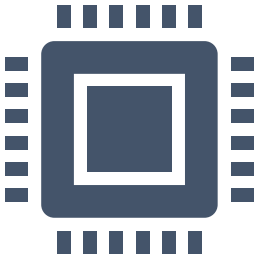
Reversing.kr 문제풀이

이지훈

목차

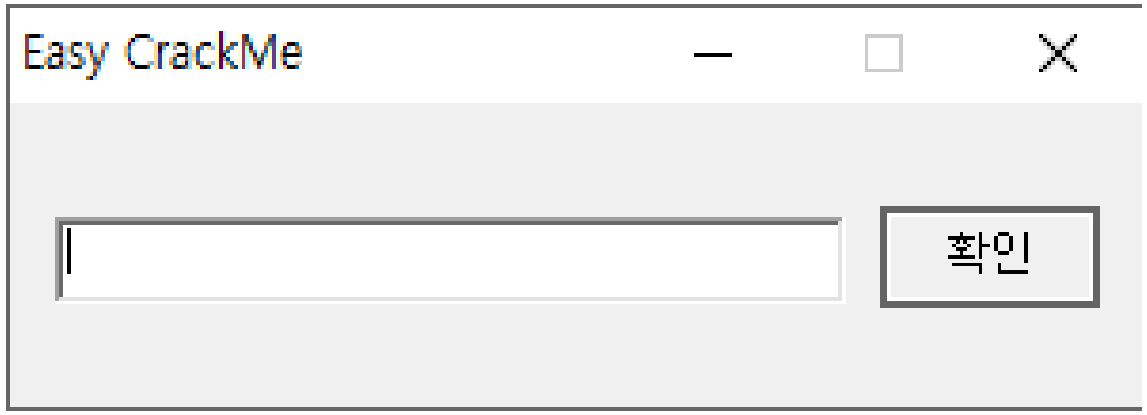


Easy Crack

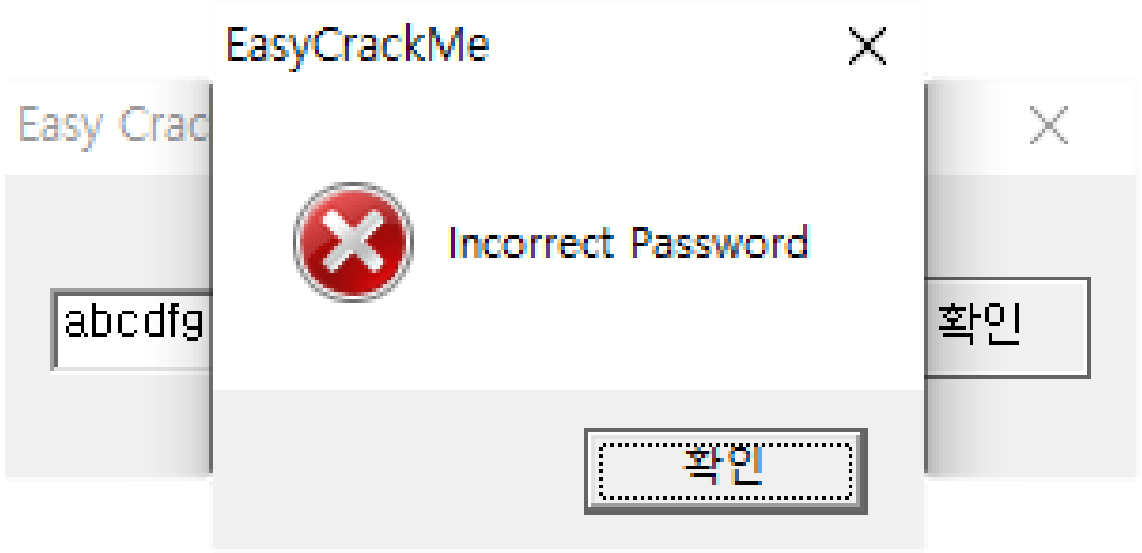
Easy Crack.exe

Message Box

CMP, JNZ

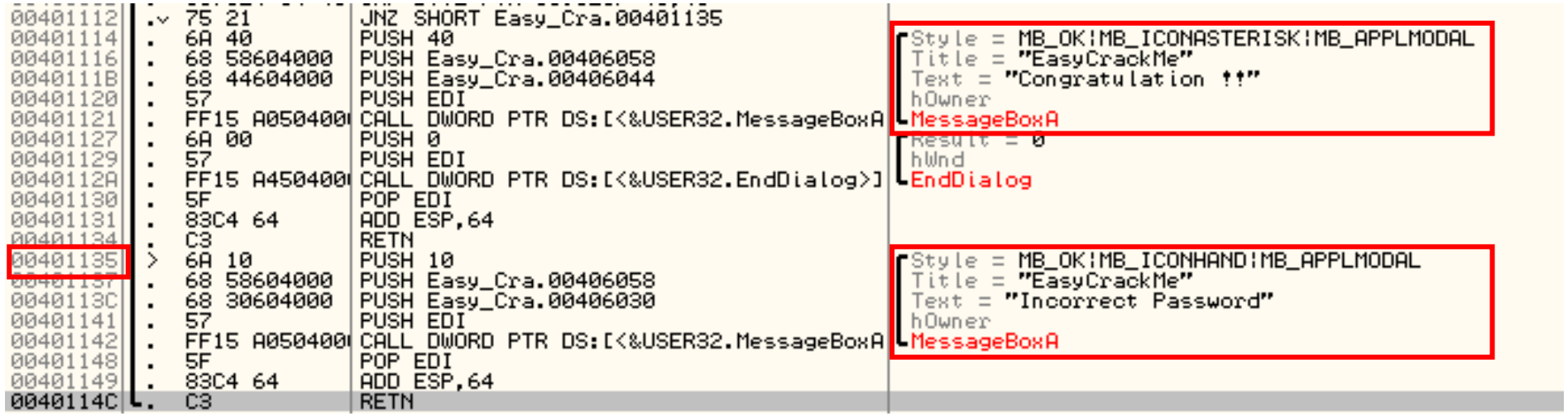


Easy Crack.exe



Easy Crack.exe

비밀번호 입력 시 메시지 박스가 뜨는 것을 확인할 수 있었다.



Easy Crack.exe

성공 / 실패의 메시지 박스가 각각 존재

실패의 경우 시작 주소 : 401135

```
TEST EAX,EAX
JNZ SHORT Easy_Cra.00401135
CMP BYTE PTR SS:[ESP+4],45
JNZ SHORT Easy_Cra.00401135
```

```
CMP BYTE PTR SS:[ESP+5],61
JNZ SHORT Easy_Cra.00401135
PUSH 2
LEA ECX,DWORD PTR SS:[ESP+A]
PUSH Easy_Cra.00406078                ASCII "5y"
PUSH ECX
CALL Easy_Cra.00401150
ADD ESP,0C
TEST EAX,EAX
JNZ SHORT Easy_Cra.00401135
```

Easy Crack.exe

총 4곳에서 실패 분기점이 있음을 확인할 수 있었고,
분기점마다 CMP혹은 TEST를 통해 비교를 하는 것을 확인했다.

```
TEST EAX,EAX
JNZ SHORT Easy_Cra.00401135
CMP BYTE PTR SS:[ESP+4],45
JNZ SHORT Easy_Cra.00401135
```

```
CMP BYTE PTR SS:[ESP+5],61
JNZ SHORT Easy_Cra.00401135
PUSH 2
LEA ECX,DWORD PTR SS:[ESP+A]
PUSH Easy_Cra.00406078          ASCII "5y"
PUSH ECX
CALL Easy_Cra.00401150
ADD ESP,0C
TEST EAX,EAX
JNZ SHORT Easy_Cra.00401135
```

Easy Crack.exe

총 4곳에서 실패 분기점이 있음을 확인할 수 있었고,
분기점마다 CMP혹은 TEST를 통해 비교를 하는 것을 확인했다.

ZF (Zero Flag) : 앞의 연산의 결과가 0일 경우 ZF 값은 1이 된다.

CMP : 비교하는 두 값이 같을 경우 ZF 값을 1로 설정

JNZ (Jump if Not Zero) : 앞의 연산이 00이 아닐 때 = ZF 값이 0일 때 JMP

What is ZF, CMP, JNZ?

CMP : SUB를 통해 뺀 값이 0일 경우 ZF = 1, 아닐 경우 ZF = 0

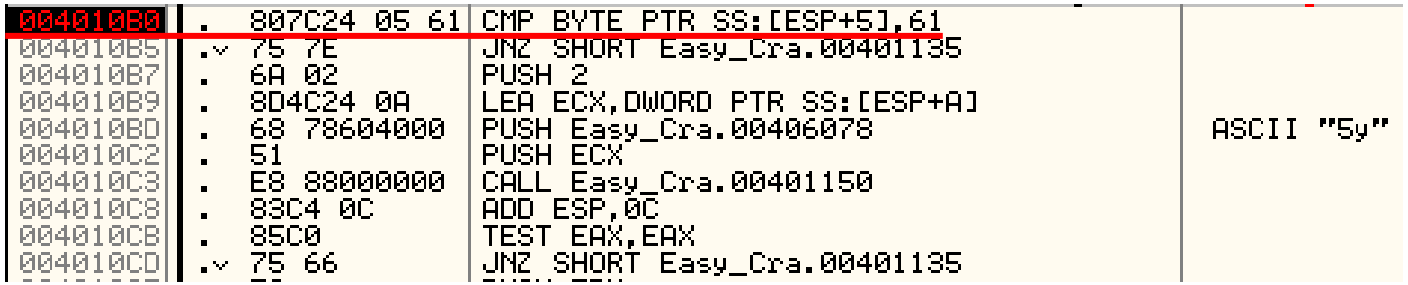
Ex) CMP 2,1 -> 2 - 1 = 1, 0이 아니므로 ZF = 0

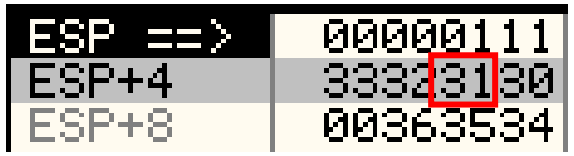
TEST : 논리 비교 연산자 AND 를 통해 0일 경우 ZF = 1, 둘 다 참일 경우 ZF = 0

TEST EAX, EAX 를 통해 NULL CHECK 할 경우에 주로 사용, CMP와 다르게 결과값 저장 X

Ex) TEST 1,1 -> 1, ZF = 0 // TEST 0,0 -> 0, ZF = 1

CMP VS TEST





CMP (1 번째 비교)

비밀번호 입력 : 0123456

ESP+5 : 0x31 -> 1

0x61 -> a

2번째 비밀번호가 a일 경우에 JNZ 실행 X

```
004010B0  .  807C24 05 61   CMP BYTE PTR SS:[ESP+5],61
004010B5  .v 75 7E          JNZ SHORT Easy_Cra.00401135
004010B7  .  6A 02          PUSH 2
004010B9  .  8D4C24 0A      LEA ECX,DWORD PTR SS:[ESP+A]
004010BD  .  68 78604000    PUSH Easy_Cra.00406078          ASCII "5y"
004010C2  .  51             PUSH ECX
004010C3  .  E8 88000000    CALL Easy_Cra.00401150
004010C8  .  83C4 0C        ADD ESP,0C
004010CB  .  85C0           TEST EAX,EAX
004010CD  .v 75 66          JNZ SHORT Easy_Cra.00401135
```

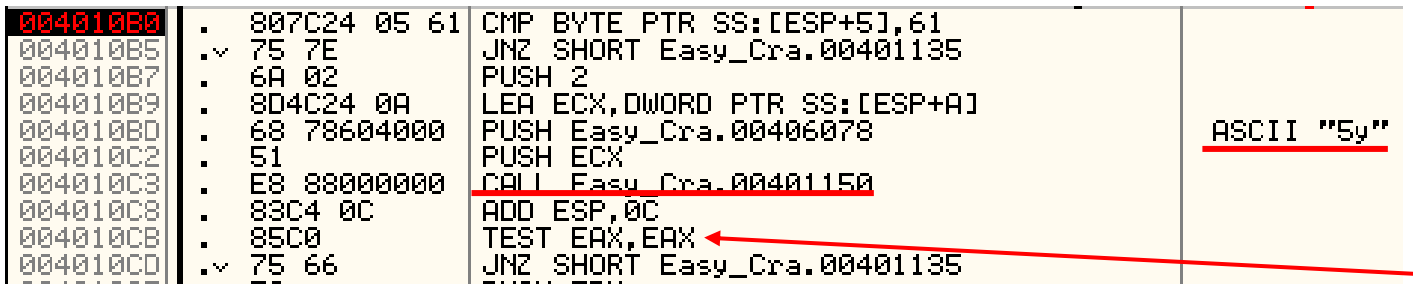
```
ESP ==>  00000002
ESP+4    00000111
ESP+8    33325130
```

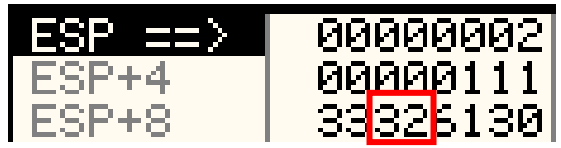
TEST (2 번째 비교)

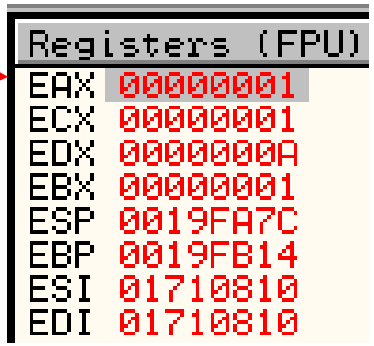
비밀번호 입력 : 0a23456

ESP+A : 0x32 -> 2

ASCII ''5y''는 3번째 비밀번호부터 비교





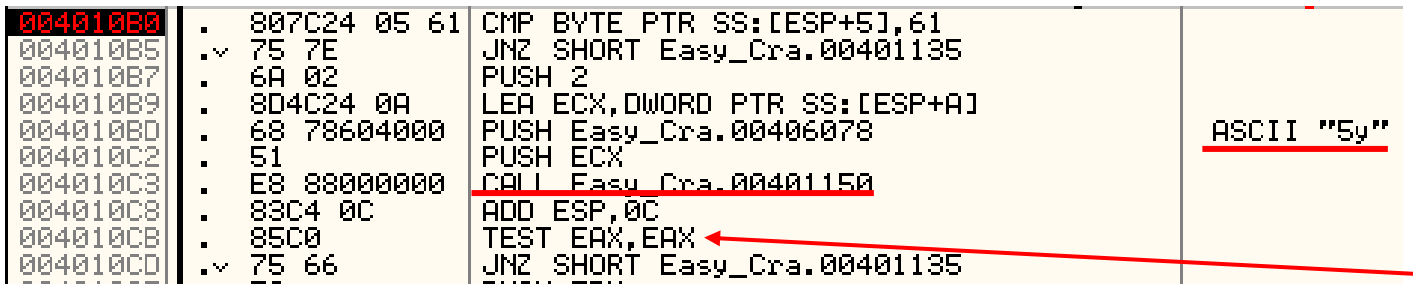


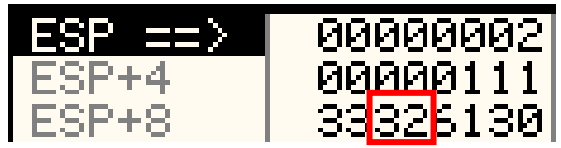
TEST (2 번째 비교)

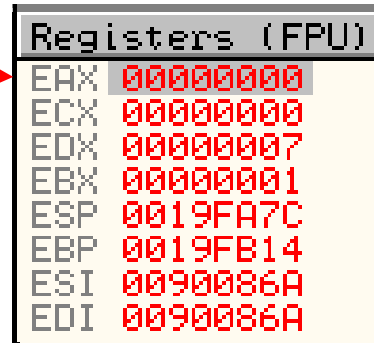
비밀번호 입력 : 0a23456

TEST 1,1 -> 1, ZF = 0

ZF = 0 일 경우 JNZ 명령어 실행 -> 실패 구문으로 JMP







TEST (2 번째 비교)

비밀번호 입력 : 0a5y456

TEST 0,0 -> 0, ZF = 1

ZF = 0 일 경우 JNZ 명령어 실행 -> 실행 안됨

```
004010D1  .  BE 6C604000    MOV ESI,Easy_Cra.0040606C                ASCII "R3versing"
004010D6  .  8D4424 10      LEA EAX,DWORD PTR SS:[ESP+10]
004010DA  >  8A10           MOV DL,BYTE PTR DS:[EAX]
004010DC  .  8A1E           MOV BL,BYTE PTR DS:[ESI]
004010DE  .  8ACA           MOV CL,DL
004010E0  .  3AD3           CMP DL,BL
```

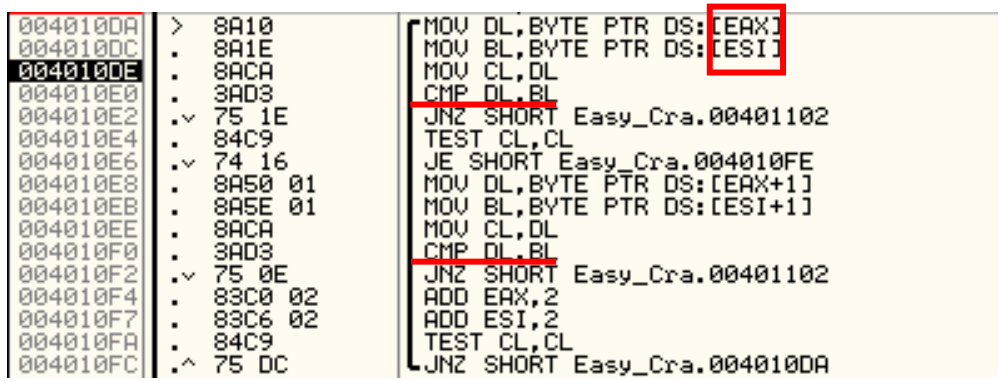
ESP ==>	00F10822
ESP+4	00000001
ESP+8	00000111
ESP+C	79356130
ESP+10	00363534

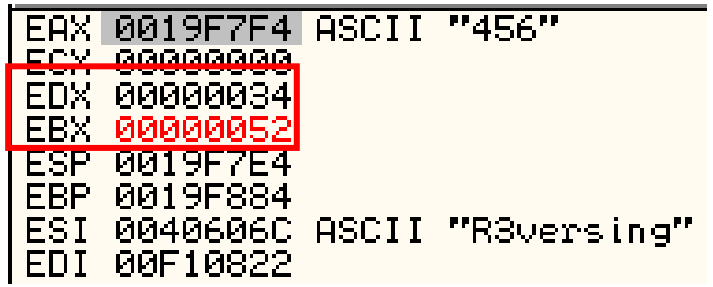
CMP (3 번째 비교)

비밀번호 입력 : 0a5y456

ESP+A : 0x34 -> 4

ASCII ''R3versing''는 5번째 비밀번호부터 비교



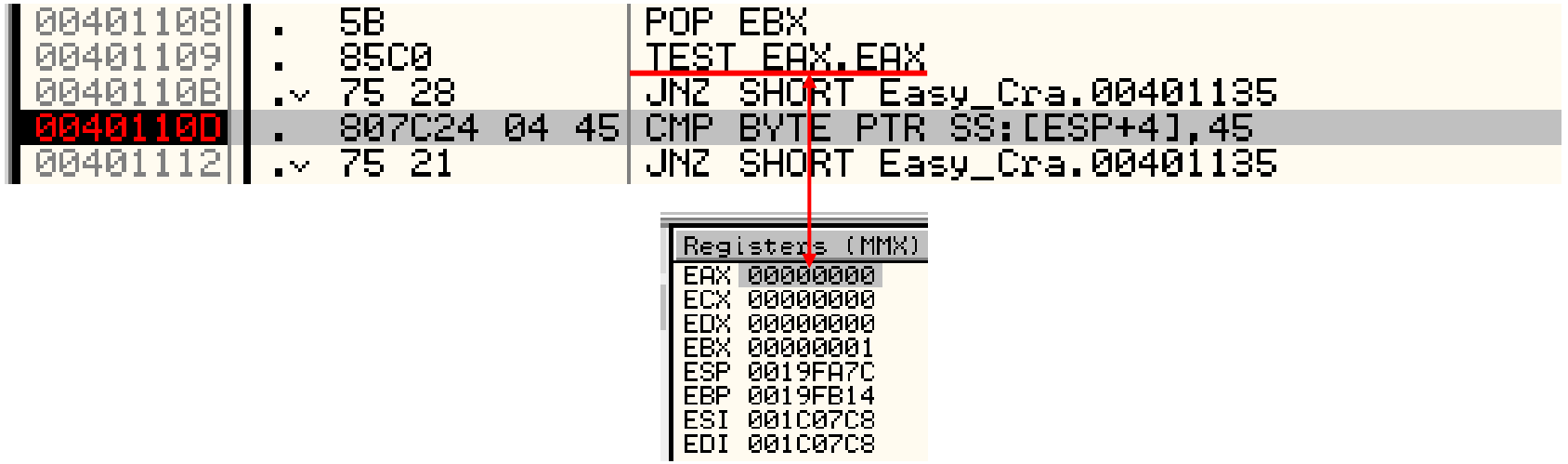


CMP (3 번째 비교)

CMP DL, BL

EAX+1, ESI+1 을 통해

반복해서 비교



TEST (3 번째 비교)

비밀번호 입력 : 0a5yR3versing

TEST 0,0 -> 0, ZF = 1

ZF = 0 일 경우 JNZ 명령어 실행 -> 실행 안됨

```
00401108  .   5B            POP EBX
00401109  .   85C0          TEST EAX,EAX
0040110B  .v  75 28         JNZ SHORT Easy_Cra.00401135
0040110D  .   807C24 04 45  CMP BYTE PTR SS:[ESP+4],45
00401112  .v  75 21         JNZ SHORT Easy_Cra.00401135
```

ESP ==>	00000111
ESP+4	79356130
ESP+8	65763352

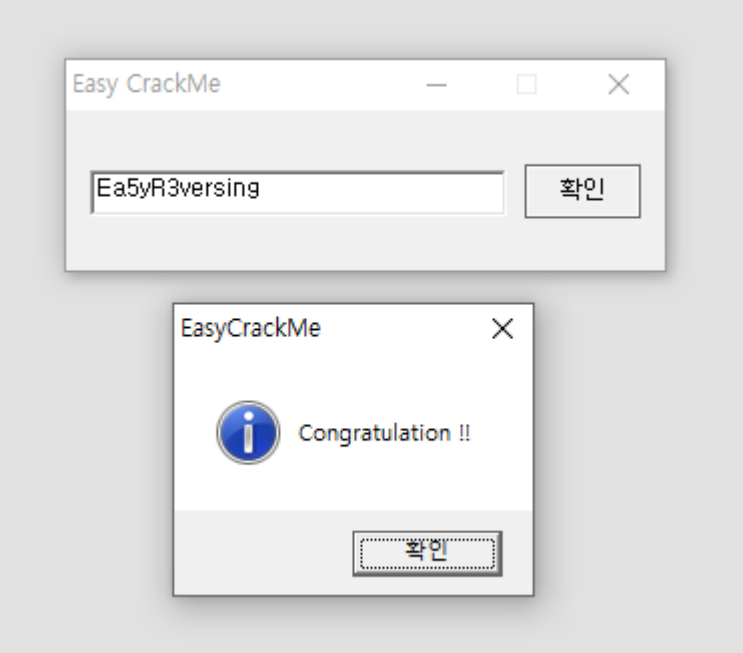
CMP (4 번째 비교)

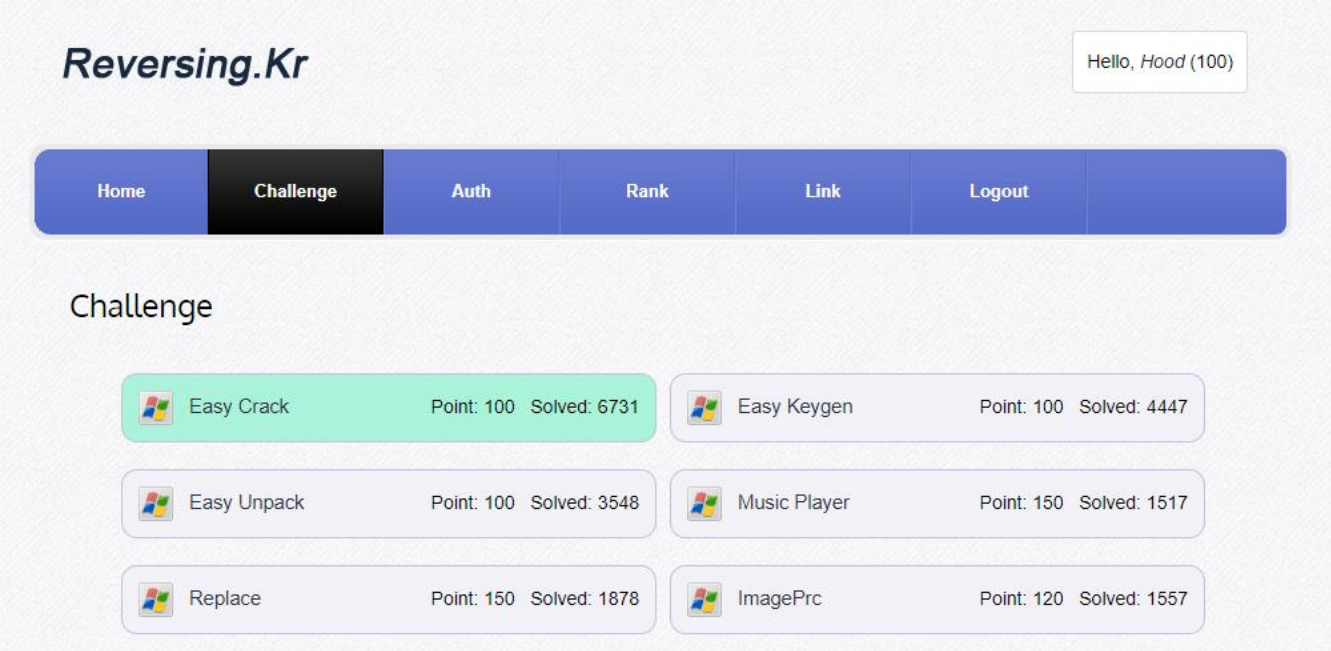
비밀번호 입력 : 0a5yR3versing

ESP+4 : 0x30 -> 0

0x45 -> E

1번째 비밀번호가 a일 경우에 JNZ 실행 X





Conguratuation!

모든 비밀번호 유추를 합해 성공 메시지 박스 출력 성공

Q&A