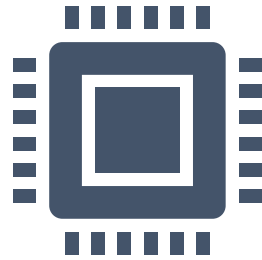




Reversing.kr 문제풀이

이지훈

목차

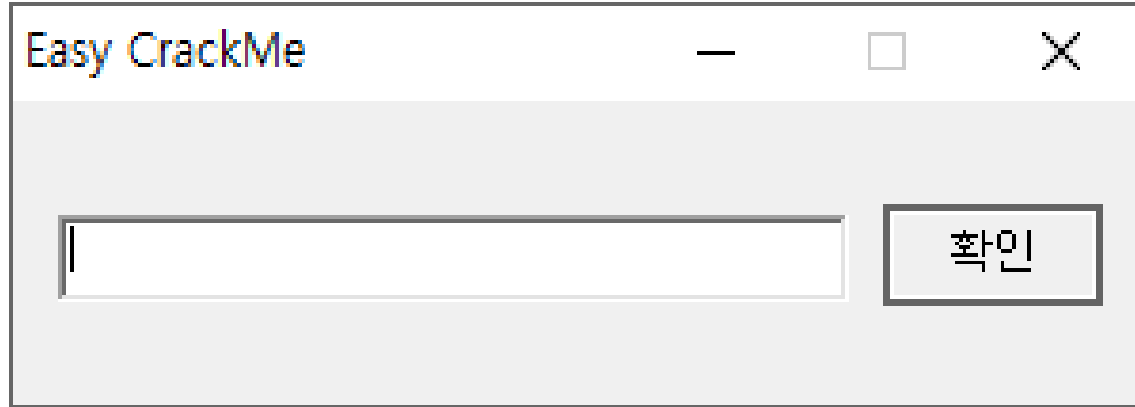


Easy Crack

Easy Crack.exe

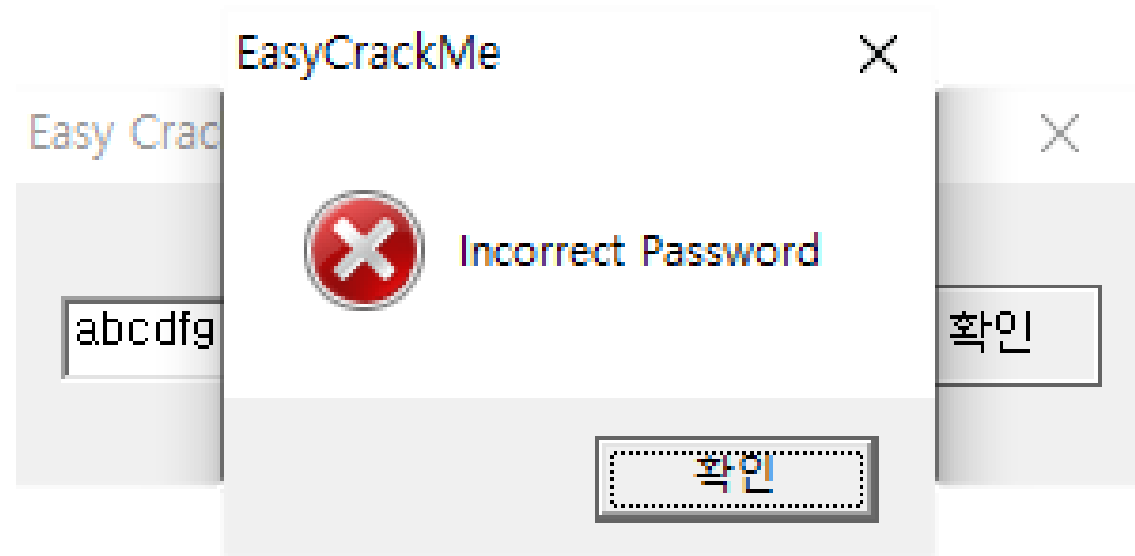
Message Box

CMP, JNZ



Easy Crack.exe





Easy Crack.exe

비밀번호 입력 시 메시지 박스가 뜨는 것을 확인할 수 있었다.



00401112	75 21	JNZ SHORT Easy_Cra.00401135	
00401114	6A 40	PUSH 40	
00401116	68 58604000	PUSH Easy_Cra.00406058	Style = MB_OK!MB_ICONASTERISK!MB_APPLMODAL
00401118	68 44604000	PUSH Easy_Cra.00406044	Title = "EasyCrackMe"
00401120	57	PUSH EDI	Text = "Congratulation !!"
00401121	FF15 A0504000	CALL DWORD PTR DS:[<&USER32.MessageBoxA	hOwner
00401127	6A 00	PUSH 0	MessageBoxA
00401129	57	PUSH EDI	Result = 0
0040112A	FF15 A4504000	CALL DWORD PTR DS:[<&USER32.EndDialog>]	hWnd
00401130	5F	POP EDI	EndDialog
00401131	83C4 64	ADD ESP,64	
00401134	C3	RETN	
00401135	6A 10	PUSH 10	Style = MB_OK!MB_ICONHAND!MB_APPLMODAL
00401137	68 58604000	PUSH Easy_Cra.00406058	Title = "EasyCrackMe"
0040113C	68 30604000	PUSH Easy_Cra.00406030	Text = "Incorrect Password"
00401141	57	PUSH EDI	hOwner
00401142	FF15 A0504000	CALL DWORD PTR DS:[<&USER32.MessageBoxA	MessageBoxA
00401148	5F	POP EDI	
00401149	83C4 64	ADD ESP,64	
0040114C	C3	RETN	

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  
PUSH ECX  
CALL Easy_Cra.00401150  
ADD ESP,0C  
TEST EAX,EAX  
JNZ SHORT Easy_Cra.00401135
```

ASCII "5y"

Easy Crack.exe

총 4곳에서 실패 분기점이 있음을 확인할 수 있었고,
분기점마다 CMP 혹은 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+4]  
PUSH Easy_Cra.00406078  
PUSH ECX  
CALL Easy_Cra.00401150  
ADD ESP,0C  
TEST EAX,EAX  
JNZ SHORT Easy_Cra.00401135
```

ASCII "5y"

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 0이 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 $\rightarrow 2 - 1 = 1$, 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 $\rightarrow 1$, ZF = 0 // TEST 0,0 $\rightarrow 0$, ZF = 1

CMP VS TEST



004010B0	. 807C24 05 61	CMP BYTE PTR SS:[ESP+5],61	
004010B5	. 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	. 75 66	JNZ SHORT Easy_Cra.00401135	

ESP ==>	00000111
ESP+4	33323130
ESP+8	00363534

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	. 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	. 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



004010B0	. 807C24 05 61	CMP BYTE PTR SS:[ESP+5],61	
004010B5	. 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	. 75 66	JNZ SHORT Easy_Cra.00401135	

Registers (FPU)	
EAX	00000001
ECX	00000001
EDX	0000000A
EBX	00000001
ESP	0019FA7C
EBP	0019FB14
ESI	01710810
EDI	01710810

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

TEST (2 번째 비교)

비밀번호 입력 : 0a23456

TEST 1,1 -> 1, ZF = 0

ZF = 0 일 경우 JNZ 명령어 실행 -> 실패 구문으로 JMP



004010B0	. 807C24 05 61	CMP BYTE PTR SS:[ESP+5],61	
004010B5	. 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	. 75 66	JNZ SHORT Easy_Cra.00401135	

Registers (FPU)	
EAX	00000000
ECX	00000000
EDX	00000007
EBX	00000001
ESP	0019FA7C
EBP	0019FB14
ESI	0090086A
EDI	0090086A

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

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



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
004010E2	.v	75 1E	JNZ SHORT Easy_Cra.00401102
004010E4	.	84C9	TEST CL, CL
004010E6	.v	74 16	JE SHORT Easy_Cra.004010FE
004010E8	.	8A50 01	MOV DL, BYTE PTR DS:[EAX+1]
004010EB	.	8A5E 01	MOV BL, BYTE PTR DS:[ESI+1]
004010EE	.	8ACA	MOV CL, DL
004010F0	.	3AD3	CMP DL, BL
004010F2	.v	75 0E	JNZ SHORT Easy_Cra.00401102
004010F4	.	83C0 02	ADD EAX, 2
004010F7	.	83C6 02	ADD ESI, 2
004010FA	.	84C9	TEST CL, CL
004010FC	.^	75 DC	JNZ SHORT Easy_Cra.004010DA

EAX	0019F7F4	ASCII "456"
ECX	00000000	
EDX	00000034	
EBX	00000052	
ESP	0019F7E4	
EBP	0019F884	
ESI	0040606C	ASCII "R3versing"
EDI	00F10822	

CMP (3 번째 비교)

CMP DL, BL
EAX+1, ESI+1 을 통해
반복해서 비교



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

Registers (MMX)	
EAX	00000000
ECX	00000000
EDX	00000000
EBX	00000001
ESP	0019FA7C
EBP	0019FB14
ESI	001C07C8
EDI	001C07C8

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)

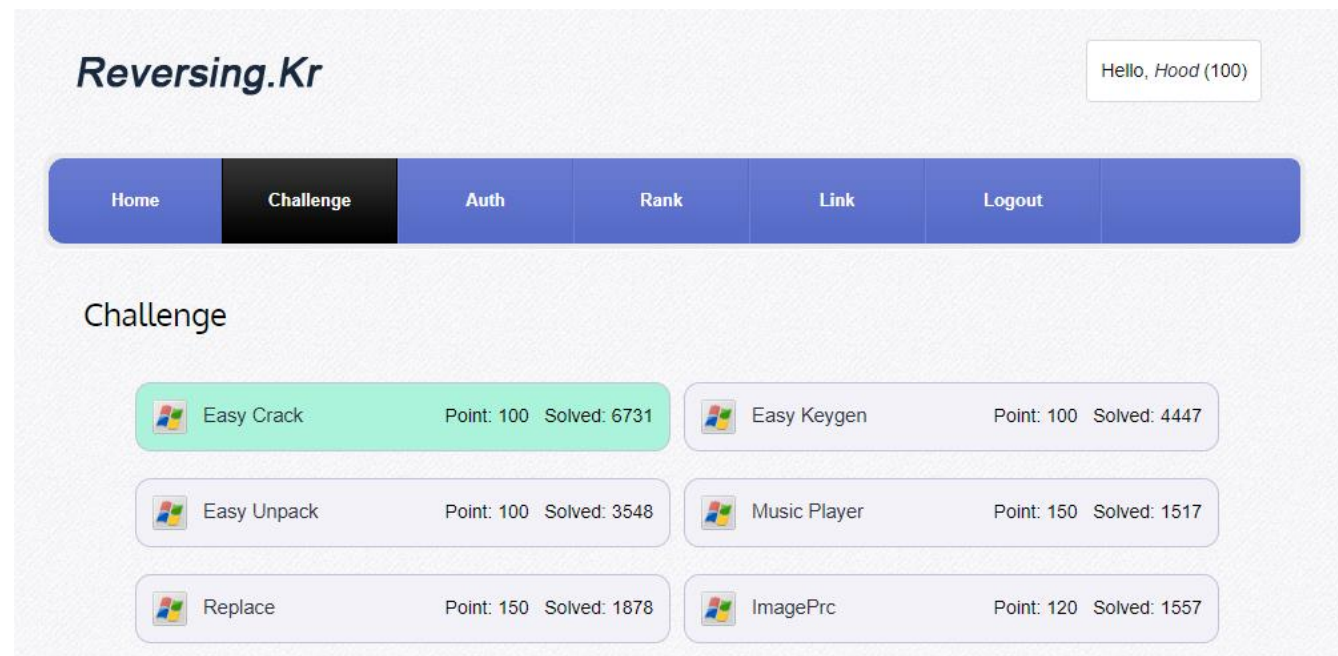
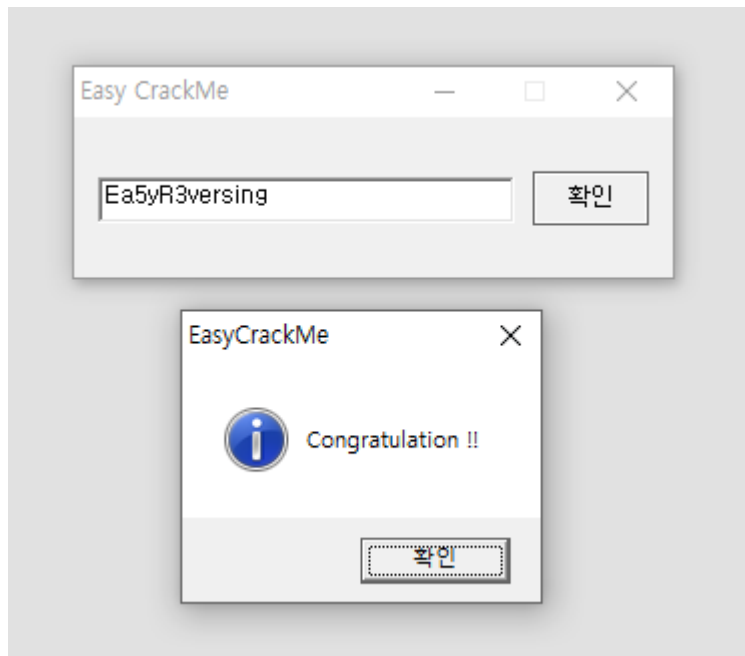
비밀번호 입력 : 0a5yR3versing

ESP+4 : 0x30 -> 0

0x45 -> E

1번째 비밀번호가 a일 경우에 JNZ 실행 X





Congratuatuion!

모든 비밀번호 유추를 합해 성공 메시지 박스 출력 성공



Q&A

