

# toaster VIP\_access\_me

<https://crackmes.one/crackme/5d0251c133c5d41c6d56e0c3>

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

Date: 04/oct/2019

To analyze this file I have used two methods: *static*, with **Ghidra**, and *dynamic* with **x64dbg**. (In Ghidra there are few notes. I am still learning).

## Ghidra : Some useful notes

- After analyzing the binary, if we look at the strings in memory it is easy to identify what the user names would be, and probably encrypted vip codes.

### User names and encrypted passwords strings

004bc396 6a 6f 65 00	ds	"joe"	XREF[1]:	004b	004bc396 Please enter lower english letters and numbers only!	004bc396 Please enter lower english letters and numbers only!	ds
004bc39a 6e 69 63 6b 00	ds	"nick"	XREF[1]:	004b	004bc39a "nick"	004bc39a "nick"	ds
004bc39f 6d 6f 6e 6b 65 7...	ds	"monkey"	XREF[1]:	004b	004bc39f monkey	004bc39f monkey	ds
004bc3a6 64 6d 69 74 72 7...	ds	"dmitry"	XREF[1]:	004b	004bc3a6 dmitry	004bc3a6 dmitry	ds
004bc3ad 6c 65 6f 6e 61 7...	ds	"leonard"	XREF[1]:	004b	004bc3ad leonard	004bc3ad leonard	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 e9hy94nono2hhk52k4dihy64k	004bc3b5 e9hy94nono2hhk52k4dihy64k	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 abc1236encrypted99fnszf	004bc3b5 abc1236encrypted99fnszf	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 lol566kokoko602mm6/2h35n2	004bc3b5 lol566kokoko602mm6/2h35n2	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 jokes843toohard567asm7b73	004bc3b5 jokes843toohard567asm7b73	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 five2156szx67o3m7m89jh2	004bc3b5 five2156szx67o3m7m89jh2	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 std::future_error:	004bc3b5 std::future_error:	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 basic_string::M_create	004bc3b5 basic_string::M_create	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 %s: __pos (which is %zu) > this->size() (which is ...	004bc3b5 %s: __pos (which is %zu) > this->size()...	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 basic_string::at: __n (which is %zu) >= this->size(...	004bc3b5 basic_string::at: __n (which is %zu) >=...	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 basic_string::erase	004bc3b5 basic_string::erase	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 basic_string::M_replace_aux	004bc3b5 basic_string::M_replace_aux	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 basic_string::insert	004bc3b5 basic_string::insert	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 basic_string::replace	004bc3b5 basic_string::replace	ds
004bc3b5 65 39 68 79 39 3...	ds	"e9hy94nono2hhk52k4dihy64k"	XREF[1]:	004b	004bc3b5 basic_string::M_replace	004bc3b5 basic_string::M_replace	ds

## x64dbg : Some useful notes

- Main function is located at **00401000**
- At the beginning of this subroutine, it sets a value of 1 over a memory position, where at the end of the process it returns to 0, so it is apparently a Boolean control variable.

### Some type of control variable

00427AE7	EB C6	jmp vip_access_me.427AAF	esi:EntryPoint
00427AE9	8DB426 00000000	lea esi,dword ptr ds:[esi]	decode_info
00427AF0	8B0D 50AC4C00	mov ecx,dword ptr ds:[<var_is_decoding>]	
00427AF6	85C9	test ecx,ecx	
00427AF8	74 06	je vip_access_me.427B00	
00427AFA	F3:C3	ret	
00427AFC	8D7426 00	lea esi,dword ptr ds:[esi]	esi:EntryPoint
00427B00	C705 50AC4C00 01000000	mov dword ptr ds:[<var_is_decoding>],1	Some boolean flag to control process
00427B0A	EB 94	jmp vip_access_me.427AA0	
00427B0C	90	nop	
00427B0D	90	nop	
00427B0E	90	nop	
00427B0F	90	nop	

- At address **006CFE16** fills char 'a' 64 times.

- Create a Mutex using string **"gcc-shmem-tdm2-use\_fc\_key"**.

This information is probably not relevant to find the VIP CODES, but I liked to put it.

:sweat\_smile:

### Mutex creation

00428EAB	8043 10	lea eax,dword ptr ds:[ebx+10]	edi:"aaaaaaaaaaaaaaaaaaaaaaaaaaaa", esi+eax*1:"^	Occultar FPU
00428EAC	8043 0C	lea edi,dword ptr ds:[esi+eax]		EAX 0000001A
00428EAD	8945 0C	mov dword ptr ss:[ebp-8],eax	edi:"aaaaaaaaaaaaaaaaaaaaaaaaaaaa"	EBX 0000000A
00428EAE	C707 61616161	mov dword ptr ds:[edi],61616161	edi+4:"aaaaaaaaaaaaaaaaaaaaaaaaaaaa"	ECX 00000002
00428EAF	C747 04 61616161	mov dword ptr ds:[edi+4],61616161	edi+8:"aaaaaaaaaaaaaaaaaaaaaaaaaaaa"	EDX 00000001
00428EB0	C747 08 61616161	mov dword ptr ds:[edi+8],61616161	edi+C:"aaaaaaaaaaaaaaaaaaaaaaaaaaaa"	EBP 006CFE68
00428EB1	C747 0C 61616161	mov dword ptr ds:[edi+C],61616161	edi+10:"aaaaaaaaaaaaaaaaaaaa"	ESP 006CFD00
00428EB2	C747 10 61616161	mov dword ptr ds:[edi+10],61616161	edi+14:"aaaaaaaaaaaa"	ESI 006CFDFC
00428EB3	C747 14 61616161	mov dword ptr ds:[edi+14],61616161	edi+18:"aaaaaaa"	EDI 006CFE16
00428EB4	C747 18 61616161	mov dword ptr ds:[edi+18],61616161	edi+1C:"aaaa"	
00428EB5	C747 1C 61616161	mov dword ptr ds:[edi+1C],61616161		
00428EB6	C6441C 3C 00	mov byte ptr ss:[esp+ebx+3C],0	esp+ebx*1+3C:var_1	EIP 00428F08
00428EB7	C6441C 18 00	mov byte ptr ss:[esp+ebx+18],0	esp+ebx*1+18:var_2	
00428EB8	897424 08	mov dword ptr ss:[esp+8],esi	esi:EntryPoint	EFLAGS 00000216
00428EB9	C74424 04 00000000	mov dword ptr ss:[esp+4],0	BOOL bInitialOwner = FALSE	ZF 0 PF 1 AF 1
00428EBA	C70424 00000000	mov dword ptr ss:[esp],0	LPSECURITY_ATTRIBUTES lpMutexAttributes = NULL	OF 0 SF 0 DF 0
00428EBB	E8 28F00000	call <Cmp.>CreateMutexA	LPCTSTR lpName = esi:EntryPoint	CF 0 TF 0 IF 1
00428EBC	83EC 0C	sub esp,C	esi+ebx*1+4:var_2, 2D: '-'	LastError 00000000 (ERROR_SUCCESS)
00428EBD	C6441E 0F 2D	mov byte ptr ds:[esi+ebx+1F],2D	DWORD dwMilliseconds = INFINITE	LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)
00428EBE	8945 E0	mov dword ptr ss:[ebp-20],eax	HANDLE hHandle	GS 002B FS 0053
00428EBF	C74424 04 FFFFFFFF	mov dword ptr ss:[esp+4],FFFFFFFF	WaitForSingleObject	OF 02B DS 002B
00428EC0	E8 18F00000	call <Cmp.>WaitForSingleObject		CS 0023 SS 002B
00428EC1	83EC 08	sub esp,8		
00428EC2	83C0	test eax,ecx		
00428EC3	74 01	je vip_access_me.428F30		
00428EC4	CC	int3	LPCTSTR lpString = esi:EntryPoint	
00428EC5	894424	mov dword ptr ss:[esp],esi	FindAtomA	
00428EC6	E8 10F00000	call <Cmp.>FindAtomA		
00428EC7	83EC 04	sub esp,4		
00428EC8	66 85C0	test ax,ax		
00428EC9	75 07	jne vip_access_me.428F00		
00428ECA	OF85 8C000000	jmp vip_access_me.428F00		

- At address **006CFDFC**, after the creation of Mutex, to the string used are added all the 'a' that had been created previously, but changing some lowercase 'a' to uppercase 'A'. Remaining the resulting string as follows: **"gcc-shmem-tdm2-use\_fc\_key-aaaaaaaaAAaaAaaAaaaAaAaAAAAaaaa"**
- At address **004B8080** It makes a comparison of different memory positions and activates a flag (Boolean variable) for each memory position that has the value 1 activated that is also supposedly Boolean. The same at address **004B7FF0 & 004B7F20 & 004B7E50** (other information that is not useful to solve)

### A sub that do memory comparisons and activate boolean flag

004B807F	90	nop	
004B8080	803D 50B14B00 00	cmp byte ptr ds:[4BB150],0	do_comparisons_and_flag
004B8087	75 07	jne vip_access_me.4B8090	
004B8089	C605 50B14B00 01	mov byte ptr ds:[4BB150],1	
004B8090	803D 58B14B00 00	cmp byte ptr ds:[4BB158],0	
004B8097	75 07	jne vip_access_me.4B80A0	
004B8099	C605 58B14B00 01	mov byte ptr ds:[4BB158],1	
004B80A0	803D A8B14B00 00	cmp byte ptr ds:[4BB1A8],0	
004B80A7	75 07	jne vip_access_me.4B80B0	
004B80A9	C605 A8B14B00 01	mov byte ptr ds:[4BB1A8],1	
004B80B0	803D B8B14B00 00	cmp byte ptr ds:[4BB1B8],0	
004B80B7	75 07	jne vip_access_me.4B80C0	
004B80B9	C605 88B14B00 01	mov byte ptr ds:[4BB1B8],1	
004B80C0	803D 88B14B00 00	cmp byte ptr ds:[4BB1B8],0	
004B80C7	75 07	jne vip_access_me.4B80D0	
004B80C9	C605 88B14B00 01	mov byte ptr ds:[4BB1B8],1	
004B80D0	803D 98B14B00 00	cmp byte ptr ds:[4BB198],0	
004B80D7	75 07	jne vip_access_me.4B80E0	
004B80D9	C605 98B14B00 01	mov byte ptr ds:[4BB198],1	
004B80E0	803D 78B14B00 00	cmp byte ptr ds:[4BB178],0	
004B80E7	75 07	jne vip_access_me.4B80F0	
004B80E9	C605 78B14B00 01	mov byte ptr ds:[4BB178],1	
004B80F0	803D 68B14B00 00	cmp byte ptr ds:[4BB168],0	
004B80F7	75 07	jne vip_access_me.4B8100	
004B80F9	C605 68B14B00 01	mov byte ptr ds:[4BB168],1	
004B8100	F3:C3	ret	
004B8102	90	nop	

- From the address **004B769F** are the functions that the user names reveal to us. The names are: **joe, nick, monkey, dmitry** and **leonard**.



## Username strings

004B769C	83EC 04	sub esp,4	
004B769F	C70424 90144000	mov dword ptr ss:[esp],<vip_access_me.sub_401490>	[Arg1 = <vip_access_me.sub_401490>
004B76A6	E8 159CF4FF	call <vip_access_me.sub_4012C0>	[sub_4012C0
004B76A8	B9 F8904C00	mov ecx,vip_access_me.4C90F8	4C90F8:&"joe"
004B76B0	C70424 96C34B00	mov dword ptr ss:[esp],<vip_access_me.users>	[Arg1 = "joe"
004B76B7	E8 D49EF4FF	call <vip_access_me.sub_401590>	[sub_401590
004B76B8	83EC 04	sub esp,4	
004B76B8	C70424 70144000	mov dword ptr ss:[esp],<vip_access_me.sub_401470>	[Arg1 = <vip_access_me.sub_401470>
004B76C6	E8 F59BF4FF	call <vip_access_me.sub_4012C0>	[sub_4012C0
004B76C8	B9 60904C00	mov ecx,vip_access_me.4C90E0	4C90E0:&"nick"
004B76D0	C70424 9AC34B00	mov dword ptr ss:[esp],vip_access_me.4BC39A	[Arg1 = "nick"
004B76D7	E8 B49EF4FF	call <vip_access_me.sub_401590>	[sub_401590
004B76DC	83EC 04	sub esp,4	
004B76DF	C70424 50144000	mov dword ptr ss:[esp],<vip_access_me.sub_401450>	[Arg1 = <vip_access_me.sub_401450>
004B76E6	E8 D59BF4FF	call <vip_access_me.sub_4012C0>	[sub_4012C0
004B76EB	B9 C8904C00	mov ecx,vip_access_me.4C90C8	4C90C8:&"monkey"
004B76F0	C70424 9FC34B00	mov dword ptr ss:[esp],vip_access_me.4BC39F	[Arg1 = "monkey"
004B76F7	E8 949EF4FF	call <vip_access_me.sub_401590>	[sub_401590
004B76FC	83EC 04	sub esp,4	
004B76FF	C70424 30144000	mov dword ptr ss:[esp],<vip_access_me.sub_401430>	[Arg1 = <vip_access_me.sub_401430>
004B7706	E8 B59BF4FF	call <vip_access_me.sub_4012C0>	[sub_4012C0
004B770B	B9 B0904C00	mov ecx,vip_access_me.4C90B0	4C90B0:&"dmitry"
004B7710	C70424 A6C34B00	mov dword ptr ss:[esp],vip_access_me.4BC3A6	[Arg1 = "dmitry"
004B7717	E8 749EF4FF	call <vip_access_me.sub_401590>	[sub_401590
004B771C	83EC 04	sub esp,4	
004B771F	C70424 10144000	mov dword ptr ss:[esp],<vip_access_me.sub_401410>	[Arg1 = <vip_access_me.sub_401410>
004B7726	E8 559BF4FF	call <vip_access_me.sub_4012C0>	[sub_4012C0
004B772B	B9 98904C00	mov ecx,vip_access_me.4C9098	4C9098:&"leonard"
004B7730	C70424 ADC34B00	mov dword ptr ss:[esp],vip_access_me.4BC3AD	[Arg1 = "leonard"
004B7737	E8 549EF4FF	call <vip_access_me.sub_401590>	[sub_401590
004B773C	83EC 04	sub esp,4	

- At 004B4160 there is the function that compares the string with the username.

## Compare Username

004B4160	53	push ebx	check_name
004B4161	B8 01000000	mov eax,1	
004B4166	83EC 18	sub esp,18	
004B4169	885424 20	mov edx,dword ptr ss:[esp+20]	[esp+20]:&"nick"
004B416D	884C24 24	mov ecx,dword ptr ss:[esp+24]	[esp+24]:&"joe"
004B4171	8B5A 04	mov ebx,dword ptr ds:[edx+4]	
004B4174	3B59 04	cmp ebx,dword ptr ds:[ecx+4]	
004B4177	75 19	jne vip_access_me.4B4192	
004B4179	895C24 08	mov dword ptr ss:[esp+8],ebx	size_t count
004B417D	8B01	mov eax,dword ptr ds:[ecx]	const void* buf2
004B417F	894424 04	mov dword ptr ss:[esp+4],eax	[edx]:"nick"
004B4183	8B02	mov eax,dword ptr ds:[edx]	const void* buf1
004B4185	890424	mov dword ptr ss:[esp],eax	memcpy
004B4188	E8 F3D3F7FF	call <JMP.&memcmp>	
004B418D	85C0	test eax,eax	
004B418F	0F95C0	setne al	
004B4192	83C4 18	add esp,18	
004B4195	5B	pop ebx	
004B4196	C3	ret	

- From address 004B7750 some operations with strings like: e9hy94nono2hhk52k4dihy64k, abc12316encrypted99fsnzsf. They are the "VIP codes" that are encrypted.

## These resulting encrypted strings, are the VIP Codes

004B773C

83EC 04

sub esp,4

004B773F

C70424 F0134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013F0

[Arg1 = <vip\_access\_me.sub\_4013F0>

004B7746

E8 159BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7748

B9 80904C00

mov ecx,vip\_access\_me.4C9080

4C9080:&"e9hy94nono2hhk52k4dihy64k"

004B7749

C70424 B3C34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3B5

[Arg1 = "e9hy94nono2hhk52k4dihy64k"

004B7750

E8 499EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B775C

83EC 04

sub esp,4

004B775F

C70424 D0134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013D0

[Arg1 = <vip\_access\_me.sub\_4013D0>

004B7766

E8 559BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7768

B9 68904C00

mov ecx,vip\_access\_me.4C9068

4C9068:&"abc12316encrypted99fsnzsf"

004B7770

C70424 CFC34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3CF

[Arg1 = "abc12316encrypted99fsnzsf"

004B7777

E8 149EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B777C

83EC 04

sub esp,4

004B777F

C70424 80134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013B0

[Arg1 = <vip\_access\_me.sub\_4013B0>

004B7786

E8 559BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7788

B9 50904C00

mov ecx,vip\_access\_me.4C9050

4C9050:&"101566kokoko602hm612h35n2"

004B7790

C70424 E9C34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3E9

[Arg1 = "101566kokoko602hm612h35n2"

004B7797

E8 F49EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B779C

83EC 04

sub esp,4

004B779F

C70424 90134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401390

[Arg1 = <vip\_access\_me.sub\_401390>

004B77A6

E8 159BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77AB

B9 38904C00

mov ecx,vip\_access\_me.4C9038

4C9038:&"f0kes843toohard567asm7b73"

004B77B0

C70424 03C44B00

mov dword ptr ss:[esp],vip\_access\_me.4BC403

[Arg1 = "f0kes843toohard567asm7b73"

004B77B7

E8 049EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B77BC

83EC 04

sub esp,4

004B77BF

C70424 70134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401370

[Arg1 = <vip\_access\_me.sub\_401370>

004B77C6

E8 599EF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77CB

B9 20904C00

mov ecx,vip\_access\_me.4C9020

4C9020:&"five2156izx7o1hn7m891h2"

004B77D0

C70424 10C44B00

mov dword ptr ss:[esp],vip\_access\_me.4BC41D

[Arg1 = "five2156izx7o1hn7m891h2"

004B77D7

E8 B49EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B77DC

83EC 04

sub esp,4

004B77DF

C70424 50134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401350

[Arg1 = <vip\_access\_me.sub\_401350>

004B77E6

E8 D59BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77EB

8045 C4

lea eax,dword ptr ss:[ebp-3C]

004B77EE

890424

mov dword ptr ss:[esp],eax

[Arg1 = ...

004B77F3

83EC 04

sub esp,4

004B773C

83EC 04

sub esp,4

004B773F

C70424 F0134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013F0

[Arg1 = <vip\_access\_me.sub\_4013F0>

004B7746

E8 159BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7748

B9 80904C00

mov ecx,vip\_access\_me.4C9080

4C9080:&"e9hy94nono2hhk52k4dihy64k"

004B7749

C70424 B3C34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3B5

[Arg1 = "e9hy94nono2hhk52k4dihy64k"

004B7750

E8 499EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B775C

83EC 04

sub esp,4

004B775F

C70424 D0134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013D0

[Arg1 = <vip\_access\_me.sub\_4013D0>

004B7766

E8 559BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7768

B9 68904C00

mov ecx,vip\_access\_me.4C9068

4C9068:&"abc12316encrypted99fsnzsf"

004B7770

C70424 CFC34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3CF

[Arg1 = "abc12316encrypted99fsnzsf"

004B7777

E8 149EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B777C

83EC 04

sub esp,4

004B777F

C70424 80134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013B0

[Arg1 = <vip\_access\_me.sub\_4013B0>

004B7786

E8 559BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7788

B9 50904C00

mov ecx,vip\_access\_me.4C9050

4C9050:&"101566kokoko602hm612h35n2"

004B7790

C70424 E9C34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3E9

[Arg1 = "101566kokoko602hm612h35n2"

004B7797

E8 F49EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B779C

83EC 04

sub esp,4

004B779F

C70424 90134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401390

[Arg1 = <vip\_access\_me.sub\_401390>

004B77A6

E8 159BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77AB

B9 38904C00

mov ecx,vip\_access\_me.4C9038

4C9038:&"f0kes843toohard567asm7b73"

004B77B0

C70424 03C44B00

mov dword ptr ss:[esp],vip\_access\_me.4BC403

[Arg1 = "f0kes843toohard567asm7b73"

004B77B7

E8 049EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B77BC

83EC 04

sub esp,4

004B77BF

C70424 70134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401370

[Arg1 = <vip\_access\_me.sub\_401370>

004B77C6

E8 599EF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77CB

B9 20904C00

mov ecx,vip\_access\_me.4C9020

4C9020:&"five2156izx7o1hn7m891h2"

004B77D0

C70424 10C44B00

mov dword ptr ss:[esp],vip\_access\_me.4BC41D

[Arg1 = "five2156izx7o1hn7m891h2"

004B77D7

E8 B49EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B77DC

83EC 04

sub esp,4

004B77DF

C70424 50134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401350

[Arg1 = <vip\_access\_me.sub\_401350>

004B77E6

E8 D59BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77EB

8045 C4

lea eax,dword ptr ss:[ebp-3C]

004B77EE

890424

mov dword ptr ss:[esp],eax

[Arg1 = ...

004B77F3

83EC 04

sub esp,4

004B773C

83EC 04

sub esp,4

004B773F

C70424 F0134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013F0

[Arg1 = <vip\_access\_me.sub\_4013F0>

004B7746

E8 159BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7748

B9 80904C00

mov ecx,vip\_access\_me.4C9080

4C9080:&"e9hy94nono2hhk52k4dihy64k"

004B7749

C70424 B3C34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3B5

[Arg1 = "e9hy94nono2hhk52k4dihy64k"

004B7750

E8 499EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B775C

83EC 04

sub esp,4

004B775F

C70424 D0134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013D0

[Arg1 = <vip\_access\_me.sub\_4013D0>

004B7766

E8 559BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7768

B9 68904C00

mov ecx,vip\_access\_me.4C9068

4C9068:&"abc12316encrypted99fsnzsf"

004B7770

C70424 CFC34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3CF

[Arg1 = "abc12316encrypted99fsnzsf"

004B7777

E8 149EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B777C

83EC 04

sub esp,4

004B777F

C70424 80134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013B0

[Arg1 = <vip\_access\_me.sub\_4013B0>

004B7786

E8 559BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7788

B9 50904C00

mov ecx,vip\_access\_me.4C9050

4C9050:&"101566kokoko602hm612h35n2"

004B7790

C70424 E9C34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3E9

[Arg1 = "101566kokoko602hm612h35n2"

004B7797

E8 F49EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B779C

83EC 04

sub esp,4

004B779F

C70424 90134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401390

[Arg1 = <vip\_access\_me.sub\_401390>

004B77A6

E8 159BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77AB

B9 38904C00

mov ecx,vip\_access\_me.4C9038

4C9038:&"f0kes843toohard567asm7b73"

004B77B0

C70424 03C44B00

mov dword ptr ss:[esp],vip\_access\_me.4BC403

[Arg1 = "f0kes843toohard567asm7b73"

004B77B7

E8 049EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B77BC

83EC 04

sub esp,4

004B77BF

C70424 70134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401370

[Arg1 = <vip\_access\_me.sub\_401370>

004B77C6

E8 599EF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77CB

B9 20904C00

mov ecx,vip\_access\_me.4C9020

4C9020:&"five2156izx7o1hn7m891h2"

004B77D0

C70424 10C44B00

mov dword ptr ss:[esp],vip\_access\_me.4BC41D

[Arg1 = "five2156izx7o1hn7m891h2"

004B77D7

E8 B49EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B77DC

83EC 04

sub esp,4

004B77DF

C70424 50134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401350

[Arg1 = <vip\_access\_me.sub\_401350>

004B77E6

E8 D59BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77EB

8045 C4

lea eax,dword ptr ss:[ebp-3C]

004B77EE

890424

mov dword ptr ss:[esp],eax

[Arg1 = ...

004B77F3

83EC 04

sub esp,4

004B773C

83EC 04

sub esp,4

004B773F

C70424 F0134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013F0

[Arg1 = <vip\_access\_me.sub\_4013F0>

004B7746

E8 159BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7748

B9 80904C00

mov ecx,vip\_access\_me.4C9080

4C9080:&"e9hy94nono2hhk52k4dihy64k"

004B7749

C70424 B3C34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3B5

[Arg1 = "e9hy94nono2hhk52k4dihy64k"

004B7750

E8 499EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B775C

83EC 04

sub esp,4

004B775F

C70424 D0134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013D0

[Arg1 = <vip\_access\_me.sub\_4013D0>

004B7766

E8 559BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7768

B9 68904C00

mov ecx,vip\_access\_me.4C9068

4C9068:&"abc12316encrypted99fsnzsf"

004B7770

C70424 CFC34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3CF

[Arg1 = "abc12316encrypted99fsnzsf"

004B7777

E8 149EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B777C

83EC 04

sub esp,4

004B777F

C70424 80134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013B0

[Arg1 = <vip\_access\_me.sub\_4013B0>

004B7786

E8 559BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7788

B9 50904C00

mov ecx,vip\_access\_me.4C9050

4C9050:&"101566kokoko602hm612h35n2"

004B7790

C70424 E9C34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3E9

[Arg1 = "101566kokoko602hm612h35n2"

004B7797

E8 F49EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B779C

83EC 04

sub esp,4

004B779F

C70424 90134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401390

[Arg1 = <vip\_access\_me.sub\_401390>

004B77A6

E8 159BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77AB

B9 38904C00

mov ecx,vip\_access\_me.4C9038

4C9038:&"f0kes843toohard567asm7b73"

004B77B0

C70424 03C44B00

mov dword ptr ss:[esp],vip\_access\_me.4BC403

[Arg1 = "f0kes843toohard567asm7b73"

004B77B7

E8 049EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B77BC

83EC 04

sub esp,4

004B77BF

C70424 70134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401370

[Arg1 = <vip\_access\_me.sub\_401370>

004B77C6

E8 599EF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77CB

B9 20904C00

mov ecx,vip\_access\_me.4C9020

4C9020:&"five2156izx7o1hn7m891h2"

004B77D0

C70424 10C44B00

mov dword ptr ss:[esp],vip\_access\_me.4BC41D

[Arg1 = "five2156izx7o1hn7m891h2"

004B77D7

E8 B49EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B77DC

83EC 04

sub esp,4

004B77DF

C70424 50134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401350

[Arg1 = <vip\_access\_me.sub\_401350>

004B77E6

E8 D59BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77EB

8045 C4

lea eax,dword ptr ss:[ebp-3C]

004B77EE

890424

mov dword ptr ss:[esp],eax

[Arg1 = ...

004B77F3

83EC 04

sub esp,4

004B773C

83EC 04

sub esp,4

004B773F

C70424 F0134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013F0

[Arg1 = <vip\_access\_me.sub\_4013F0>

004B7746

E8 159BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7748

B9 80904C00

mov ecx,vip\_access\_me.4C9080

4C9080:&"e9hy94nono2hhk52k4dihy64k"

004B7749

C70424 B3C34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3B5

[Arg1 = "e9hy94nono2hhk52k4dihy64k"

004B7750

E8 499EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B775C

83EC 04

sub esp,4

004B775F

C70424 D0134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013D0

[Arg1 = <vip\_access\_me.sub\_4013D0>

004B7766

E8 559BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7768

B9 68904C00

mov ecx,vip\_access\_me.4C9068

4C9068:&"abc12316encrypted99fsnzsf"

004B7770

C70424 CFC34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3CF

[Arg1 = "abc12316encrypted99fsnzsf"

004B7777

E8 149EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B777C

83EC 04

sub esp,4

004B777F

C70424 80134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013B0

[Arg1 = <vip\_access\_me.sub\_4013B0>

004B7786

E8 559BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7788

B9 50904C00

mov ecx,vip\_access\_me.4C9050

4C9050:&"101566kokoko602hm612h35n2"

004B7790

C70424 E9C34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3E9

[Arg1 = "101566kokoko602hm612h35n2"

004B7797

E8 F49EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B779C

83EC 04

sub esp,4

004B779F

C70424 90134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401390

[Arg1 = <vip\_access\_me.sub\_401390>

004B77A6

E8 159BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77AB

B9 38904C00

mov ecx,vip\_access\_me.4C9038

4C9038:&"f0kes843toohard567asm7b73"

004B77B0

C70424 03C44B00

mov dword ptr ss:[esp],vip\_access\_me.4BC403

[Arg1 = "f0kes843toohard567asm7b73"

004B77B7

E8 049EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B77BC

83EC 04

sub esp,4

004B77BF

C70424 70134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401370

[Arg1 = <vip\_access\_me.sub\_401370>

004B77C6

E8 599EF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77CB

B9 20904C00

mov ecx,vip\_access\_me.4C9020

4C9020:&"five2156izx7o1hn7m891h2"

004B77D0

C70424 10C44B00

mov dword ptr ss:[esp],vip\_access\_me.4BC41D

[Arg1 = "five2156izx7o1hn7m891h2"

004B77D7

E8 B49EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B77DC

83EC 04

sub esp,4

004B77DF

C70424 50134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_401350

[Arg1 = <vip\_access\_me.sub\_401350>

004B77E6

E8 D59BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B77EB

8045 C4

lea eax,dword ptr ss:[ebp-3C]

004B77EE

890424

mov dword ptr ss:[esp],eax

[Arg1 = ...

004B77F3

83EC 04

sub esp,4

004B773C

83EC 04

sub esp,4

004B773F

C70424 F0134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013F0

[Arg1 = <vip\_access\_me.sub\_4013F0>

004B7746

E8 159BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7748

B9 80904C00

mov ecx,vip\_access\_me.4C9080

4C9080:&"e9hy94nono2hhk52k4dihy64k"

004B7749

C70424 B3C34B00

mov dword ptr ss:[esp],vip\_access\_me.4BC3B5

[Arg1 = "e9hy94nono2hhk52k4dihy64k"

004B7750

E8 499EF4FF

call vip\_access\_me.sub\_401590

[sub\_401590

004B775C

83EC 04

sub esp,4

004B775F

C70424 D0134000

mov dword ptr ss:[esp],vip\_access\_me.sub\_4013D0

[Arg1 = <vip\_access\_me.sub\_4013D0>

004B7766

E8 559BF4FF

call vip\_access\_me.sub\_4012C0

[sub\_4012C0

004B7768

B9 68904C00

mov ecx,vip\_access\_me.4C9068

4C9068:&"abc12

```

004B6400 804C24 04 lea ecx,dword ptr ss:[esp+4]
004B6404 83E4 F0 and esp,FFFFFFFF0
004B6407 FF71 FC push dword ptr ds:[ecx-4]
004B640A 55 push ebp
004B640B 89E5 mov ebp,esp
004B640D 57 push edi
004B640E 56 push esi
004B640F 8045 E8 lea eax,dword ptr ss:[ebp-18]
004B6412 53 push ebx
004B6413 51 push ecx
004B6414 81EC B8010000 sub esp,1B8
004B641A 8985 84FFFFFF mov dword ptr ss:[ebp-17C],eax
004B6420 8085 64FFFFFF lea eax,dword ptr ss:[ebp-19C]
004B6426 C785 7CFFFFFF 2022 mov dword ptr ss:[ebp-184],<vip_access_me.sub_402220>
004B6430 C785 80FFFFFF E481 mov dword ptr ss:[ebp-180],vip_access_me.4B81E4
004B643A C785 88FFFFFF DE6E mov dword ptr ss:[ebp-178],<vip_access_me.sub_4B86EDE>
004B6444 89A5 8CFFFFFF mov dword ptr ss:[ebp-174],esp
004B644A 890424 mov dword ptr ss:[esp],eax
004B644D E8 0E1FF7FF call <vip_access_me.sub_428360>
004B6452 E8 9916F7FF call <vip_access_me.sub_427AF0>
004B6457 8D85 A0FFFFFF lea eax,dword ptr ss:[ebp-160]
004B645D 8D8D B0FFFFFF lea ecx,dword ptr ss:[ebp-150]
004B6463 C785 9CFFFFFF 000C mov dword ptr ss:[ebp-164],0
004B646D C685 A0FFFFFF 00 mov byte ptr ss:[ebp-160],0
004B6474 8985 98FFFFFF mov dword ptr ss:[ebp-168],eax
004B647A C70424 1CC24B00 mov dword ptr ss:[esp],vip_access_me.4BC21C
004B6481 C785 68FFFFFF 010C mov dword ptr ss:[ebp-198],1
004B6488 E8 00B1F4FF call <vip_access_me.calc_len_of_string>
004B6490 5EC 04 sub esp,4
004B649B C74424 04 1DC24B00 mov dword ptr ss:[esp+4],vip_access_me.4BC21D
004B64A2 C70424 009D4C00 mov dword ptr ss:[esp],vip_access_me.4C9D00
004B64A9 C785 68FFFFFF 020C mov dword ptr ss:[ebp-198],2
004B64AC E8 FFDF4FFF call <vip_access_me.print_message>
004B64B1 8D85 B0FFFFFF lea eax,dword ptr ss:[ebp-150]
004B64B7 C70424 A09D4C00 mov dword ptr ss:[esp],vip_access_me.4C9DA0
004B64BE 894424 04 mov dword ptr ss:[esp+4],eax
004B64C2 E8 F9E3F4FF call <vip_access_me.input_string>
004B64C7 8D8D B0FFFFFF lea ecx,dword ptr ss:[ebp-150]

```

sub\_ask\_for\_data\_and\_check

esi:&"e9hy94nono2hhk52k4dihy64k"

[ebp-17C]:sub\_404860+1A

[ebp-184]:&"f5gz51xyxy6ggj96j1mlgz21j"

[esp]:&"f5gz51xyxy6ggj96j1mlgz21j"

Arg1 = 4BC21C

calc\_len\_of\_string

Arg2 = "Are you a vip member? (y/n): "

Arg1 = 4C9D00

print\_message

Arg2 = 4C9DA0

Arg1

input\_string

- And now, the function that really matters to us. The one that decrypts the VIP Code. It is in the address **00401CF0**. Just put a breakpoint at address **00401D67** and check that it is what is loaded into the **EAX** register that contains the memory address where the **VIP CODE** is.

```

00401CF0 55 push ebp
00401CF1 89E5 mov ebp,esp
00401CF3 81EC 88000000 sub esp,88
00401CF9 8045 F8 lea eax,dword ptr ss:[ebp-8]
00401CFF 8965 BC mov dword ptr ss:[ebp-4],esp
00401D06 C745 AC 20224000 mov dword ptr ss:[ebp-54],<vip_access_me.sub_402220>
00401D0D C745 B8 E41D4000 mov dword ptr ss:[ebp-50],vip_access_me.4B81DC
00401D14 8945 B4 mov dword ptr ss:[ebp-48],vip_access_me.401DE4
00401D17 8045 94 mov dword ptr ss:[ebp-4C],eax
00401D1A 890424 mov dword ptr ss:[esp],eax
00401D1D E8 3E660200 call <vip_access_me.sub_428360>
00401D22 8D45 D0 lea eax,dword ptr ss:[ebp-30]
00401D25 8B4D 0C mov ecx,dword ptr ss:[ebp+C]
00401D28 8945 C8 mov dword ptr ss:[ebp-38],eax
00401D2B 8B45 0C mov eax,dword ptr ss:[ebp+C]
00401D2E 8051 94 mov edx,dword ptr ds:[ecx+4]
00401D31 8D4D C8 lea ecx,dword ptr ss:[ebp-38]
00401D34 8B00 mov eax,dword ptr ds:[eax]
00401D36 01C2 add edx,eax
00401D38 890424 mov dword ptr ss:[esp],eax
00401D3B 895424 04 mov dword ptr ss:[esp+4],edx
00401D3F C745 98 FFFFFFFF mov dword ptr ss:[ebp-68],FFFFFFFF
00401D46 E8 B5F7FFFF call <vip_access_me.sub_401500>
00401D48 8D45 C8 lea eax,dword ptr ss:[ebp-38]
00401D4E 83EC 08 sub esp,8
00401D51 894424 04 mov dword ptr ss:[esp+4],eax
00401D55 8D45 E0 lea eax,dword ptr ss:[ebp-20]
00401D58 890424 mov dword ptr ss:[esp],eax
00401D5B C745 98 01000000 mov dword ptr ss:[ebp-68],1
00401D62 E8 39FDFFFF call <vip_access_me.decrypt_string>
00401D6A 8D45 E0 lea eax,dword ptr ss:[ebp-20]
00401D6D 890424 mov dword ptr ss:[esp],eax
00401D70 8B4D 0C mov ecx,dword ptr ss:[ebp+C]
00401D73 C745 98 02000000 mov dword ptr ss:[ebp-68],2
00401D77 E8 D4340A00 call <vip_access_me.search_string>
00401D7C 8B45 E0 mov eax,dword ptr ss:[ebp-20]
00401D7F 8D55 E8 lea ecx,dword ptr ss:[ebp-18]

```

decrypt\_vip\_code

[ebp-54]:sub\_402220

[esp]:&"f5gz51xyxy6ggj96j1mlgz21j"

[ebp+C]:&"e9hy94nono2hhk52k4dihy64k"

[ebp-38]:&"f5gz51xyxy6ggj96j1mlgz21j"

[ebp+C]:&"e9hy94nono2hhk52k4dihy64k"

[ebp-38]:&"f5gz51xyxy6ggj96j1mlgz21j"

eax:&"f5gz51xyxy6ggj96j1mlgz21j", [eax]

eax:&"f5gz51xyxy6ggj96j1mlgz21j"

Arg2

Arg1 = edx:EntryPoint

sub\_401500

[ebp-38]:&"f5gz51xyxy6ggj96j1mlgz21j"

Arg2

[ebp-20]:&"f5gz51xyxy6ggj96j1mlgz21j"

Arg1

sub\_401AA0

Decrypted string

Arg1

[ebp+C]:&"e9hy94nono2hhk52k4dihy64k"

search\_string

[ebp-20]:&"f5gz51xyxy6ggj96j1mlgz21j"

Here are the list of names, encoded and decoded vip codes are:

name	encrypted vip code	decrypted vip code
joe	e9hy94nono2hhk52k4dihy64k	f5gz51xyxy6ggj96j1mlgz21j
nick	abc12316encrypted99fsnzs	bac468i2fxctzvrfm55eqx0qe
monkey	lol566kokoko602hm6i2h35n2	iyi922jyjjy2o6gd216g89x6
dmitry	jokes843toohard567asm7b73	kyjfq318ryygbtm927bqd7a78
leonard	five2156sizx67olhn7m891h2	elwf6492q10n27y4gx7d354g6



But something curious happens. Only work VIP Codes for *joe* and *monkey* users. The other VIP Codes that are generated when tested do not seem correct as the following message is displayed: **"Please enter lower english letters and numbers only!"**

*Result of the two VIP Codes that work.*

```

CrackMe\crackmes.one\toaster-VIP_access_me>VIP_access_me.exe
Are you a vip member? (y/n): y
What is your name?: monkey
Please enter your vip code: iyi922jyjjy2o6gd2l6g89x6
Welcome vip member monkey!
#####
#                                     #
#      --\` \                         #
#      | \   \ \ \                   #
#      --\c` ` )                     #
#      ~~~~~ /  / ~~~               #
#      == /  /                      #
#                                     #
#####
Presione una tecla para continuar . . .

```

```

CrackMe\crackmes.one\toaster-VIP_access_me>VIP_access_me.exe
Are you a vip member? (y/n): y
What is your name?: joe
Please enter your vip code: f5gz51xyxy6ggj96j1mlgz21j
Welcome vip member joe!
#####
#                                     #
#      --\` \                         #
#      | \   \ \ \                   #
#      --\c` ` )                     #
#      ~~~~~ /  / ~~~               #
#      == /  /                      #
#                                     #
#####
Presione una tecla para continuar . . .

```

*VIP Codes that do not work: "Please enter lower english letters and numbers only!"*

```

CrackMe\crackmes.one\toaster-VIP_access_me>VIP_access_me.exe
Are you a vip member? (y/n): y
What is your name?: nick
Please enter your vip code: bac468i2fxctzvrfm55eqx0qe
Please enter lower english letters and numbers only!
Presione una tecla para continuar . . .

```

That's all folks!!!