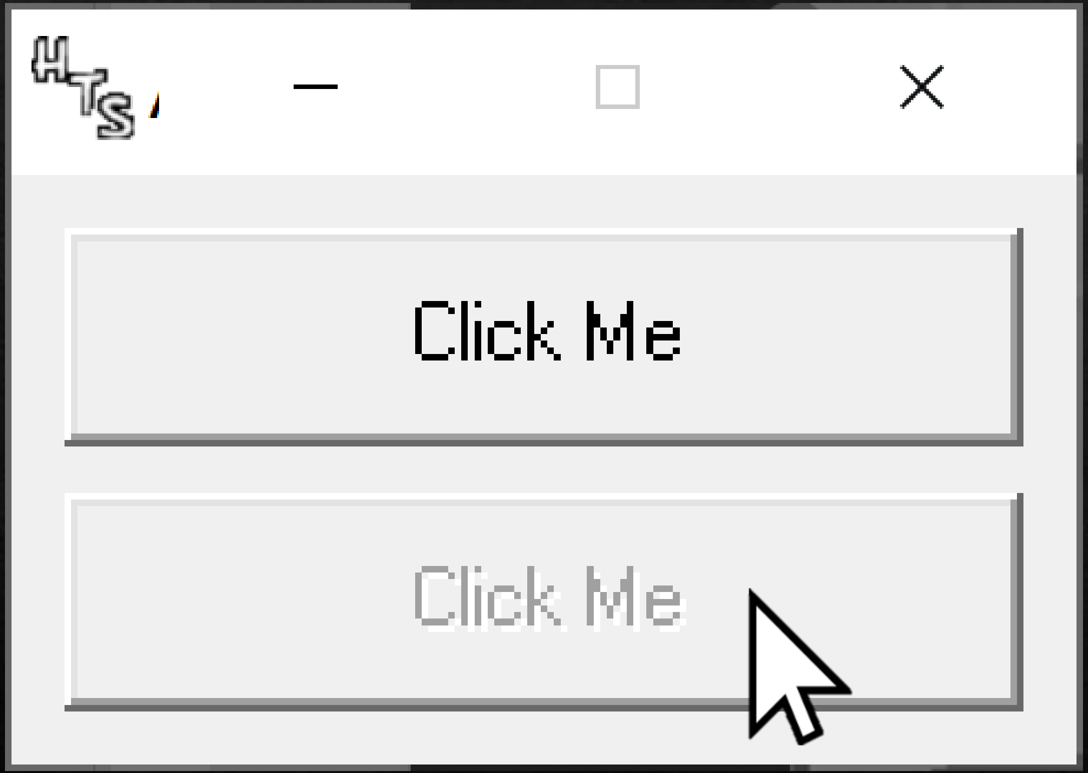
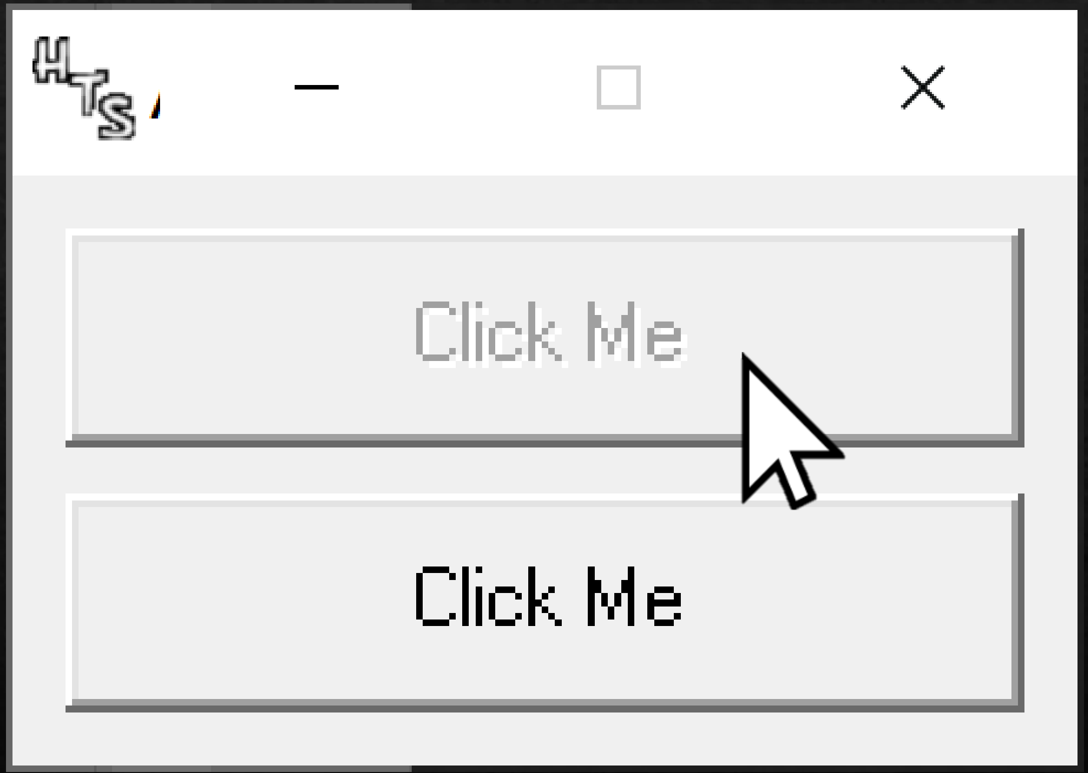
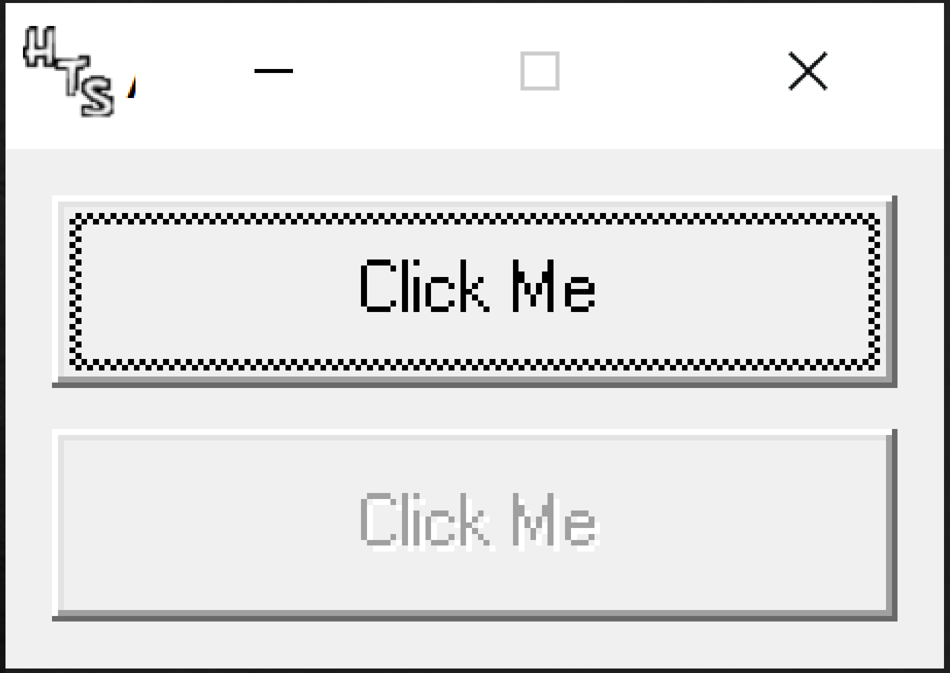
Application Challenge 4
Press the Button.

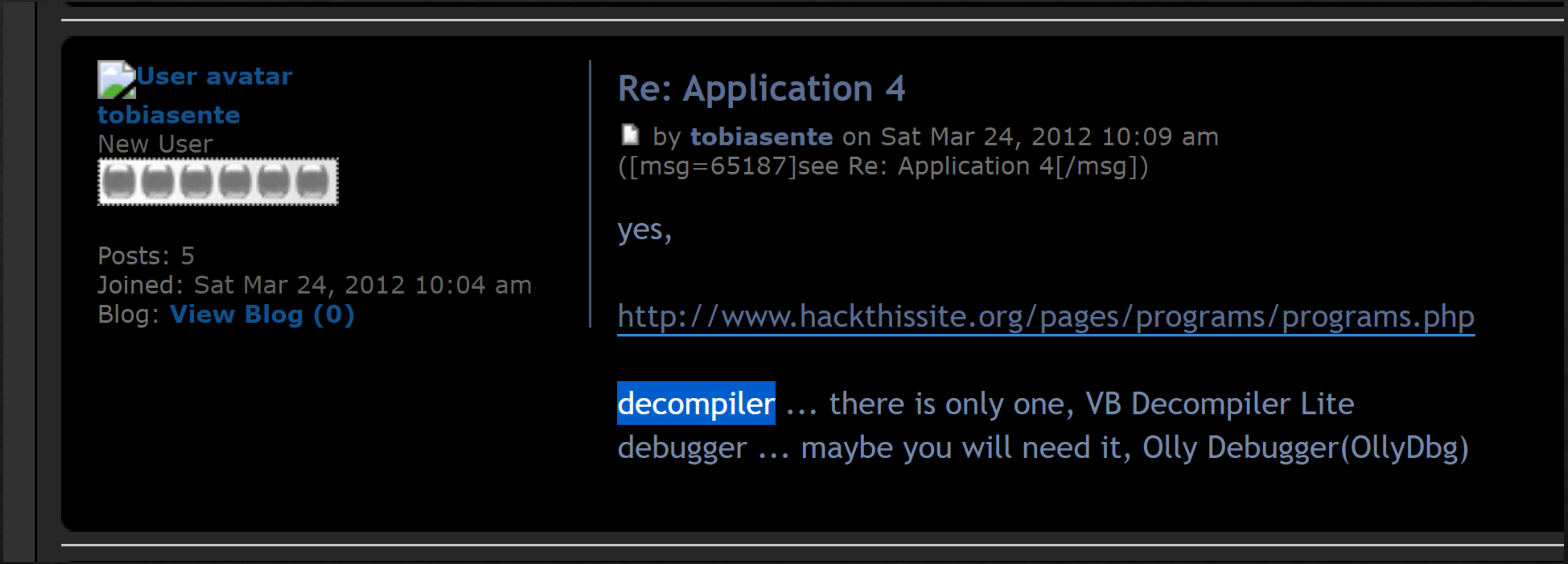
第六組 1053328 黃子庭


Click Me
Click Me


Click Me
Click Me



使用鍵盤也無法按下按鈕



User avatar
tobiasente
New User

Posts: 5
Joined: Sat Mar 24, 2012 10:04 am
Blog: View Blog (0)

Re: Application 4

by tobiasente on Sat Mar 24, 2012 10:09 am
([msg=65187]see Re: Application 4[/msg])

yes,

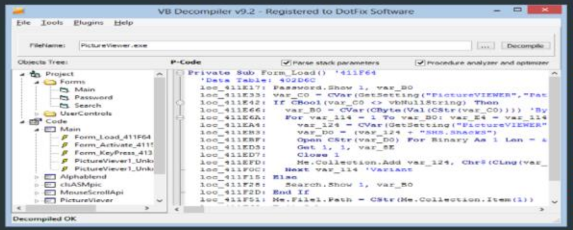
http://www.hackthissite.org/pages/programs/programs.php

decompiler ... there is only one, VB Decompiler Lite
debugger ... maybe you will need it, Olly Debugger(OllyDbg)

搜尋解法 - 使用VB反組譯工具

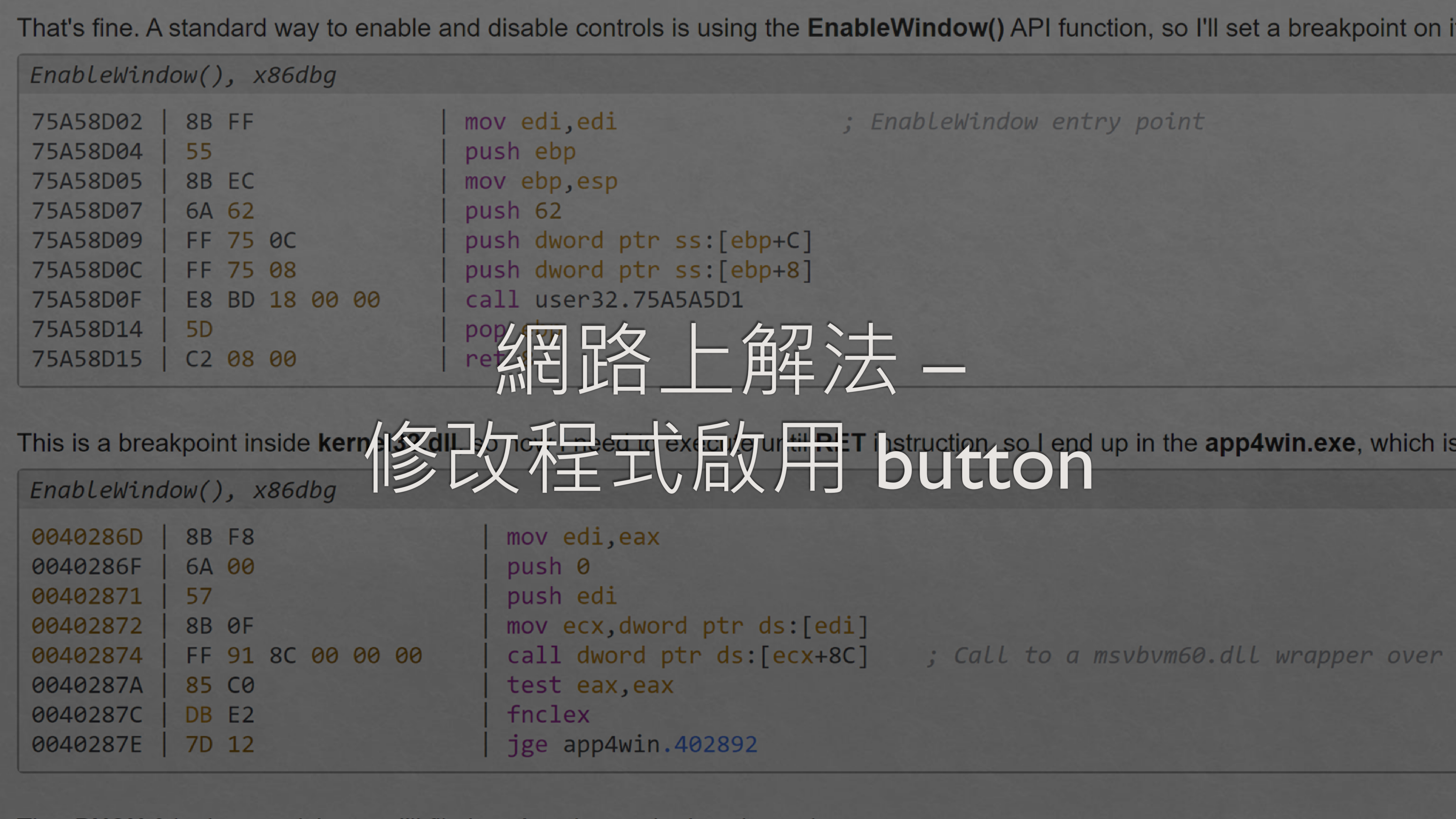
VB Decompiler Lite

VB Decompiler is decompiler for programs (EXE, DLL or OCX) written in Visual Basic 5.0 and 6.0 and disassembler for programs written on .NET technology.



```
Private Sub Form_Load() '411F64
  'Data Table: 402D6C
  loc_411E17: Password.Show 1, var_B0
  loc_411E33: var_C0 = CVar(GetSetting("PictureVIEWER","Pat
  loc_411E42: If CBool(var_C0 <> vbNullString) Then
  loc_411E66:   var_B0 = CVar(CByte(Val(CStr(var_C0)))) 'By
  loc_411E6A:   For var_114 = 1 To var_B0: var_E4 = var_114
  loc_411EA4:     var_124 = CVar(GetSetting("PictureVIEWER"
  loc_411EB3:     var_D0 = (var_124 + "SHS.SnackS")
  loc_411EBF:     Open CStr(var_D0) For Binary As 1 Len =
  loc_411ED3:     Get 1, 1, var_8E
  loc_411ED7:     Close 1
  loc_411EFD:     Me.Collection.Add var_124, Chr$(CLng(var_
  loc_411F0C:   Next var_114 'Variant
  loc_411F15: Else
  loc_411F28:   Search.Show 1, var_B0
  loc_411F2D: End If
  loc_411F51: Me.File1.Path = CStr(Me.Collection.Item(1))
```

網路上解法 –
修改程式啟用 button



That's fine. A standard way to enable and disable controls is using the **EnableWindow()** API function, so I'll set a breakpoint on i

EnableWindow(), x86dbg

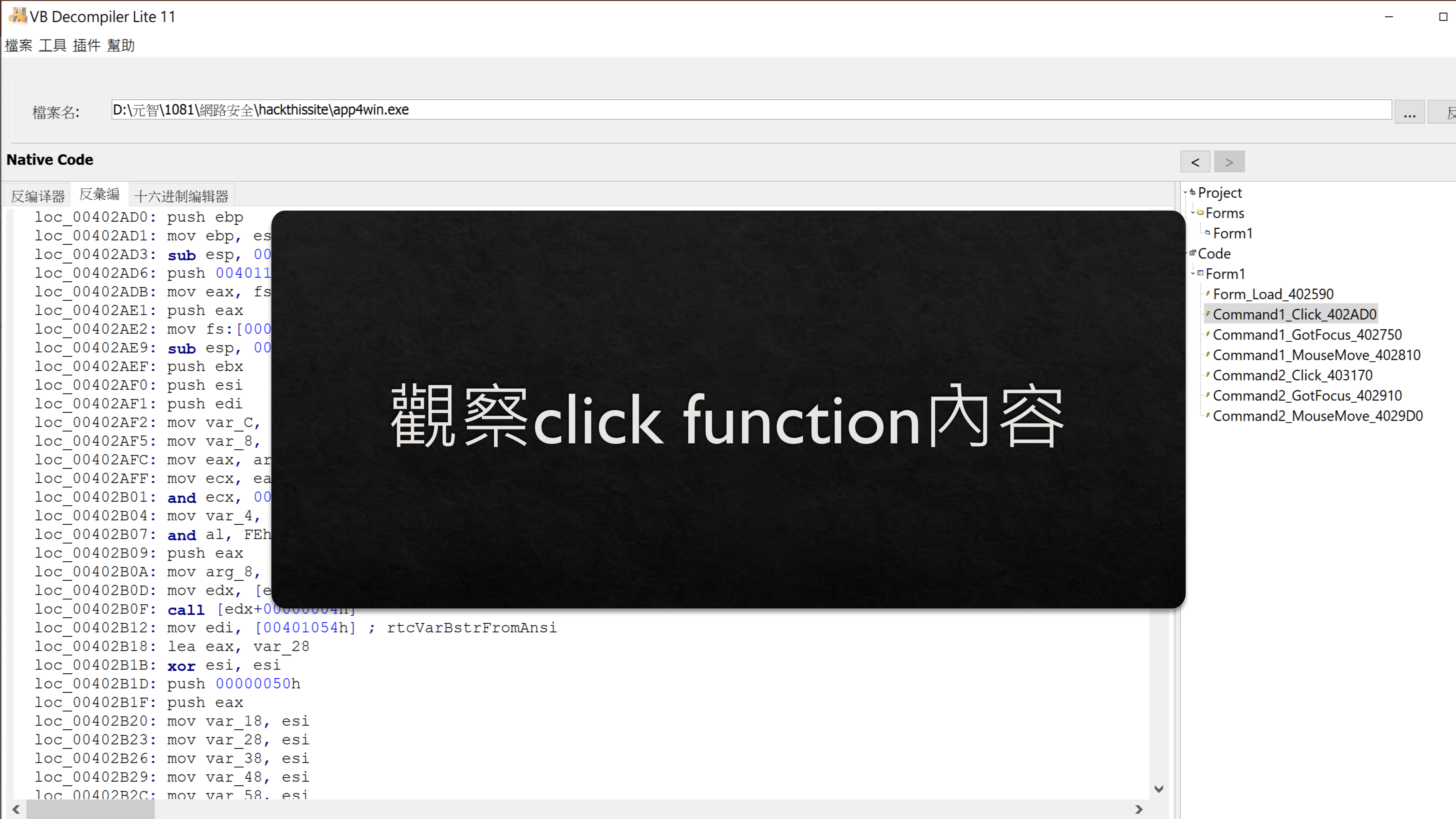
```
75A58D02 | 8B FF                 | mov edi,edi                  ; EnableWindow entry point
75A58D04 | 55                    | push ebp
75A58D05 | 8B EC                 | mov ebp,esp
75A58D07 | 6A 62                 | push 62
75A58D09 | FF 75 0C              | push dword ptr ss:[ebp+C]
75A58D0C | FF 75 08              | push dword ptr ss:[ebp+8]
75A58D0F | E8 BD 18 00 00        | call user32.75A5A5D1
75A58D14 | 5D                    | pop ebp
75A58D15 | C2 08 00              | ret 8
```

This is a breakpoint inside **kernel32.dll** so no need to execute until **RET** instruction, so I end up in the **app4win.exe**, which is

EnableWindow(), x86dbg

```
0040286D | 8B F8                   | mov edi,eax
0040286F | 6A 00                   | push 0
00402871 | 57                      | push edi
00402872 | 8B 0F                   | mov ecx,dword ptr ds:[edi]
00402874 | FF 91 8C 00 00 00       | call dword ptr ds:[ecx+8C]    ; Call to a msvbvm60.dll wrapper over
0040287A | 85 C0                   | test eax,eax
0040287C | DB E2                   | fnclex
0040287E | 7D 12                   | jge app4win.402892
```

思考方向

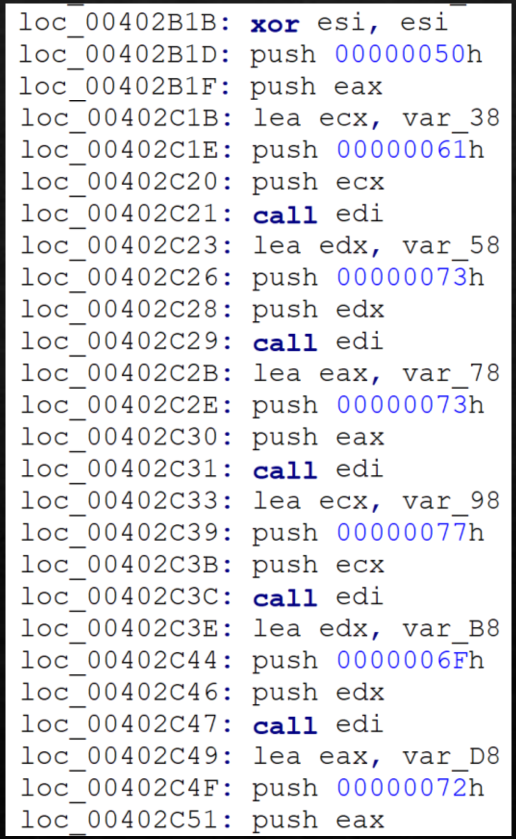


D:\元智\1081\網路安全\hackthissite\app4win.exe

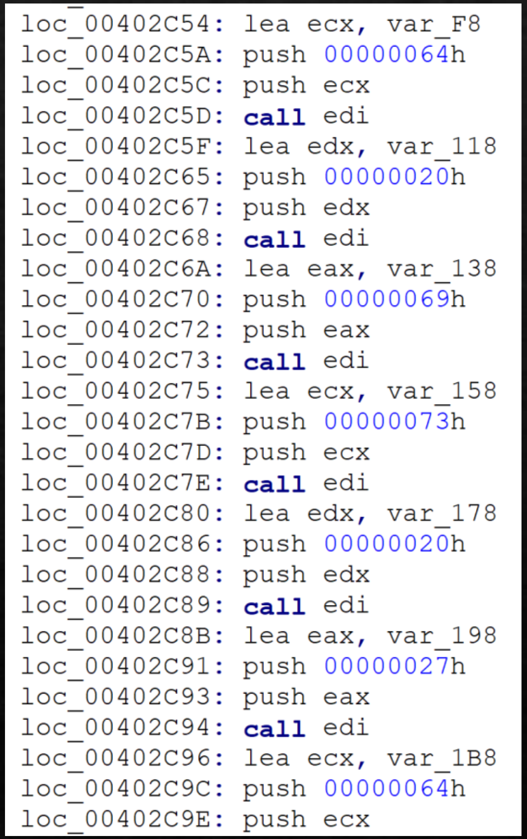
```
loc_00402AD0: push ebp
loc_00402AD1: mov ebp, es
loc_00402AD3: sub esp, 00
loc_00402AD6: push 004011
loc_00402ADB: mov eax, fs
loc_00402AE1: push eax
loc_00402AE2: mov fs:[000
loc_00402AE9: sub esp, 00
loc_00402AEF: push ebx
loc_00402AF0: push esi
loc_00402AF1: push edi
loc_00402AF2: mov var_C,
loc_00402AF5: mov var_8,
loc_00402AFC: mov eax, ar
loc_00402AFF: mov ecx, ea
loc_00402B01: and ecx, 00
loc_00402B04: mov var_4,
loc_00402B07: and al, FEh
loc_00402B09: push eax
loc_00402B0A: mov arg_8,
loc_00402B0D: mov edx, [e
loc_00402B0F: call [edx+00000004h]
loc_00402B12: mov edi, [00401054h] ; rtcVarBstrFromAnsi
loc_00402B18: lea eax, var_28
loc_00402B1B: xor esi, esi
loc_00402B1D: push 00000050h
loc_00402B1F: push eax
loc_00402B20: mov var_18, esi
loc_00402B23: mov var_28, esi
loc_00402B26: mov var_38, esi
loc_00402B29: mov var_48, esi
loc_00402B2C: mov var_58, esi
```

觀察click function內容

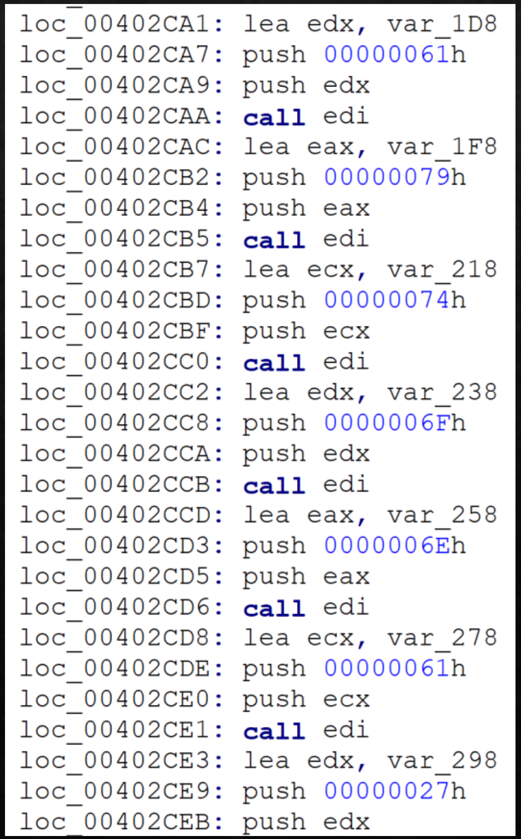
發現多行類似程式碼



```
loc_00402B1B: xor esi, esi
loc_00402B1D: push 00000050h
loc_00402B1F: push eax
loc_00402C1B: lea ecx, var_38
loc_00402C1E: push 00000061h
loc_00402C20: push ecx
loc_00402C21: call edi
loc_00402C23: lea edx, var_58
loc_00402C26: push 00000073h
loc_00402C28: push edx
loc_00402C29: call edi
loc_00402C2B: lea eax, var_78
loc_00402C2E: push 00000073h
loc_00402C30: push eax
loc_00402C31: call edi
loc_00402C33: lea ecx, var_98
loc_00402C39: push 00000077h
loc_00402C3B: push ecx
loc_00402C3C: call edi
loc_00402C3E: lea edx, var_B8
loc_00402C44: push 0000006Fh
loc_00402C46: push edx
loc_00402C47: call edi
loc_00402C49: lea eax, var_D8
loc_00402C4F: push 00000072h
loc_00402C51: push eax
```

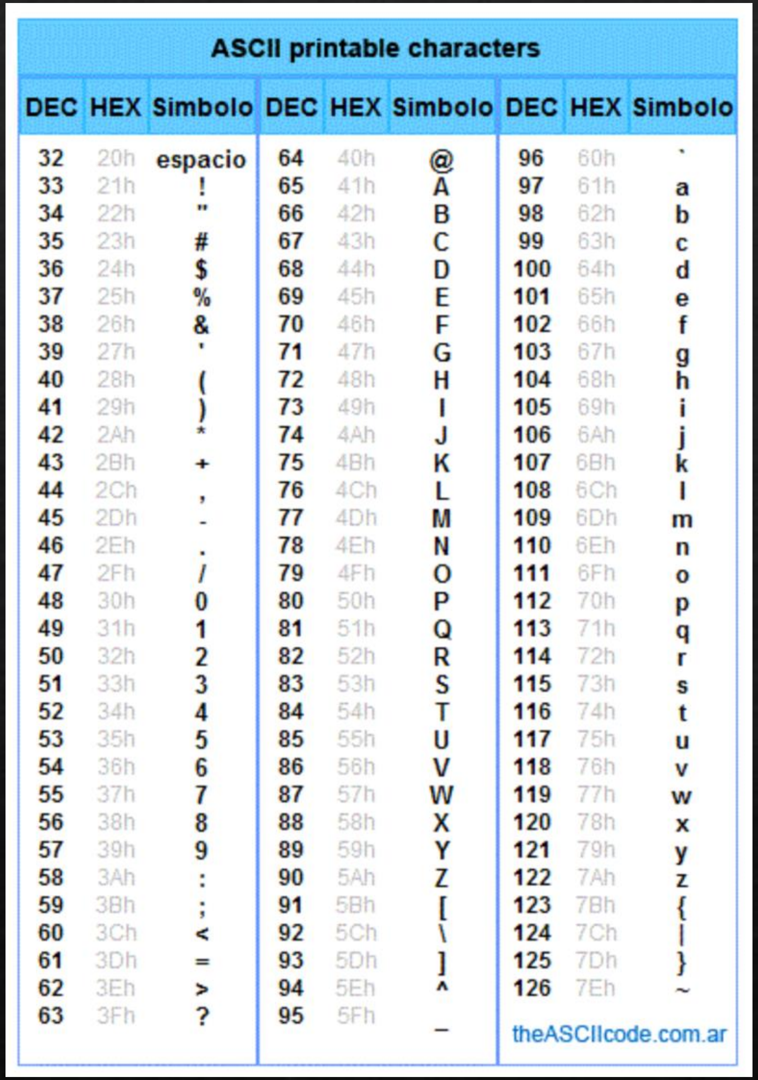


```
loc_00402C54: lea ecx, var_F8
loc_00402C5A: push 00000064h
loc_00402C5C: push ecx
loc_00402C5D: call edi
loc_00402C5F: lea edx, var_118
loc_00402C65: push 00000020h
loc_00402C67: push edx
loc_00402C68: call edi
loc_00402C6A: lea eax, var_138
loc_00402C70: push 00000069h
loc_00402C72: push eax
loc_00402C73: call edi
loc_00402C75: lea ecx, var_158
loc_00402C7B: push 00000073h
loc_00402C7D: push ecx
loc_00402C7E: call edi
loc_00402C80: lea edx, var_178
loc_00402C86: push 00000020h
loc_00402C88: push edx
loc_00402C89: call edi
loc_00402C8B: lea eax, var_198
loc_00402C91: push 00000027h
loc_00402C93: push eax
loc_00402C94: call edi
loc_00402C96: lea ecx, var_1B8
loc_00402C9C: push 00000064h
loc_00402C9E: push ecx
```



```
loc_00402CA1: lea edx, var_1D8
loc_00402CA7: push 00000061h
loc_00402CA9: push edx
loc_00402CAA: call edi
loc_00402CAC: lea eax, var_1F8
loc_00402CB2: push 00000079h
loc_00402CB4: push eax
loc_00402CB5: call edi
loc_00402CB7: lea ecx, var_218
loc_00402CBD: push 00000074h
loc_00402CBF: push ecx
loc_00402CC0: call edi
loc_00402CC2: lea edx, var_238
loc_00402CC8: push 0000006Fh
loc_00402CCA: push edx
loc_00402CCB: call edi
loc_00402CCD: lea eax, var_258
loc_00402CD3: push 0000006Eh
loc_00402CD5: push eax
loc_00402CD6: call edi
loc_00402CD8: lea ecx, var_278
loc_00402CDE: push 00000061h
loc_00402CE0: push ecx
loc_00402CE1: call edi
loc_00402CE3: lea edx, var_298
loc_00402CE9: push 00000027h
loc_00402CEB: push edx
```

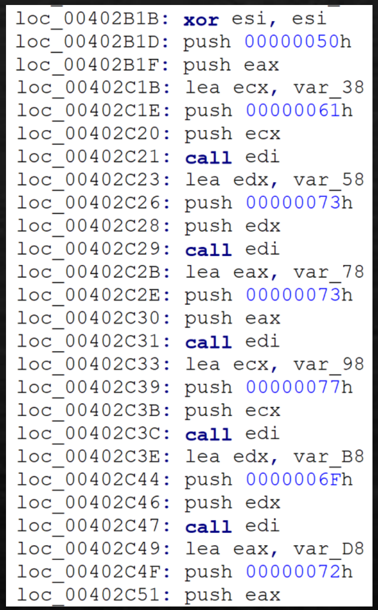
比對ASCII碼



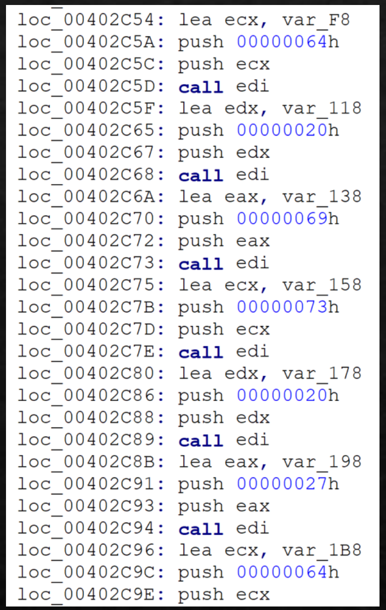
ASCII printable characters

DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo
32	20h	espacio	64	40h	@	96	60h	`
33	21h	!	65	41h	A	97	61h	a
34	22h	"	66	42h	B	98	62h	b
35	23h	#	67	43h	C	99	63h	c
36	24h	$	68	44h	D	100	64h	d
37	25h	%	69	45h	E	101	65h	e
38	26h	&	70	46h	F	102	66h	f
39	27h	'	71	47h	G	103	67h	g
40	28h	(	72	48h	H	104	68h	h
41	29h	)	73	49h	I	105	69h	i
42	2Ah	*	74	4Ah	J	106	6Ah	j
43	2Bh	+	75	4Bh	K	107	6Bh	k
44	2Ch	,	76	4Ch	L	108	6Ch	l
45	2Dh	-	77	4Dh	M	109	6Dh	m
46	2Eh	.	78	4Eh	N	110	6Eh	n
47	2Fh	/	79	4Fh	O	111	6Fh	o
48	30h	0	80	50h	P	112	70h	p
49	31h	1	81	51h	Q	113	71h	q
50	32h	2	82	52h	R	114	72h	r
51	33h	3	83	53h	S	115	73h	s
52	34h	4	84	54h	T	116	74h	t
53	35h	5	85	55h	U	117	75h	u
54	36h	6	86	56h	V	118	76h	v
55	37h	7	87	57h	W	119	77h	w
56	38h	8	88	58h	X	120	78h	x
57	39h	9	89	59h	Y	121	79h	y
58	3Ah	:	90	5Ah	Z	122	7Ah	z
59	3Bh	;	91	5Bh	[	123	7Bh	{
60	3Ch	<	92	5Ch	\	124	7Ch	|
61	3Dh	=	93	5Dh	]	125	7Dh	}
62	3Eh	>	94	5Eh	^	126	7Eh	~
63	3Fh	?	95	5Fh	_			

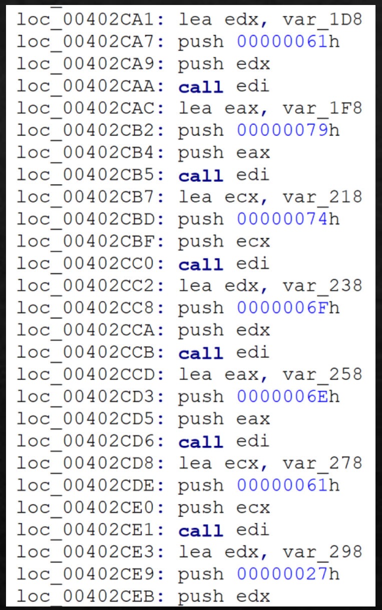
theASCIIcode.com.ar



```
loc_00402B1B: xor esi, esi
loc_00402B1D: push 00000050h
loc_00402B1F: push eax
loc_00402C1B: lea ecx, var_38
loc_00402C1E: push 00000061h
loc_00402C20: push ecx
loc_00402C21: call edi
loc_00402C23: lea edx, var_58
loc_00402C26: push 00000073h
loc_00402C28: push edx
loc_00402C29: call edi
loc_00402C2B: lea eax, var_78
loc_00402C2E: push 00000073h
loc_00402C30: push eax
loc_00402C31: call edi
loc_00402C33: lea ecx, var_98
loc_00402C39: push 00000077h
loc_00402C3B: push ecx
loc_00402C3C: call edi
loc_00402C3E: lea edx, var_B8
loc_00402C44: push 0000006Fh
loc_00402C46: push edx
loc_00402C47: call edi
loc_00402C49: lea eax, var_D8
loc_00402C4F: push 00000072h
loc_00402C51: push eax
```

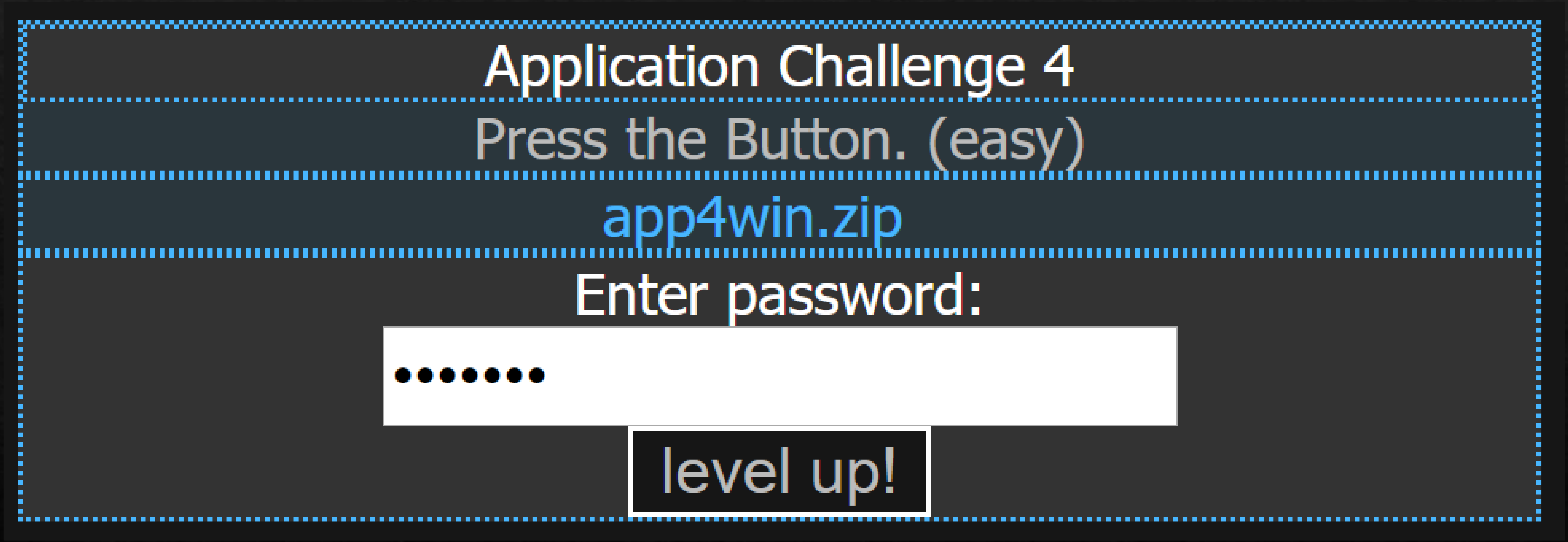


```
loc_00402C54: lea ecx, var_F8
loc_00402C5A: push 00000064h
loc_00402C5C: push ecx
loc_00402C5D: call edi
loc_00402C5F: lea edx, var_118
loc_00402C65: push 00000020h
loc_00402C67: push edx
loc_00402C68: call edi
loc_00402C6A: lea eax, var_138
loc_00402C70: push 00000069h
loc_00402C72: push eax
loc_00402C73: call edi
loc_00402C75: lea ecx, var_158
loc_00402C7B: push 00000073h
loc_00402C7D: push ecx
loc_00402C7E: call edi
loc_00402C80: lea edx, var_178
loc_00402C86: push 00000020h
loc_00402C88: push edx
loc_00402C89: call edi
loc_00402C8B: lea eax, var_198
loc_00402C91: push 00000027h
loc_00402C93: push eax
loc_00402C94: call edi
loc_00402C96: lea ecx, var_1B8
loc_00402C9C: push 00000064h
loc_00402C9E: push ecx
```



```
loc_00402CA1: lea edx, var_1D8
loc_00402CA7: push 00000061h
loc_00402CA9: push edx
loc_00402CAA: call edi
loc_00402CAC: lea eax, var_1F8
loc_00402CB2: push 00000079h
loc_00402CB4: push eax
loc_00402CB5: call edi
loc_00402CB7: lea ecx, var_218
loc_00402CBD: push 00000074h
loc_00402CBF: push ecx
loc_00402CC0: call edi
loc_00402CC2: lea edx, var_238
loc_00402CC8: push 0000006Fh
loc_00402CCA: push edx
loc_00402CCB: call edi
loc_00402CCD: lea eax, var_258
loc_00402CD3: push 0000006Eh
loc_00402CD5: push eax
loc_00402CD6: call edi
loc_00402CD8: lea ecx, var_278
loc_00402CDE: push 00000061h
loc_00402CE0: push ecx
loc_00402CE1: call edi
loc_00402CE3: lea edx, var_298
loc_00402CE9: push 00000027h
loc_00402CEB: push edx
```

Password is 'daytona'



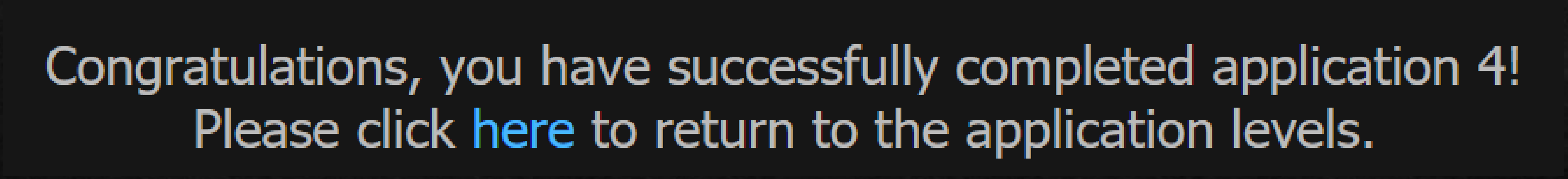
Application Challenge 4

Press the Button. (easy)

app4win.zip

Enter password:

•••••••



Congratulations, you have successfully completed application 4!
Please click here to return to the application levels.