Basic 03 Report

파일을 실행하면 다음과 같은 창이 뜬다.

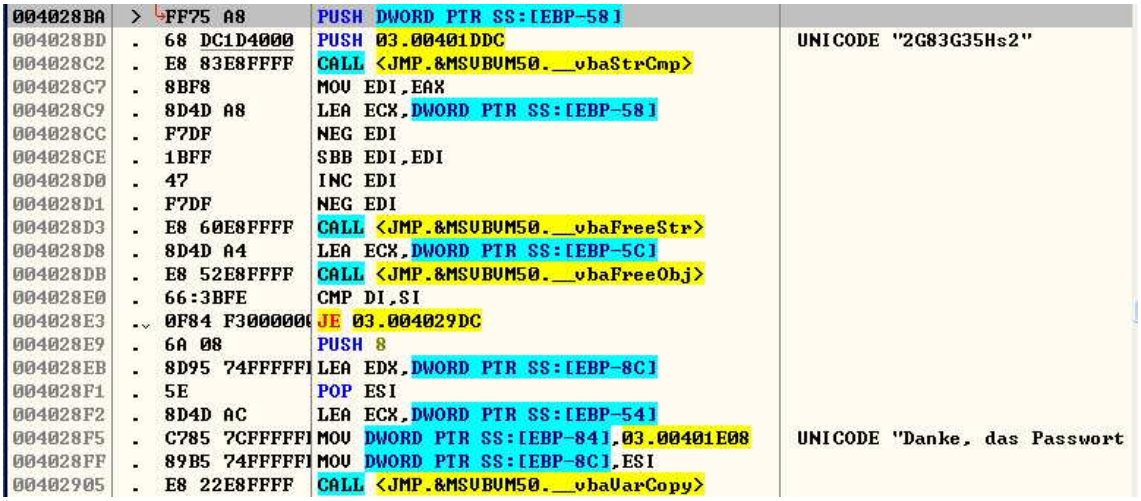
무슨말인지 잘은 모르겠으나 일단 확인을 누르면,

위와 같은 화면이 뜨는데 Recode를 입력하여 원하는 메시지를 얻어야 하는 문제인 것 같다.
일단 abcde를 입력한 후 Registrieren을 클릭 하였다.

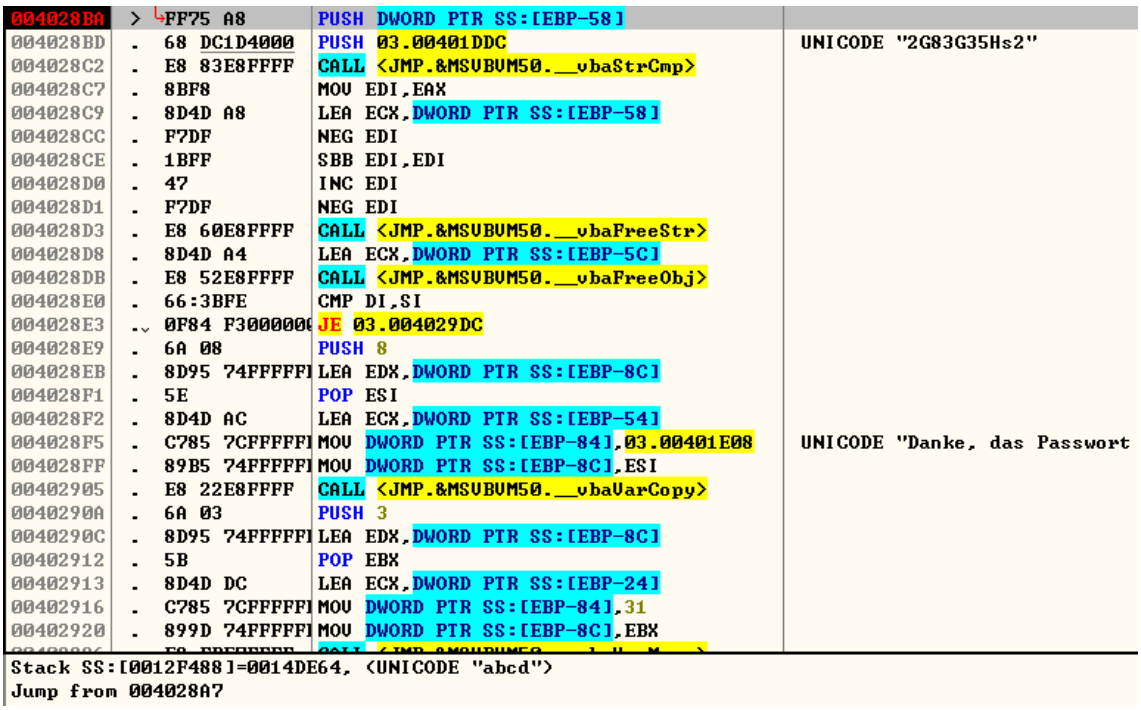
그러자 위와 같은 메시지가 뜬다, 아무래도 Password가 맞지 않다는 내용인 것 같다.
OllyDbg로 파일을 열고 All referenced text strings에서 위 메시지가 생성되는 위치를 찾아 보겠다.

```
004028BD  PUSH 03.00401DDC                  UNICODE "2G83G35Hs2"
004028F5  MOV DWORD PTR SS:[EBP-84],03.00401E08  UNICODE "Danke, das Passwort ist richtig !"
00402A2A  PUSH 03.00401DDC                  UNICODE "2G83G35Hs2"
00402A69  MOV DWORD PTR SS:[EBP-84],03.00401E70  UNICODE "Error ! Das Passwort ist falsch !"
00402AA9  MOV DWORD PTR SS:[EBP-84],03.00401EB8  UNICODE "PASSWORT FALSCH !"
00402C85  MOV DWORD PTR SS:[EBP-7C],03.00401EF0  UNICODE "Entferne diesen Nag, oder bekomme d
00402CBE  MOV DWORD PTR SS:[EBP-7C],03.00401F78  UNICODE "Nag Meldung"
00402E28  MOV DWORD PTR SS:[EBP-5C],03.00401F94  UNICODE "VB5-CrackMe 1.0 by Blaster99 [DCD]"
```

그러자 위 그림과 같은 유니코드를 찾을 수 있었고, 위 쪽을 살펴 보니 "Danke, das Passwort ist richtig ! " 라는 문장이 아마도 올바른 Password를 입력하면 출력되는 메시지인 것 같다. 또한 "2G83G35Hs2"라는 유니코드도 있는데 이것이 아마도 Password인 것 같다.
일단은 "Danke,..“로 시작하는 유니코드로 이동해 보겠다.



해당 위치로 이동하니 위쪽에 Password로 추측되는 유니코드와 vbaStrCmp라는 함수를 호출 하는 것이 보인다. 아무래도 이 함수가 입력한 값과 Password를 비교하는 함수인 것 같다. 확인 해 보기 위해 004024BA부분에 Break를 걸고 함수를 실행하여 abcd를 입력해 보겠다.



예상대로 [EBP-58]는 입력한 텍스트인 abcd의 주소를 기억하는 스택이었다.
vbaStrCmp의 결과 EAX=00000001이 되었고, SI=0000와 비교 결과 "Error...“문구가 출력되는 함수로 jump하였다.

이제 제대로 Password로 예상되는 "2G83G35Hs2"를 입력해 보겠다.

```
>  FF75 A8        PUSH DWORD PTR SS:[EBP-58]
.  68 DC1D4000    PUSH 03.00401DDC                 UNICODE "2G83G35Hs2"
.  E8 83E8FFFF    CALL <JMP.&MSVBVM50.__vbaStrCmp>
.  8BF8           MOV EDI,EAX
.  8D4D A8        LEA ECX,DWORD PTR SS:[EBP-58]
.  F7DF           NEG EDI
.  1BFF           SBB EDI,EDI
.  47             INC EDI
.  F7DF           NEG EDI
.  E8 60E8FFFF    CALL <JMP.&MSVBVM50.__vbaFreeStr>
.  8D4D A4        LEA ECX,DWORD PTR SS:[EBP-5C]
.  E8 52E8FFFF    CALL <JMP.&MSVBVM50.__vbaFreeObj>
.  66:3BFE        CMP DI,SI
.  0F84 F3000000  JE 03.004029DC
.  6A 08          PUSH 8
.  8D95 74FFFFFF  LEA EDX,DWORD PTR SS:[EBP-8C]
.  5E             POP ESI
.  8D4D AC        LEA ECX,DWORD PTR SS:[EBP-54]
.  C785 7CFFFFFF  MOV DWORD PTR SS:[EBP-84],03.00401E08   UNICODE "Danke, das Passwort
.  89B5 74FFFFFF  MOV DWORD PTR SS:[EBP-8C],ESI
.  E8 22E8FFFF    CALL <JMP.&MSVBVM50.__vbaVarCopy>
.  6A 03          PUSH 3
.  8D95 74FFFFFF  LEA EDX,DWORD PTR SS:[EBP-8C]
.  5B             POP EBX
.  8D4D DC        LEA ECX,DWORD PTR SS:[EBP-24]
.  C785 7CFFFFFF  MOV DWORD PTR SS:[EBP-84],31
.  899D 74FFFFFF  MOV DWORD PTR SS:[EBP-8C],EBX
.  E8 FBE7FFFF    CALL <JMP.&MSVBVM50.__vbaVarMove>
.  8D95 74FFFFFF  LEA EDX,DWORD PTR SS:[EBP-8C]
```

```
Registers (FP
EAX 00000000
ECX 00000000
EDX 00CF0608
EBX 0014C708
ESP 0012F410
EBP 0012F4E0
ESI 00000000
EDI 00CFC1E4

EIP 004028C7

C 0  ES 0023
P 1  CS 001B
A 0  SS 0023
Z 1  DS 0023
S 0  FS 003B
T 0  GS 0000
D 0
O 0  LastErr

EFL 00000246

ST0 empty -1.
ST1 empty 1.5
ST2 empty -3.
ST3 empty +UN
ST4 empty 0.0
ST5 empty 5.9
```

vbaStrCmp결과 EAX는 0이 되었고, 위 그림과 같은 문구가 출력되었다.

해석 해보니 “감사합니다 이 암호는 올바릅니다” 대충 이런뜻이다.

결국 스트링 비교함수는 vbaStrCmp라는 것을 알 수 있고, 스트링이 같을 때는 0이 리턴되고 다를 때는 1이 리턴되는 것을 알 수 있다.