

Q1: In order to make any 'Serial' input work for any 'Name' input I simply changed the push commands to all be the same and allow the "Correct" screen to be displayed.

| | |
|---|--|
| <pre> 01344 ^EB DF JMP SHORT CRACKMEV.00401325 01346 > B8 00000000 MOV EAX,0 01348 ^EB D8 JMP SHORT CRACKMEV.00401325 0134D \$ 6A 30 PUSH 30 0134F . 68 29214000 PUSH CRACKMEV.00402129 01354 . 68 34214000 PUSH CRACKMEV.00402134 01359 . FF75 08 PUSH DWORD PTR SS:[EBP+8] 0135C . E8 D9000000 CALL <JMP.&USER32.MessageBoxA> 01361 . C3 RETN 01362 \$ 6A 00 PUSH 0 01364 . E8 AD000000 CALL <JMP.&USER32.MessageBeep> 01369 . 6A 30 PUSH 30 0136B . 68 29214000 PUSH CRACKMEV.00402129 01370 . 68 34214000 PUSH CRACKMEV.00402134 01375 . FF75 08 PUSH DWORD PTR SS:[EBP+8] 01378 . E8 BD000000 CALL <JMP.&USER32.MessageBoxA> 0137D . C3 RETN 0137E \$ 8B7424 04 MOV ESI,DWORD PTR SS:[ESP+4] 01382 . 56 PUSH ESI 01383 > 8A06 MOV AL,BYTE PTR DS:[ESI] 01385 . 84C0 TEST AL,AL 01387 ^74 13 JE SHORT CRACKMEV.0040139C 01389 . 3C 41 CMP AL,41 0138B ^72 1F JB SHORT CRACKMEV.004013AC 0138D . 3C 5A CMP AL,5A 0138F ^73 03 JNB SHORT CRACKMEV.00401394 01391 . 46 INC ESI 01392 ^EB EF JMP SHORT CRACKMEV.00401383 01394 > E8 39000000 CALL CRACKMEV.004013D2 01399 . 46 INC ESI 0139A ^EB E7 JMP SHORT CRACKMEV.00401383 0139C > 5E POP ESI 0139D . E8 20000000 CALL CRACKMEV.004013C2 013A2 . 81F7 78560000 XOR EDI,5678 013A8 . 8BC7 MOV EAX,EDI 013AA ^EB 15 JMP SHORT CRACKMEV.004013C1 013AC > 5E POP ESI 013AD . 6A 30 PUSH 30 013AF . 68 29214000 PUSH CRACKMEV.00402129 013B4 . 68 34214000 PUSH CRACKMEV.00402134 013B9 . FF75 08 PUSH DWORD PTR SS:[EBP+8] 013BC . E8 79000000 CALL <JMP.&USER32.MessageBoxA> 013C1 > C3 RETN 013C2 \$ 33FF XOR EDI,EDI </pre> | <pre> [Style = MB_OK;MB_ICONEXCLAMATION;MB_APPLMODAL Title = "Good work!" Text = "Great work, mate!Now try the next CrackMe!" hOwner]MessageBoxA [BeepType = MB_OK MessageBeep] [Style = MB_OK;MB_ICONEXCLAMATION;MB_APPLMODAL ASCII "Good work!" Text = "Great work, mate!Now try the next CrackMe!" hOwner]MessageBoxA [Style = MB_OK;MB_ICONEXCLAMATION;MB_APPLMODAL ASCII "Good work!" Text = "Great work, mate!Now try the next CrackMe!" hOwner]MessageBoxA </pre> |
|---|--|

Now no matter what name is entered, the Great Work page will be displayed.