045A9    8945 A0         mov dword ptr ss:[ebp-60],eax
004045AC    8945 B0         mov dword ptr ss:[ebp-50],eax
004045AF    8945 C0         mov dword ptr ss:[ebp-40],eax
004045B2    C745 98 AC2B4000 mov dword ptr ss:[ebp-68],music_player.402BAC  402BAC:L"1분 미리듣기만 가능합니다."
```

1분이 지났을 때 출력되는 메시지로 1분 루틴 구문을 찾아 보았는데,

EA60과 비교하는 구문을 찾았다. 0xEA60은 10진수로 60000이고 60000ms는 1분이다.

여기서 비교하는 것 같다. 브레이크 포인트를 걸고 디버깅을 해본다.

```
00404556    50              push eax
00404557    FF15 3C104000   call dword ptr ds:[<&__vbaHresultCheckObj>]
0040455D    8B85 5CFFFFFF   mov eax,dword ptr ss:[ebp-A4]
00404563    3D FFFF0F00     cmp eax,FFFFF
00404568    8945 E8         mov dword ptr ss:[ebp-18],eax
0040456B    0F8C 8D000000   jl music_player.4045FE
00404571    8B0E            mov ecx,dword ptr ds:[esi]                  esi:"pt@"
00404573    56              push esi                                    esi:"pt@"
00404574    FF91 08070000   call dword ptr ds:[ecx+708]
```

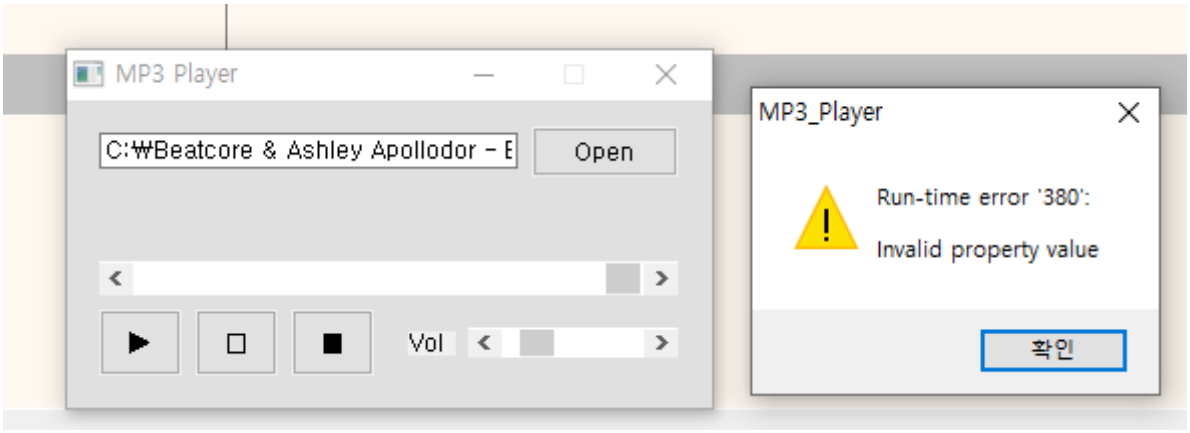
확인해보니 구문이 맞았고 비교하는 부분을 1분보다 훨씬 큰 값으로 수정한 뒤, 패치하여 새로 파일을 열어본다.

디버거로 열어서 음악을 재생해보니,

```
767BB97C    FF15 FCC38676   call dword ptr ds:[<&RtlRaiseException>]
767BB982  .  8B4C24 54      mov ecx,dword ptr ss:[esp+54]               sub_767BB982
767BB986  .  33CC           xor ecx,esp
767BB988  .  E8 934D0000    call kernelbase.767C0720
767BB98D  .  8BE5           mov esp,ebp
767BB98F  .  5D             pop ebp
767BB990  .  C2 1000        ret 10
```

이 부분에서 멈추게 되었고 이 부분은 예외 처리를 하는 구문이였다.

계속 실행해보니,



또 다른 경고 메시지가 나왔다.

수정한 FFFFF를 비교하는 구문으로 다시 가서 F8로 천천히 디버깅을 했다.

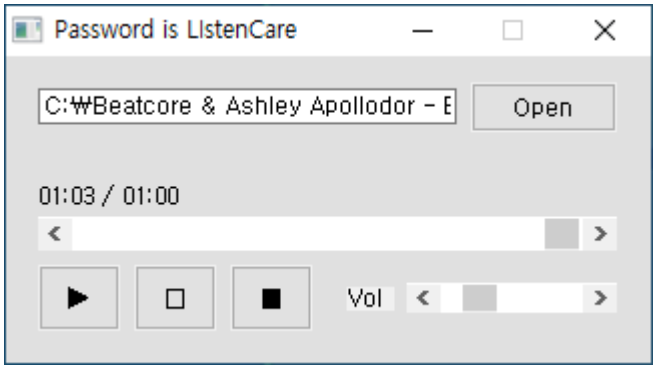
```
004046A1   FF91 BC000000   call dword ptr ds:[ecx+BC]
004046A7   85C0            test eax,eax
004046A9   DBE2            fnclex
004046AB   7D 12           jge patched.4046BF
004046AD   68 BC000000     push BC
004046B2   68 582B4000     push patched.402B58
004046B7   57              push edi
004046B8   50              push eax
004046B9   FF15 3C104000   call dword ptr ds:[<&__vbaHresultCheckObj>]
004046BF   8D4D E0         lea ecx,dword ptr ss:[ebp-20]
004046C2   FF15 28114000   call dword ptr ds:[<&__vbaFreeObj>]
004046C8   33DB            xor ebx,ebx
004046CA   8B46 34         mov eax,dword ptr ds:[esi+34]   esi+34:"P늘"
004046CD   8D7E 34         lea edi,dword ptr ds:[esi+34]   esi+34:"P늘"
```

vbaHresultCheckObj함수가 호출되면 프로그램 흐름은 예외처리가 되어 오류가 발생 하였고,

이 함수를 호출하는 구문은 jge에서 점프를 뛰지 않게되면 호출이 되었다.

jge를 jmp로 바꾸어 무조건 점프를 뛰게 만들어주면,

```
004046A7   85C0            test eax,eax
004046A9   DBE2            fnclex
004046AB   EB 12           jmp patched.4046BF
004046AD   68 BC000000     push BC
004046B2   68 582B4000     push patched.402B58
004046B7   57              push edi                        edi:"@>f"
004046B8   50              push eax
004046B9   FF15 3C104000   call dword ptr ds:[<&__vbaHresultCheckObj>]
004046BF   8D4D E0         lea ecx,dword ptr ss:[ebp-20]   [ebp-20]:"@>f"
004046C2   FF15 28114000   call dword ptr ds:[<&__vbaFreeObj>]
```



title에 flag가 설정되며 음악이 계속 재생된다.

성공!