تأليف : **JAAS**
Jaas1001@hotmail.com

الموقع : **الفريق العربي للبرمجة**
http://www.arabteam2000.com

ملف غـير مــوجود ؟!!

السلام عليكم ورحمة الله

الملف المرفق مع الدرس يوجد بة خطأ أو بمعنى آخر نقص وسبب الخطأ هو عدم وجود المكتبة Mylib0va.dll
لأن البرنامج عندما يبدأ التنفيذ يقوم بالتحقق من وجود هذة المكتبة . إذا وجد الملف يستمر فـــي التنفيذ و إذا لم يجدة يظهر رسالة الخطأ وينهي البرنامج.

و الذي نريدة الآن من البرنامج أن لا يقوم بالتحقق من وجود هذة المكتبة وينسى أمرها..ويستمر في التنفيذ

بسم الله نبدأ :

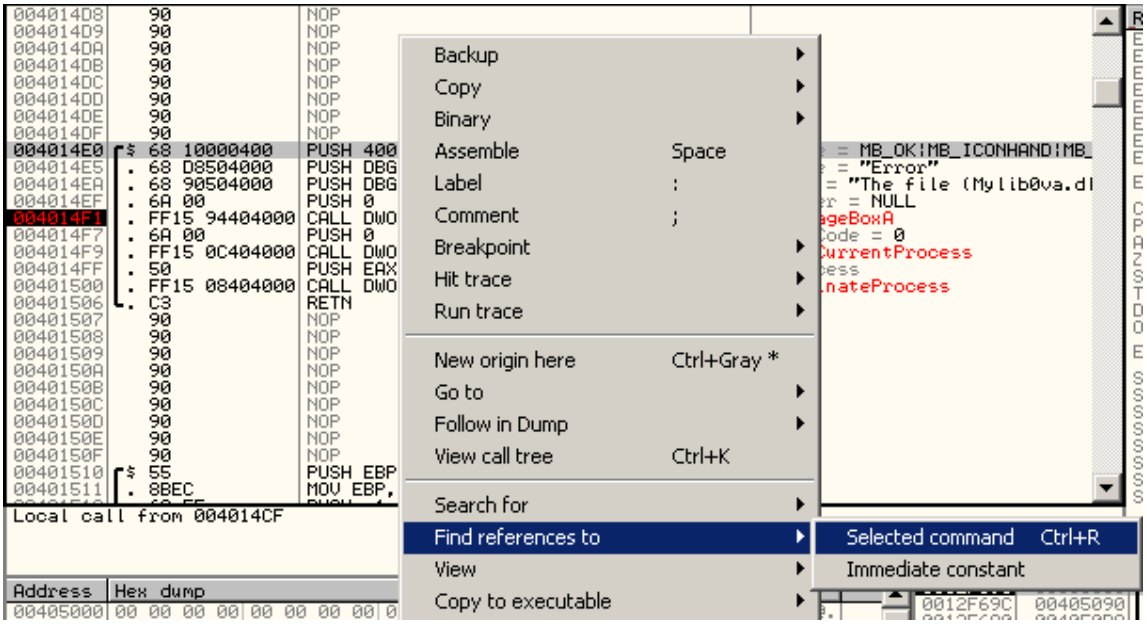
شغل Olly ثم File ثم Open وإختر الملف المرفق ثم من نافذة CPU إضغط Ctrl+N لتعرض دوال البرنامج (أضف نقطة توقف عند دالة المسج MessageBox)

وبعد ذلك شغل البرنامج – و لاحظ أين يتوقف

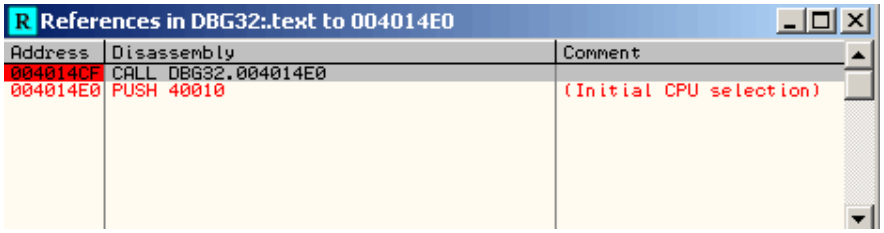
```
004014D8    90              NOP
004014D9    90              NOP
004014DA    90              NOP
004014DB    90              NOP
004014DC    90              NOP
004014DD    90              NOP
004014DE    90              NOP
004014DF    90              NOP
004014E0  $ 68 10000400     PUSH 40010                  Style = MB_OK|MB_ICONHAND|MB_
004014E5  . 68 D8504000     PUSH DBG32.004050D8         Title = "Error"
004014EA  . 68 90504000     PUSH DBG32.00405090         Text = "The file (Mylib0va.dl
004014EF  . 6A 00           PUSH 0                      hOwner = NULL
004014F1  . FF15 94404000   CALL DWORD PTR DS:[<&USER32.MessageBoxA  MessageBoxA
004014F7  . 6A 00           PUSH 0                      ExitCode = 0
004014F9  . FF15 0C404000   CALL DWORD PTR DS:[<&KERNEL32.GetCurren  GetCurrentProcess
004014FF  . 50              PUSH EAX                    hProcess
00401500  . FF15 08404000   CALL DWORD PTR DS:[<&KERNEL32.Terminate  TerminateProcess
00401506  . C3              RETN
00401507    90              NOP
00401508    90              NOP
00401509    90              NOP
0040150A    90              NOP
0040150B    90              NOP
0040150C    90              NOP
0040150D    90              NOP
0040150E    90              NOP
0040150F    90              NOP
00401510  $ 55              PUSH EBP
00401511  . 8BEC            MOV EBP,ESP
```

هل تجد أي أمر يمكن أن نغيرة لتجاوز هذا المسج ودالة الإنهاء(أكيد لا)
إذا سنقوم بالبحث عن التعليمة التي أوصلتنا إلى هذة الورطة ؟!
إذهب إلى بداية الدالة (دائما بداية الدالة تأتي قبلها هذة التعليمات .. NOP - RETN –JMP)

إضغط على تعليمة بداية الدالة و إختر بحث عن الإتصالات بهذة الدالة – كما يلي

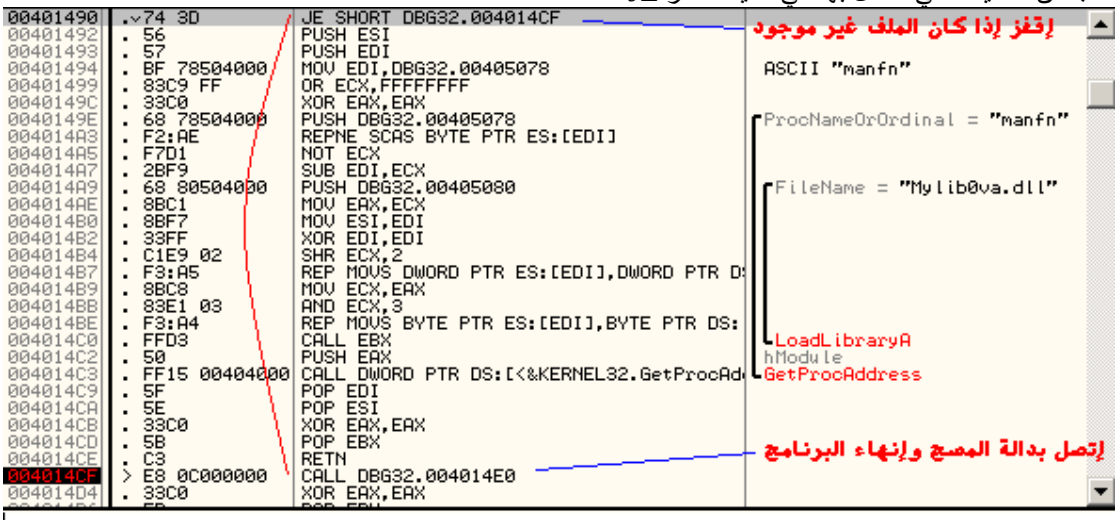


ستظهر لك مجموعة من التعليمات التي تقوم بتنفيذ هذة الدالة وفي مثالنا تعليمة واحدة



أضف لها نقطة توقف عن طريق مفتاح F2 ثم أعد تشغيل البرنامج >>
ثم شغل البرنامج F9 سيتم إقاف البرنامج عند تعليمة Call وهي تعليمة للإتصال بدالة المسح

لو بحثت عن الإتصالات لهذة الدالة (لأن التعليمة التي قبلها RETN أي بداية دالة)
جرب: إختر تعليمة Call ثم إبحث عن مصدر التعليمة عن طريق Find references to أو Ctrl+R
ستجد أن التعليمة التي تتصل بها هي تعليمة القفز JE

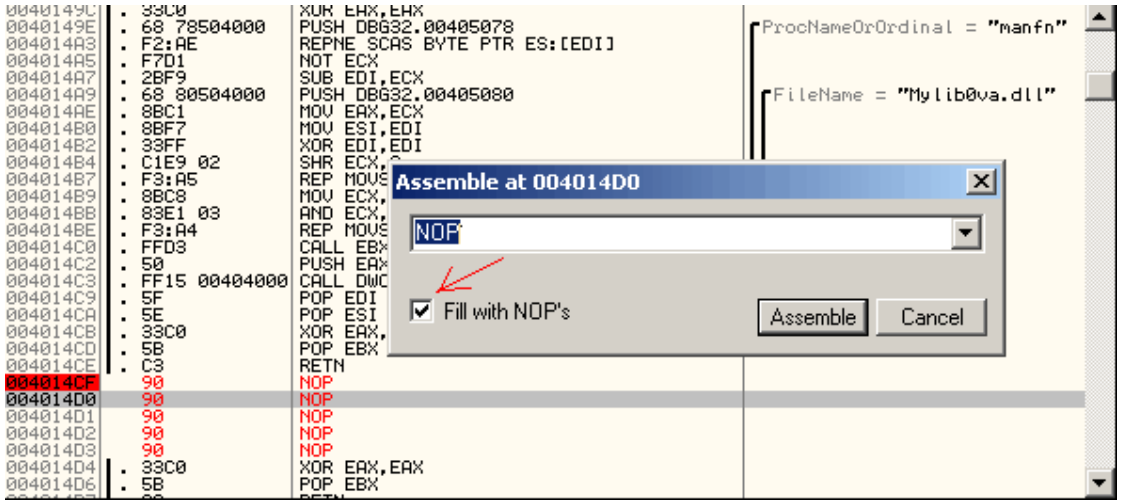


قد تعتقد أننا وجدنا الحل بتغيير القفزة (حاول تغيير القفزة لتجد الكارثة ؟؟)
إذا غيرت القفزة ستخبر البرنامج أن المكتبة موجودة - وبهذا سيقوم البرنامج بتنفيذ دالة داخل المكتبة
عن طريق نظام التشغيل طبعا – ولن يجد نظام التشغيل المكتبة وبهذا تقع في مشكلة أكبر
وسيصبح من خطأ مستخدم إلى خطأ نظام وفي هذا الحال بدل من كحلها عميناها – و الحل ؟

لهذة المشكلة توجد حلول كثيرة (لأن الإسمبلي ليس فقط قفزات)
الأول : حذف الإتصال بدالة المسج و إنهاء البرنامج عن طريق تعلمية NOP
الثاني : تغيير عنوان القفز ونحدد لة عنوان بعد تعليمة الإتصال

حذف التعليمات من البرامج التنفيذية عن طريق تعليمة واحدة وهي NOP ومعناها لا شيء
وحجمها بايت واحد

أضف نقطة توقف على تعليمة القفز Je ثم أعد تشغيل البرنامج وقم بتنفيذة F9
بعد أن يقف عند تعليمة القفز إذاهب لدالة الإتصال بالمسج (عن طريق مفتاح Enter)
ثم علم على تعليمة الإتصال وإضغط الزر الأيمن للماوس وإختر الأمر Assemble
وغير تعليمة Call بتعليمة NOP أوبمعنى آخر بسلسلة تعليمات NOP



ثم شغل البرنامج F9 وسترى أن البرنامج يعمل بشكل طبيعي !

والطريقة الثانية : تغيير العنوان

00401490 JE SHORT DBG32.004014CF

ستتحول إلى

00401490 JE SHORT DBG32.004014D4

وبهذا نكون قد تجاوزنا دالة الإتصال Call

نهاية المثال

في الحقيقة حصلت على فكرة هذا المثال من برنامج مشهور للفلاش . وهو برنامج السوتش
عندما يبدأ هذا البرنامج فإنة يقوم بتحميل مكتبة خاصة بالتحقق من حماية البرنامج وبها أكواد معقدة
لفك هذة الحماية - ولكنهم نسوا أن حذف دوال تحميل المكتبة يلغي هذة الحماية ويصبح البرنامج مفتوح
إلى الأبد

هذا والله أعلم