
How to find serial in TCA Trial - CrackMe #1

Cracker: **stealthFIGHTER**

Target: **TCA Trial - CrackMe #1**

Tools: SmartCheck
Brain

Where: <http://tca.tsx.org/>

Protection: Serial number, VB crackme.

Sorry for my English, it's not my mother language.

Step 1:

=====
Run SmartCheck > open crackme and run (F5) > Errors > Acknowledge them. Once it's loaded enter your registration details.
(I entered iNFiNiTY as a name, WorldWideWeb as a group and 2319998 as s/n.)
=====

Push "Check It!" button. Nag > bad serial. Go to SmartCheck > you'll see:
=====

Click

- Len(String:"iNFiNiTY...") returns LONG:20
- Long (20) -> Integer (20)
- Mid\$(String:"iNFiNiTY...", long:1, VARIANT:Integer:1)

Lot of strings here

- Asc(String:"i") returns Integer:105
- Mid\$(String:"iNFiNiTY...", long:1, VARIANT:Integer:1)
- Asc(String:"i") returns Integer:105
- Mid\$(String:"iNFiNiTY...", long:1, VARIANT:Integer:1)
- Asc(String:"i") returns Integer:105
- Mid\$(String:"iNFiNiTY...", long:1, VARIANT:Integer:1)
- Asc(String:"i") returns Integer:105
- Mid\$(String:"iNFiNiTY...", long:1, VARIANT:Integer:1)
- Asc(String:"i") returns Integer:105
- Mid\$(String:"iNFiNiTY...", long:1, VARIANT:Integer:1)
- Asc(String:"i") returns Integer:105
- Asc(String:"iNFiNiTY") returns Integer:105

Thread 1 [thread id:4290933777 (0xFFC27411)]

Thread 0 [thread id:4290971257 (0xFFC30679)]

- Chr\$(Integer:13)
- Chr\$(Integer:13)
- Chr\$(Integer:13)
- MsgBox(VARIANT:String:"If you a...", Integer:64, VARIANT:)

=====

=====

You'll get messagebox (MsgBox). Click on it. Now in SmartCheck click on "Show All Events" button. Now scroll up, till you find your name. For me its here:

=====

```
+ Asc(String:"INFiNiTY") returns Integer:105
  __vbaVarSub(VARIANT:Double:3.17083e+010, VARIANT:Double:3.16932e+010) returns DWord:440948
  __vbaVarMul(VARIANT:Double:1.5092e+007, VARIANT:Integer:105) returns DWord:440AF4
  __vbaVarMove(VARIANT:Double:1.58466e+009, VARIANT:Empty) returns DWord:4407B0
+ __vbaFreeStr(LPBSTR:0066F2C0) returns DWord:20
  __vbaFreeObj(LPINTERFACE *:0066F2BC)
  __vbaObjSet(LPINTERFACE *:0066F3B0, LPINTERFACE:02DFDDFC) returns L
  GetFocus() returns HWND:824
  HeapAlloc(HANDLE:02DF0000, FLAGS:00000000, DWord:00000008) returns I
  GetFocus() returns HWND:824
  MultiByteToWideChar(unsigned int:00000000, FLAGS:00000000, PTR:02DFF3A0, Count:1, LPWSTR:00000000, DWord:00000007) returns LPVOID:4407B0
  MultiByteToWideChar(unsigned int:00000000, FLAGS:00000000, PTR:02DFF3A0, Count:1, LPWSTR:00000000, DWord:00000007) returns LPVOID:4407B0
  HeapFree(HANDLE:02DF0000, FLAGS:00000000, PTR:02DFF3AC) returns BOOL:1
+ __vbaVarTstEq(VARIANT:Const String:"", VARIANT:Double:1.58466e+009) returns DWord:440D78
:
:
:
  __vbaStrMove(String:"If you a...", LPBSTR:0066F3E8) returns DWord:440948
  __vbaStrCat(String:"if you'r...", String:"If you a...") returns DWord:440AF4
  __vbaStrMove(String:"If you a...", LPBSTR:0066F3E4) returns DWord:440AF4
  __vbaStrMove(String:"I", LPBSTR:0066F3E0) returns DWord:4407B0
+ __vbaStrCat(String:"I", String:"If you a...") returns DWord:440CD4
  __vbaStrMove(String:"If you a...", LPBSTR:0066F3DC) returns DWord:440CD4
+ __vbaStrCat(String:"Try it a...", String:"If you a...") returns DWord:440D78
+ MsgBox(VARIANT:String:"If you a...", Integer:64, VARIANT:String:"Try it a...", VA
```

=====

Once you find your name look down > there is **__vbaVarMove** function > click on it and in the **Details window** you will see your s/n: **double.dbVal=yourserialnumber** (I have got 1584658110).

=====

CrackMe cracked!

=====



=====

If I make a mistake, please e-mail me
stealthFIGHTER@another.com
You can also find me on the web:

----- [<http://nitrous.hop.to/>] -----

=====