

## evilprogrammer's mexican

<https://crackmes.one/crackme/5d63011533c5d46f00e2c305>

## Crackme by b1h0 <https://crackmes.one/user/b1h0>

- Used **x64dbg** debugger.

### Some notes to get the flag and create the patch

- Once the **EntryPoint** is located, you can verify that at the address **0x00401500** a subroutine begins, which is the one shown in the *flag* text. We will call this subroutine: **sub\_result\_cracked**

| Address  | Disassembly            | Comment                      |
|----------|------------------------|------------------------------|
| 004014D5 | E9 A6FCFFFF            | jmp mexican.401180           |
| 004014DA | 8DB6 00000000          | lea esi,dword ptr ds:[esi]   |
| 004014E0 | 83EC 0C                | sub esp,C                    |
| 004014E3 | C705 34504000 00000000 | mov dword ptr ds:[405034],0  |
| 004014E9 | E8 E80A0000            | call mexican.sub_401FE0      |
| 004014F2 | 83C4 0C                | add esp,C                    |
| 004014F5 | E9 86FCFFFF            | jmp mexican.401180           |
| 004014FA | 90                     | nop                          |
| 004014FB | 90                     | nop                          |
| 004014FC | 90                     | nop                          |
| 004014FD | 90                     | nop                          |
| 004014FE | 90                     | nop                          |
| 004014FF | 90                     | nop                          |
| 00401500 | 55                     | push ebp                     |
| 00401501 | 89E5                   | mov ebp,esp                  |
| 00401503 | 83EC 28                | sub esp,28                   |
| 00401506 | C70424 1D000000        | mov dword ptr ss:[esp],1D    |
| 0040150D | E8 EE110000            | call <JMP.&malloc>           |
| 00401512 | 8945 F4                | mov dword ptr ss:[ebp-C],eax |
| 00401515 | 8845 F4                | mov byte ptr ds:[eax],66     |
| 00401518 | C600 66                | mov byte ptr ss:[ebp-C],66   |
| 0040151B | 8845 F4                | mov dword ptr ss:[ebp-C],66  |
| 0040151E | 83C0 01                | add eax,1                    |
| 00401521 | C600 6C                | mov byte ptr ds:[eax],6C     |
| 00401524 | 8845 F4                | mov dword ptr ss:[ebp-C],6C  |
| 00401527 | 83C0 02                | add eax,2                    |
| 0040152A | C600 61                | mov byte ptr ds:[eax],61     |
| 0040152D | 8845 F4                | mov dword ptr ss:[ebp-C],61  |
| 00401530 | 83C0 03                | add eax,3                    |
| 00401533 | C600 67                | mov byte ptr ds:[eax],67     |
| 00401536 | 8845 F4                | mov dword ptr ss:[ebp-C],67  |
| 00401539 | 83C0 04                | add eax,4                    |
| 0040153C | C600 7B                | mov byte ptr ds:[eax],7B     |
| 0040153F | 8845 F4                | mov dword ptr ss:[ebp-C],7B  |
| 00401542 | 83C0 05                | add eax,5                    |
| 00401545 | C600 4D                | mov byte ptr ds:[eax],4D     |
| 00401548 | 8845 F4                | mov dword ptr ss:[ebp-C],4D  |

- Then later we can find in the address **0x004013dd** a call to the address **0x0040162c** which is the subroutine that we will call **sub\_compare\_crackme**. We establish a breakpoint there and then continue step by step.

| Address  | Disassembly   | Comment                          |
|----------|---------------|----------------------------------|
| 004013C3 | A1 14504000   | mov eax,dword ptr ds:[405014]    |
| 004013C8 | 894424 08     | mov dword ptr ss:[esp+8],eax     |
| 004013CC | A1 18504000   | mov eax,dword ptr ds:[405018]    |
| 004013D1 | 894424 04     | mov dword ptr ss:[esp+4],eax     |
| 004013D5 | A1 1C504000   | mov eax,dword ptr ds:[40501C]    |
| 004013DA | 890424        | mov dword ptr ss:[esp],eax       |
| 004013DD | E8 4A020000   | call mexican.sub_compare_crackme |
| 004013E2 | 8B0D 08504000 | mov ecx,dword ptr ds:[405008]    |
| 004013E8 | A3 0C504000   | mov dword ptr ds:[40500C],eax    |
| 004013ED | 85C9          | test ecx,ecx                     |
| 004013F5 | 0F84 B6000000 | je mexican.exit_program          |
| 004013F8 | 8B15 04504000 | mov edx,dword ptr ds:[405004]    |
| 004013FD | 85D2          | test edx,edx                     |
| 004013FE | 75 0A         | jne mexican.401409               |
| 004013FF | E8 14130000   | call <JMP.&cexit>                |
| 00401404 | A1 0C504000   | mov eax,dword ptr ds:[40500C]    |
| 00401409 | 8D65 F4       | lea esp,dword ptr ss:[ebp-C]     |
| 0040140C | 5B            | pop ebx                          |

- Finally at address **0x00401642** we find a comparison of the value **0xC1** with the value **0xC1**. The key is that the two values have to be different, and in particular the first one greater than the second, therefore we change the first **0xC1** for a greater value, or the second **0xC1** for a smaller value.

```

0040161E  C70424 00404000 mov dword ptr ss:[esp],mexican.4016C0
00401620  E8 0E110000 call <JMP.&printf>
00401622  C9 leave
00401623  C3 ret
0040162C  <mexican.sub_compare_crackme> 55 push ebp
0040162D  89E5 mov ebp,esp
0040162E  83E4 F0 and esp,FFFFFFF0
0040162F  83EC 20 sub esp,20
00401630  E8 86090000 call <mexican.sub_401FC0>
00401632  C74424 1C C1000000 mov dword ptr ss:[esp+1C],C1
00401634  817C24 1C C1000000 cmp dword ptr ss:[esp+1C],C1
00401636  7E 07 jle mexican.401653
00401637  C70424 03404000 mov dword ptr ss:[esp],mexican.40165F
00401638  E8 D9100000 call <mexican.sub_result_cracked>
00401639  E8 0C jmp mexican.40165F
0040163A  C70424 03404000 mov dword ptr ss:[esp],mexican.40165F
0040163B  E8 D9100000 call <JMP.&printf>
0040163D  B8 00000000 mov eax,0
0040163E  C9 leave
0040163F  C3 ret
00401640  90 nop
00401641  90 nop

```

- So we change the 0xC1 value of the comparison line to a lower value. For example, 0 (zero)

```

00401628  <mexican.sub_compare_crackme> C3 ret
00401629  55 push ebp
0040162A  89E5 mov ebp,esp
0040162B  83E4 F0 and esp,FFFFFFF0
0040162C  83EC 20 sub esp,20
0040162D  E8 86090000 call <mexican.sub_401FC0>
0040162F  C74424 1C 00000000 mov dword ptr ss:[esp+1C],0
00401630  817C24 1C 00000000 cmp dword ptr ss:[esp+1C],0
00401632  7E 07 jle mexican.401653
00401633  C70424 03404000 mov dword ptr ss:[esp],mexican.40165F
00401634  E8 D9100000 call <mexican.sub_result_cracked>
00401635  E8 0C jmp mexican.40165F
00401636  C70424 03404000 mov dword ptr ss:[esp],mexican.40165F
00401637  E8 D9100000 call <JMP.&printf>
00401639  B8 00000000 mov eax,0
0040163A  C9 leave
0040163B  C3 ret
0040163C  90 nop
0040163D  90 nop

```

## The flag

- After the change, the flag message appears. Printed message: **flag**

```

C600 0A mov byte ptr ds:[eax],A
8B45 F4 mov eax,dword ptr ss:[ebp-C]
894424 04 mov dword ptr ss:[esp+4],eax
C70424 00404000 mov dword ptr ss:[esp],mexican.404000
E8 0E110000 call <JMP.&printf>
C9 leave
C3 ret

```

C:\Users\... Desktop\CrackMe\crackmes.one\evilprogrammer\mexican.exe

```

flag{M3x1c4nM141w4r3_pl3rro}
s\Wx\")v

```

Note one curious thing. After displaying the flag, strange or random characters are still displayed. This is because the flag string does not end with **NULL '\0'**. It is likely that there is some part of the code that adds this value to the chain or it could also be that the programmer has forgotten this detail.

## The Patch

The file for the patch is included with the name `mexican-patch.1337`

```

>mexican.exe

00001642:81->83
00001646:C1->00
00001647:00->90
00001648:00->90
00001649:00->90

```