Reverse L03

Date : 2010 / 01 / 01
PRIDE

#문제

Korea :
비주얼베이직에서 스트링 비교함수 이름은?

English :
What is the name of the Visual Basic function that compares two strings?

#문제프로그램

#프로그램실행

프로그램을 실행했다.

발음도 알아보기 힘든 콩글리시 문자열이다.
확인을 누른다.

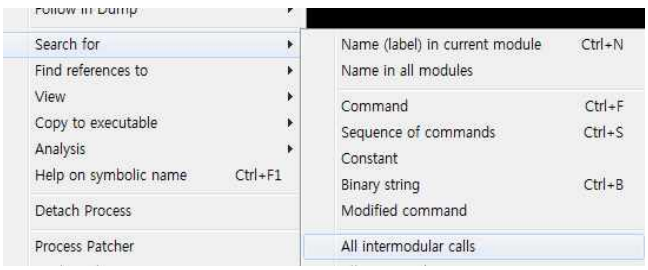
위의 사진같이 입력폼과, 폼의 값을 처리하는 버튼, 종료버튼 등이있다.
입력폼에 임의의 값을 넣은 후, Registrieren버튼을 클릭한다.

콩글리시이지만, 대략 패스워드가 틀렸다는 뜻같다.
이후 exit를 누르면 종료된다.

#With Ollydbg

Ollydbg로 해당 프로그램을 열어보았다.
Visual Basic으로 제작되었기 때문에 C기반의 프로그램과는 약간 다르게 구성되어있다.

입력한 스트링과 패스워드를 비교하는 부분을 찾아야한다.
OllyDbg의 기능인 Search for - All intermodular calls를 이용해 모듈에서의 함수이름을 찾아본다.



```
0040116D | CALL <JMP.&MSVBVM50.#100>                | MSVBVM50.ThunRTMain
00402891 | CALL <JMP.&MSVBVM50.__vbaObjSet>        | MSVBVM50.__vbaObjSet
004028B5 | CALL <JMP.&MSVBVM50.__vbaHresultCheckOb | MSVBVM50.__vbaHresultCheckObj
004028C2 | CALL <JMP.&MSVBVM50.__vbaStrCmp>        | MSVBVM50.__vbaStrCmp
004028D3 | CALL <JMP.&MSVBVM50.__vbaFreeStr>       | MSVBVM50.__vbaFreeStr
004028DB | CALL <JMP.&MSVBVM50.__vbaFreeObj>       | MSVBVM50.__vbaFreeObj
00402905 | CALL <JMP.&MSVBVM50.__vbaVarCopy>       | MSVBVM50.__vbaVarCopy
00402926 | CALL <JMP.&MSVBVM50.__vbaVarMove>       | MSVBVM50.__vbaVarMove
```

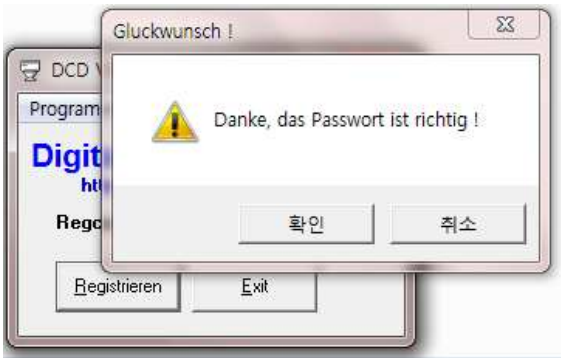
많은 함수이름이있지만 그중 vbaStrCmp함수가 스트링을 비교하는 함수로 보인다.
구글링의 결과로도 알수있었다.

이함수를 호출하는곳으로 가보았다.

```
004028BA  > FF75 A8       PUSH DWORD PTR SS:[EBP-58]
004028BD  . 68 DC1D4000   PUSH A2DC1DEA.00401DDC          UNICODE "2G83G35Hs2"
004028C2  . E8 83E8FFFF   CALL <JMP.&MSVBVM50.__vbaStrCmp>
```

EBP-58에는 사용자로부터 입력받은 값의 주소가 담겨있다.
입력받은 값과 "2G83G35Hs2"를 push하고, vbaStrCmp함수를 호출한다.
이를 통해 "2G83G35Hs2"와 입력 값을 비교한다는 것을 알 수 있다.
그러므로 프로그램 입력폼에 "2G83G35Hs2"를 입력하면 맞았다는 내용의 메시지박스가 나타날것이라고 추측할 수 있다.

실행 후 입력폼에 "2G83G35Hs2"를 입력하고 진행해본다.



대략 Thank you, that password is right로 해석할 수 있는 메시지박스가 나타났다.
크랙에 성공했다.

그리고 비주얼 베이직의 문자열비교함수인 vbaStrCmp가 답이된다.

#답 : vbaStrCmp