

# darkusurp's darkusurp login ver 1.00

## Solution By COSTY

---

The crackme is a .NET application so open the crackme with Reflector.

This is the check routine.

```
Private Sub enter1_Click(ByVal sender As Object, ByVal e As EventArgs)
    Dim str As String = Me.de3
    Me.confirmation.Text = (Me.password.Text & "ofthe" & Me.username.Text & str)
    If (Me.count >= 3) Then
        Me.confirmation.Text = "Reset Application"
        If (Me.count = 3) Then
            Interaction.MsgBox("Too Many Attempts (reset)", MsgBoxStyle.OkOnly, Nothing)
        End If
    End If
    If (Me.count < 3) Then
        If (Me.confirmation.Text = "killeroftthebees54") Then
            Me.confirmation.Text = "Correct"
            Me.Hide
            MyProject.Forms.main.Opacity = 100
        Else
            Me.confirmation.Text = "Wrong"
        End If
    End If
    If (Me.count < 3) Then
        Me.count += 1
    End If
End Sub
```

The variable “count” counts the attempts to get the valid password. If you enter 3 times an invalid name or an invalid password the program don't let you to continue.

The most important lines of the crackme are these:

```
Me.confirmation.Text = (Me.password.Text & "ofthe" & Me.username.Text & str)
```

.....

```
If (Me.count < 3) Then
    If (Me.confirmation.Text = "killeroftthebees54") Then
        Me.confirmation.Text = "Correct"
        Me.Hide
        MyProject.Forms.main.Opacity = 100
    End If
End If
```

.....

Me.confirmation.Text should be "killeroftthebees54" but Me.confirmation.Text is (Me.password.Text & "ofthe" & Me.username.Text & str) so

(Me.password.Text & "ofthe" & Me.username.Text & str) must be equal to "killeroftthebees54"

But what is str?? We have to know its value in order to chose a correct name and passoword.

In order to get it's value i made a patched verion of the program.

In fact i changed the routine enter1\_Click in this way

```
Private Sub enter1_Click(ByVal sender As Object, ByVal e As EventArgs)
    Dim str As String = Me.de3
    Me.confirmation.Text = (Me.password.Text & "ofthe" & Me.username.Text & str)
End Sub
```

I added the patched verion of the program that shows the str value to the archive.

Now if you open the patched verion and type “John” as name and “Red” as password and then you press “enter”...

in the confirmation box you will see johnofthered54.

So the password textbox is near the label “Username”, the username textbox is near the password label. And the str string is 54.

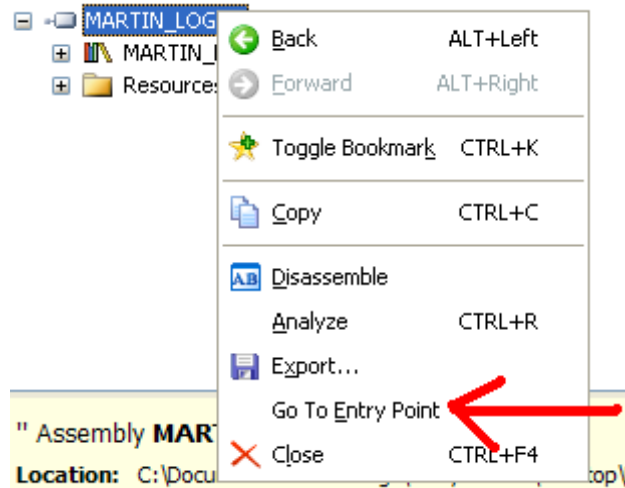
In the box at the right of username type “killer”

In the box at the right of password type “bees”

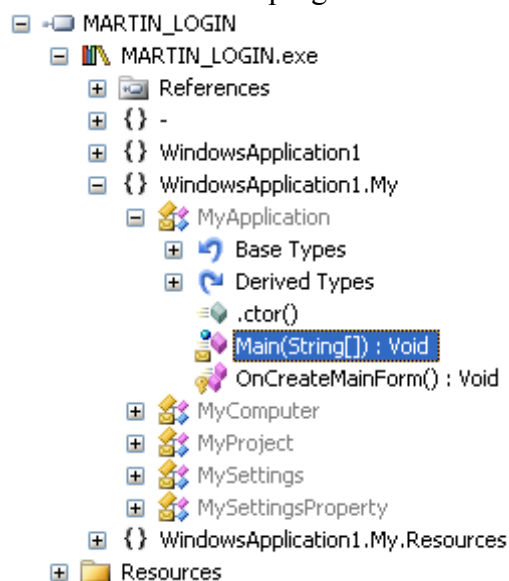


There is another way to show the main window without knowing the right serial and password.

Open the crackme in reflector and then go to the entry point as shown



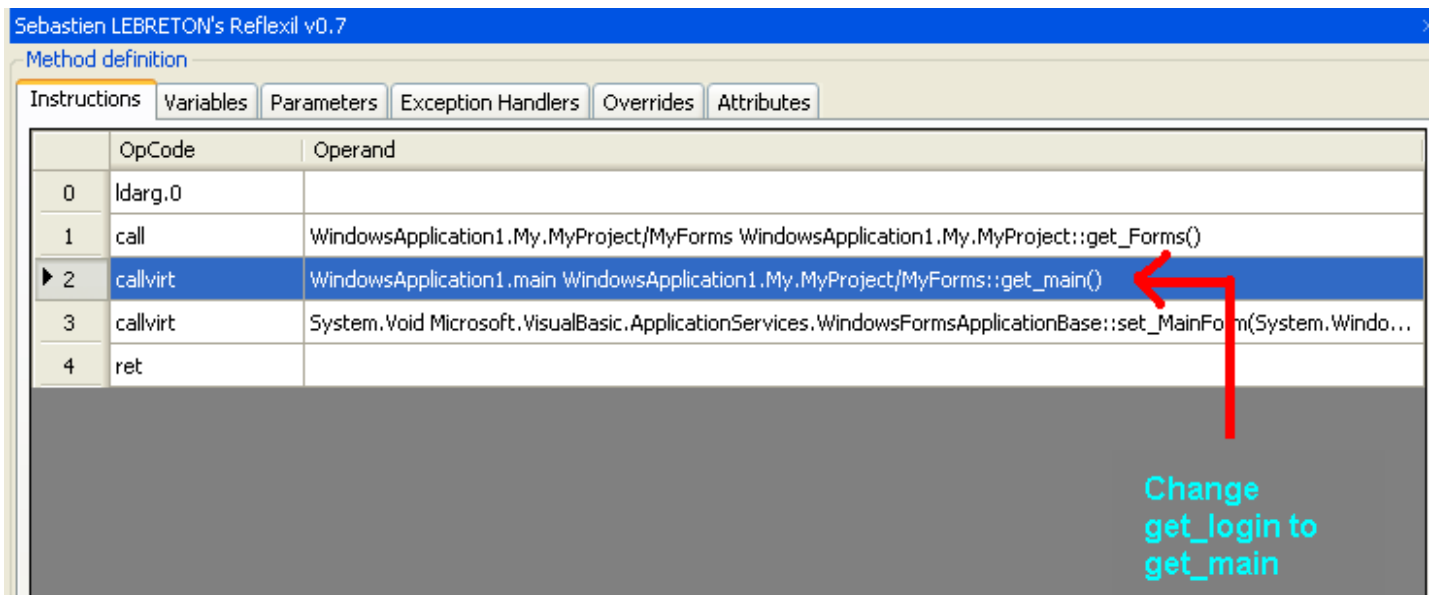
Reflector will display the first instruction that the program executes when it starts.



Look at oncreatemainform

```
<DebuggerStepThrough> _  
Protected Overrides Sub OnCreateMainForm()  
    Me.MainForm = MyProject.Forms.login  
End Sub
```

The first form created is the form of login now use Reflexil plugin to patch it in this way.



I added to the archive the patched version of the program that shows the main window directly.

Now the first form crated is the main form so you don't need to type a password.  
Bye.