تأليف : **JAAS**
Jaas1001@hotmail.com


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

# مراقبة برامج الفيجول بيسك

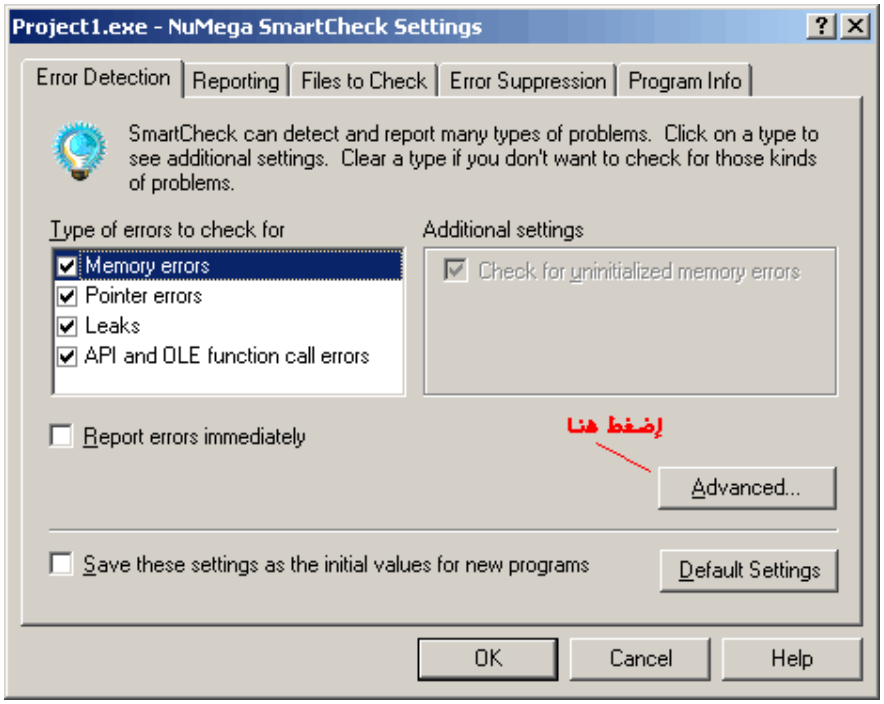
السلام عليكم ورحمة الله
برامج الفيجول بيسك هي برامج مبنية على الأحداث وعلى ملفات تشغيل وليست كغيرها من البرامج
تتصل مباشرة بدوال API
وسيتم في هذا الدرس مراقبتها والتغيير فيها بواسطة برنامجين

الأول لمراقبة أحداث البرنامج : وسنستخدم برنامج SmartCheck
الثاني مراقبة البرنامج عن طريق الإسمبلي : وسنستخدم برنامج Olly

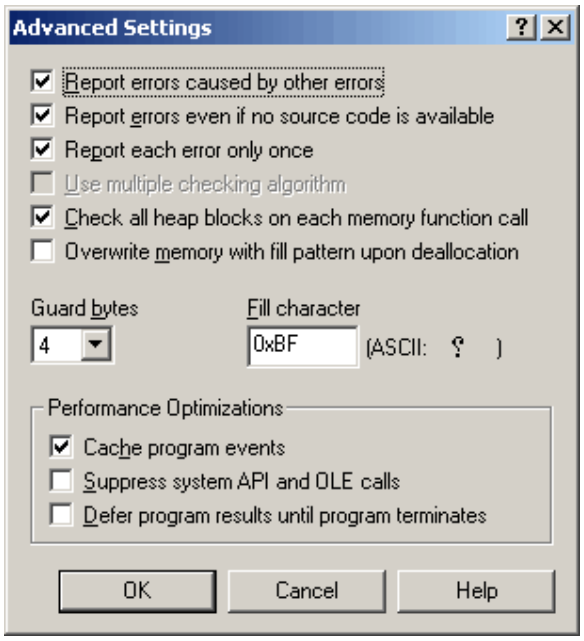
تجد في الملف المرفق برنامج مكتوب بالفيجول بيسك – وهو يطلب تحقيق شرط للإستمرار
شغل برنامج SmartCheck ومن File ثم Open وإختر الملف

في شيء مهم هنا برنامج SmartCheck يترك لك تحديد ماتريد مراقبتة في البرنامج مثل أحداث دوال .. وفي هذا الموضوع سنستخدم مراقبة الأحداث ( يجب أن نقوم بإعداد البرنامج لهذا الغرض )

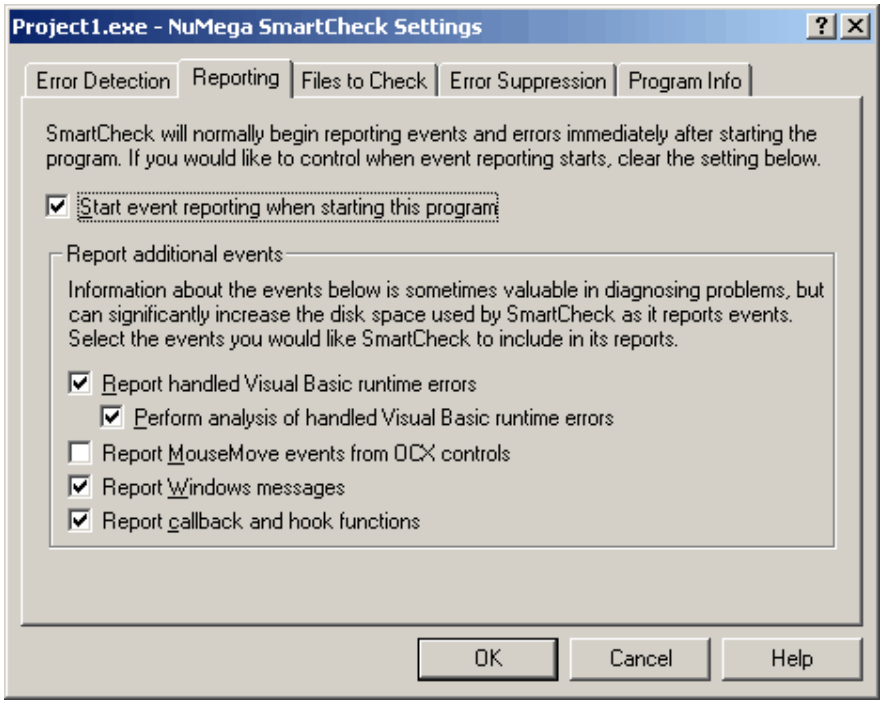
من قائمة Program ثم
Settings إتبع هذة الخطوات المبينة في الصور
تأكد من الخيارات وطبقها كما هي


Project1.exe - NuMega SmartCheck Settings
Error Detection
Reporting
Files to Check
Error Suppression
Program Info
SmartCheck can detect and report many types of problems. Click on a type to see additional settings. Clear a type if you don't want to check for those kinds of problems.
Type of errors to check for
Memory errors
Pointer errors
Leaks
API and OLE function call errors
Additional settings
Check for uninitialized memory errors
إضغط هنا
Report errors immediately
Advanced...
Save these settings as the initial values for new programs
Default Settings
OK
Cancel
Help

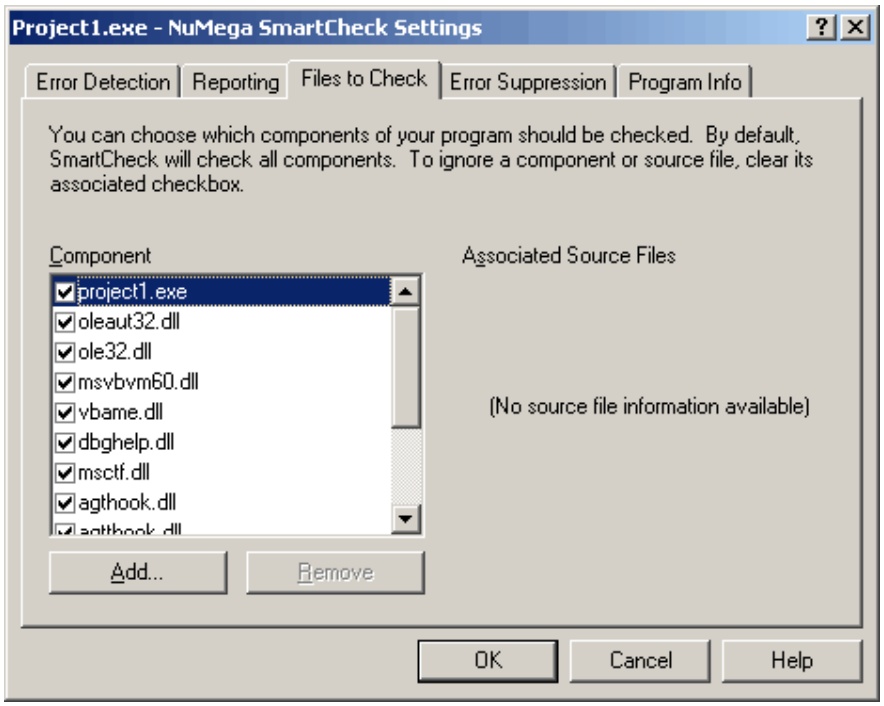
ثم


Advanced Settings
Report errors caused by other errors
Report errors even if no source code is available
Report each error only once
Use multiple checking algorithm
Check all heap blocks on each memory function call
Overwrite memory with fill pattern upon deallocation
Guard bytes
4
Fill character
0xBF
(ASCII: ? )
Performance Optimizations
Cache program events
Suppress system API and OLE calls
Defer program results until program terminates
OK
Cancel
Help

ثم



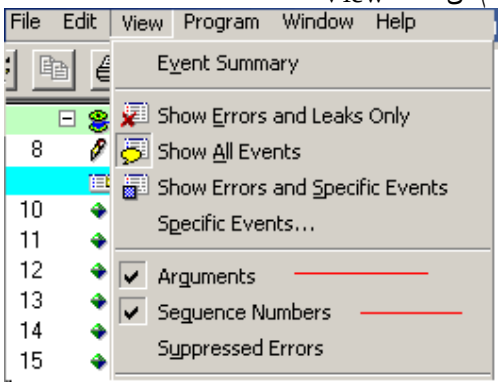

ثم




وبقية الخيارات إتركها كما هي

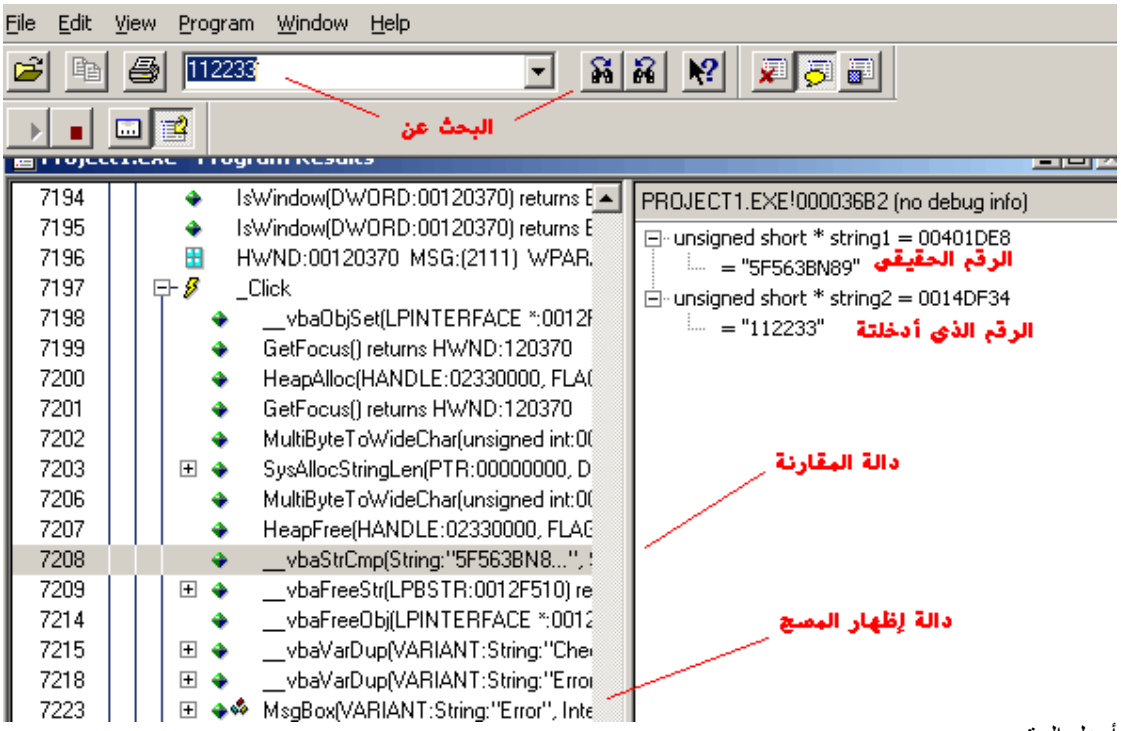
بعد ذلك تأكد من أنك إخترت ( إظهار أحداث البرنامج )

ثم من قائمة View




والآن شغل البرنامج وإكتب في مربع النص مثلا ١١٢٢٣٣ وإضغط على زر التحقق Check

وبكل بساطة إبحث عن الرقم الذي أدخلتة :

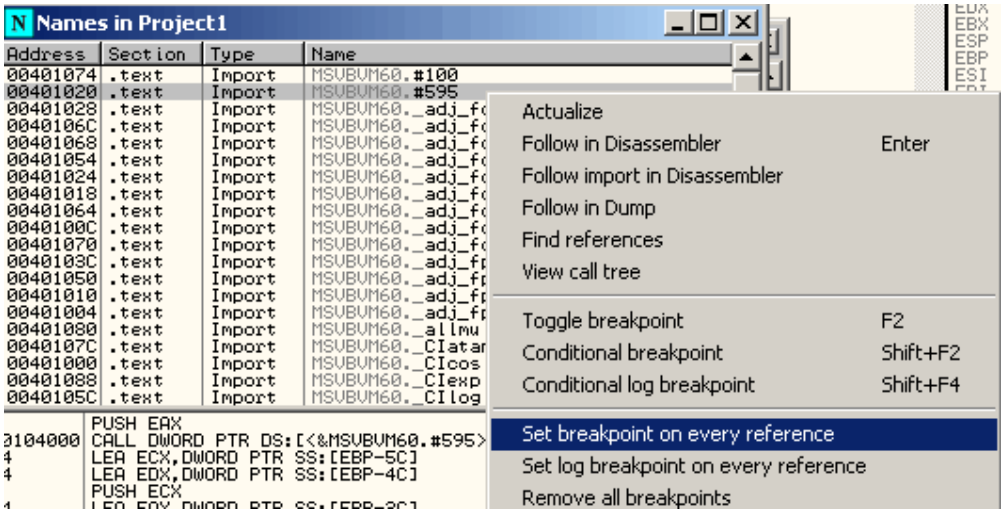



أدخل الرقم وجرب

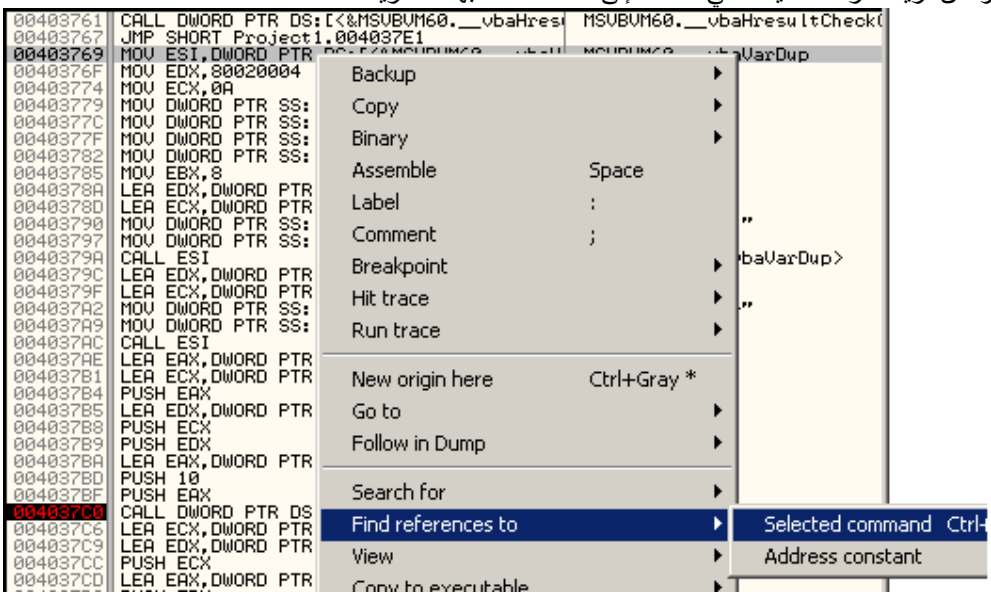
---

ولكن قد تريد تجاوز الشرط عن طريق الإسمبلي – يعني بالقوة **L**

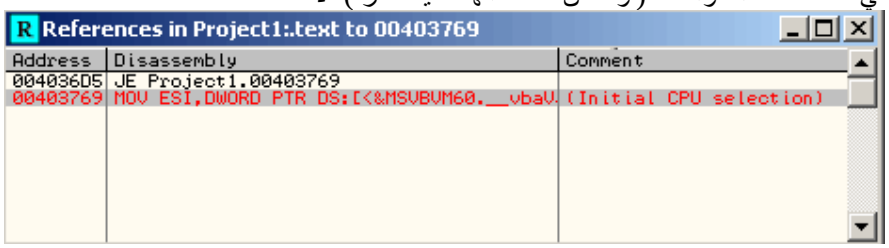
أوكي : أغلق SmartCheck ثم شغل Olly وإختر البرنامج
وفي نافذة CPU إضغط Ctrl+N لتظهر لك الدوال المستوردة
ولكن لن تجد دالة إظهار المسج MessageBox لأن برامج الفيجول بيسك تستخدم ملفات تشغيل وفي هذة الملفات نجد أن دالة المسج هي ٥٩٥ أو rtcMsgBox
ضع نقطة توقف على دالة المسج




ثم نفذ البرنامج F9 وأدخل أي رقم ثم إضغط على زر التحقق لتقف عند دالة المسج
هل تلاحظ أي تعليمة فوق تعليمة المسج يمكن أن تغير مسار التنفيذ ( أكيد لا )
بمعنى أننا داخل دالة إتصلت بها تعليمة أخرى
كما قلنا في الموضوع السابق يمكن أن يبدأ عنوان الدالة بعد هذة الأوامر
JMP - RETN - NOP
والآن نريد معرفة التعليمة التي أدخلتنا إلى هذة الدالة - بهذة الطريقة



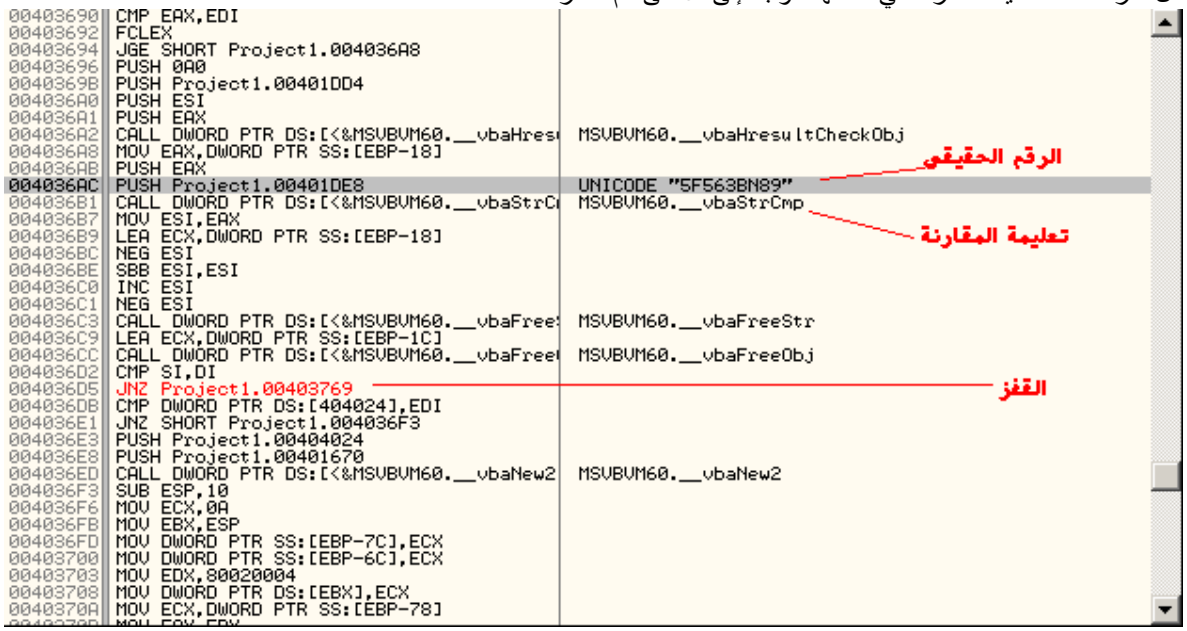

ستظهر لك نافذة بها قائمة التعليمات التي تتصل بهذة الدالة
في مثالنا فقط دالة واحدة ( ولحسن حظك أنها تعليمة قفز ) لاحظ




إختر تعليمة القفز وإضغط Enter لينقلك البرنامج إلى عنوان التعليمة

وبقي عليك تغييرها إلى JNE وبهذا تكون قد تجاوزت الشرط

وفي شغلة تجمع بين Olly و SmartCheck
هل مازلت عند تعليمة القفز التي عدلتها توجه إلى الأعلى كم سطر




---

**نهاية المثال**

هذا والله أعلم