Arctic Shell 精选文章 | 2019-01

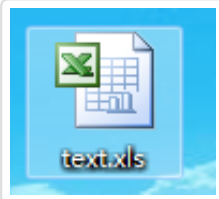
Xls Macro 4.0 利用演示

返回首页

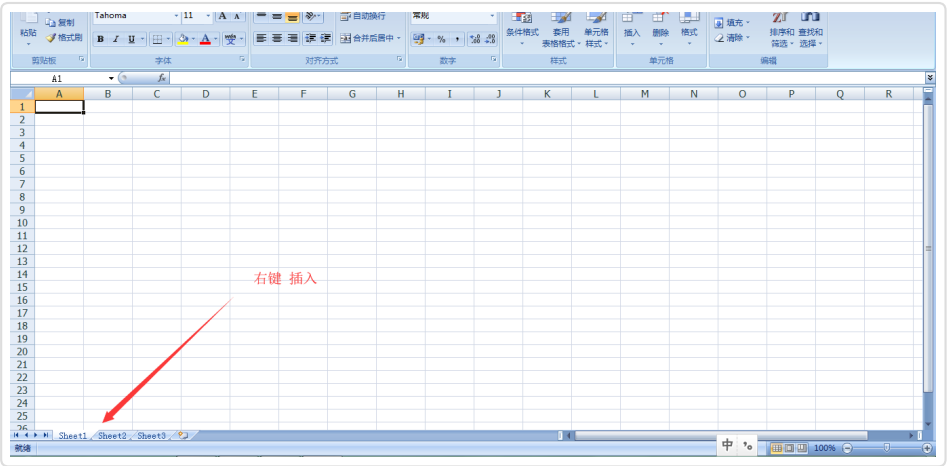
作者：crazyman_army | 版权：作者已授权 | 本文编辑：天析 | 文章状态：有删减

[0x1]:制作POC

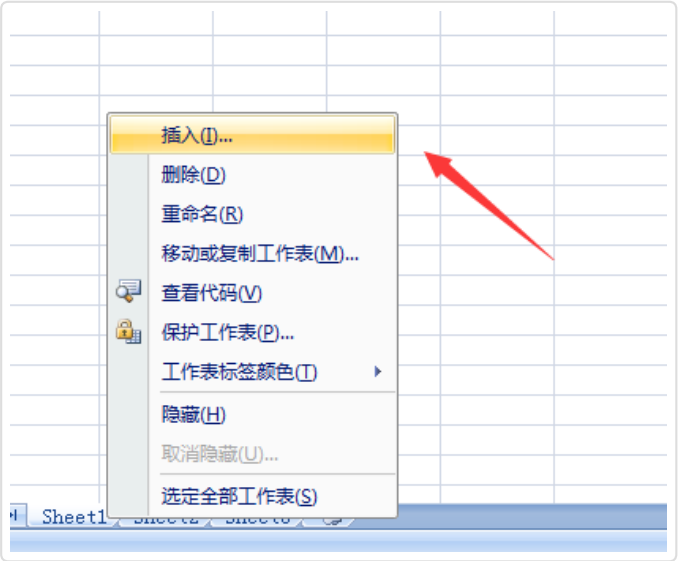
创建一个xls文件



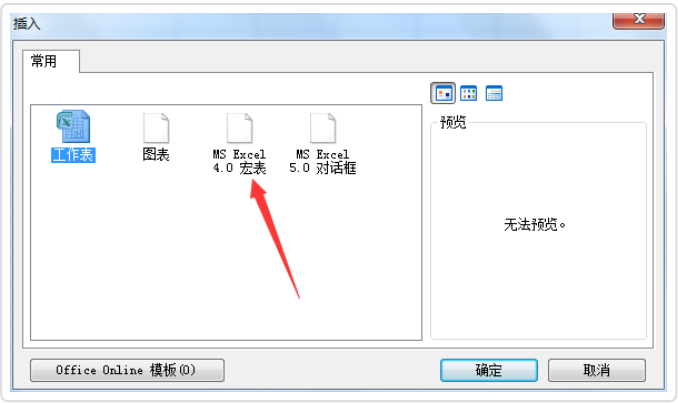
在底下的工作表标签栏上面



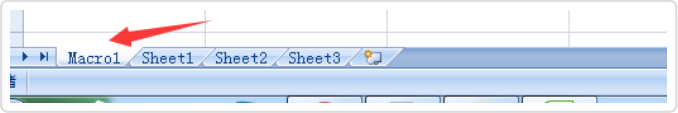
右键->插入



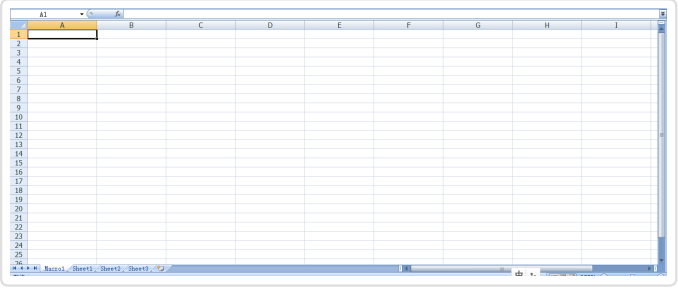
选中MS Excel 4,0宏表，然后点击确定



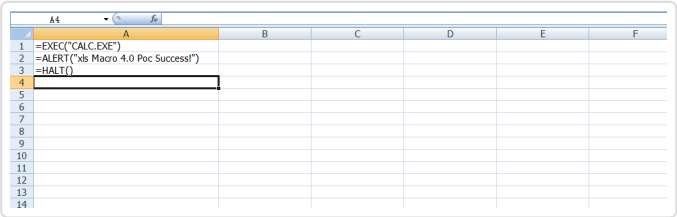
如图所示 ,多出一个叫Macro的栏



如下，看起来和一般的没什么两样,但是此时已经支持了Execl 4.0 Macro的语法

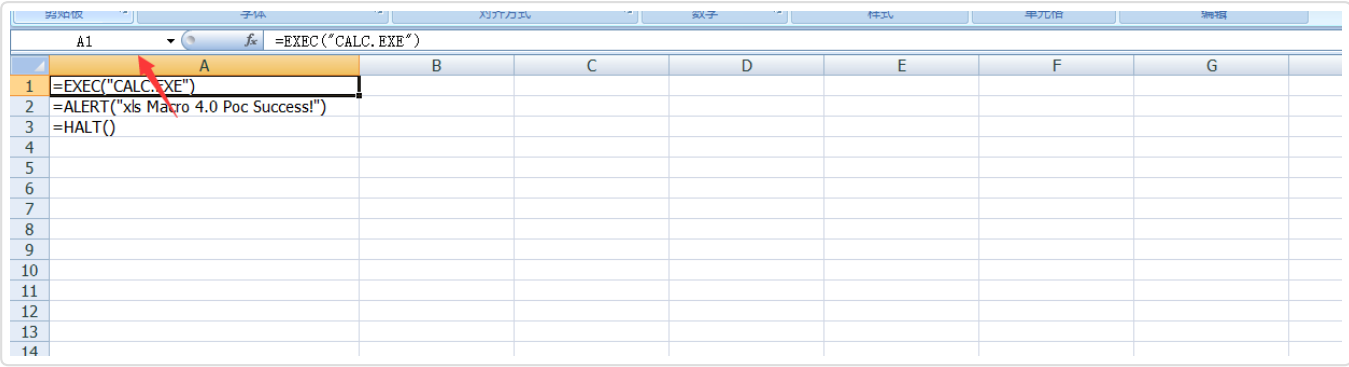


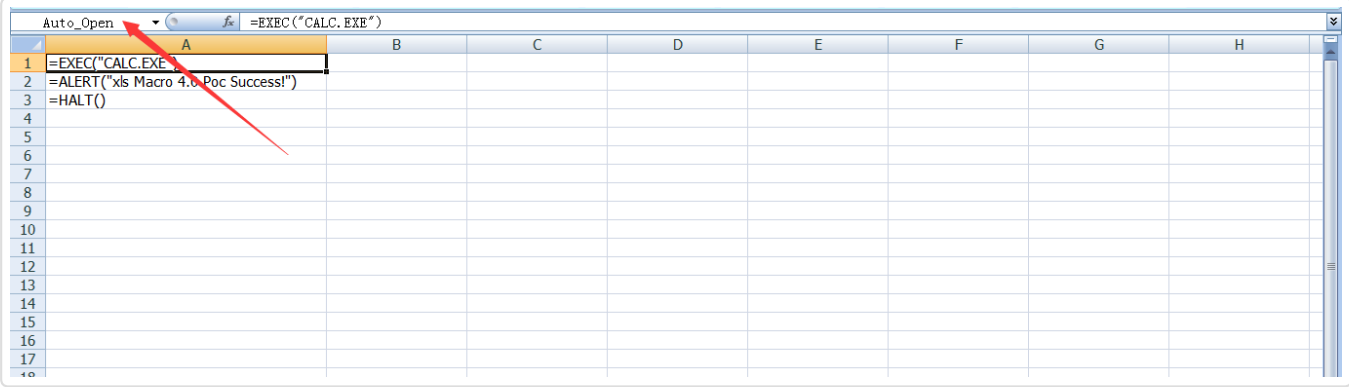
如下我们就构造了一个关于这个的Poc



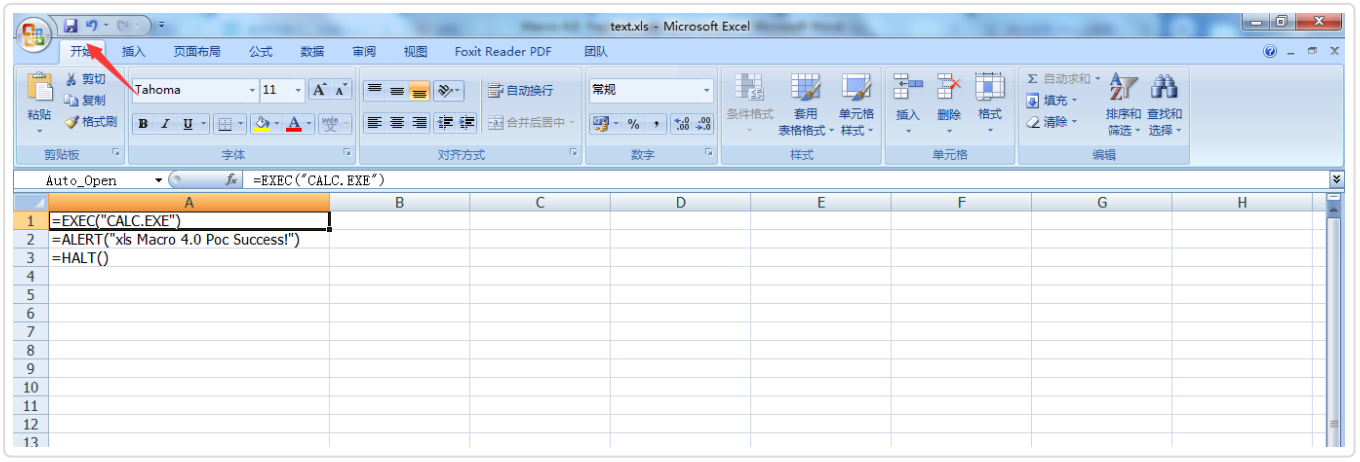
公式内容：=EXEC(“calc.exe”)	功能：内部调用WinExec函数打开计算器
公式内容：=ALERT(“xls Macro 4.0 Poc Success!”)	功能：内部调用MessageBox函数打开对话框
公式内容：=HALT()	功能：标识Excel 4.0宏结束，类似C语言return指令

将A1的名称框选中,将A1名称改为Auto_Open这样就可以达到打开文档启动(以=EXEC(“calc.exe”)这条语句开始逐句执行)的目的

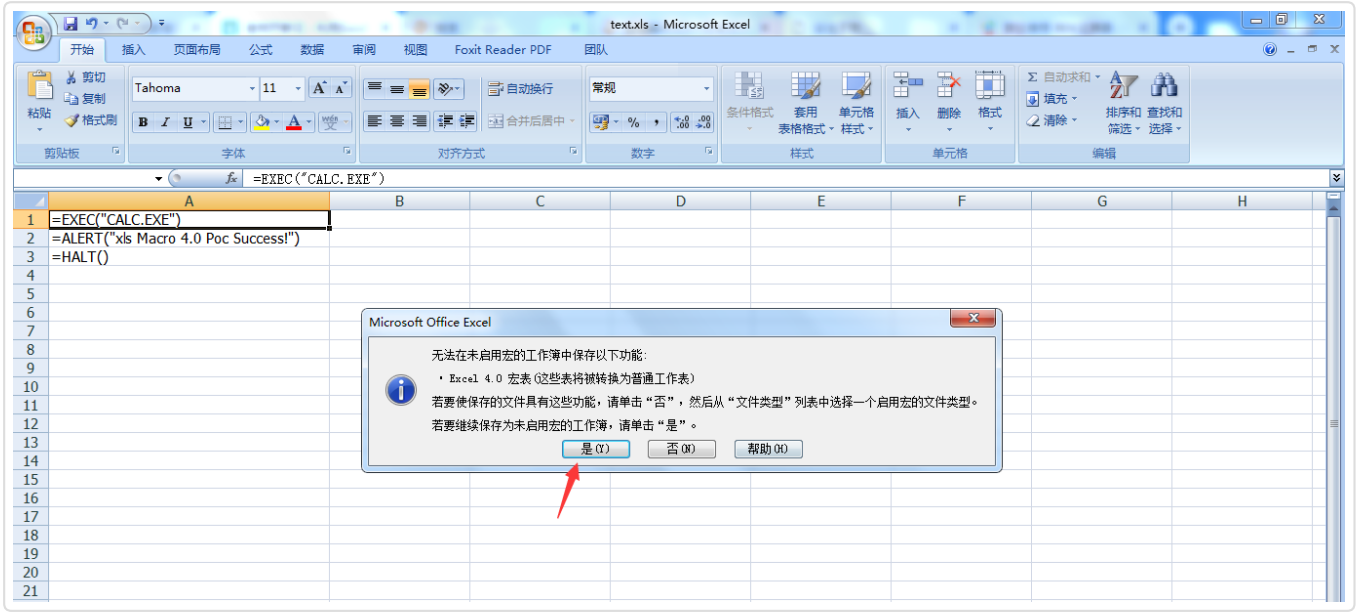




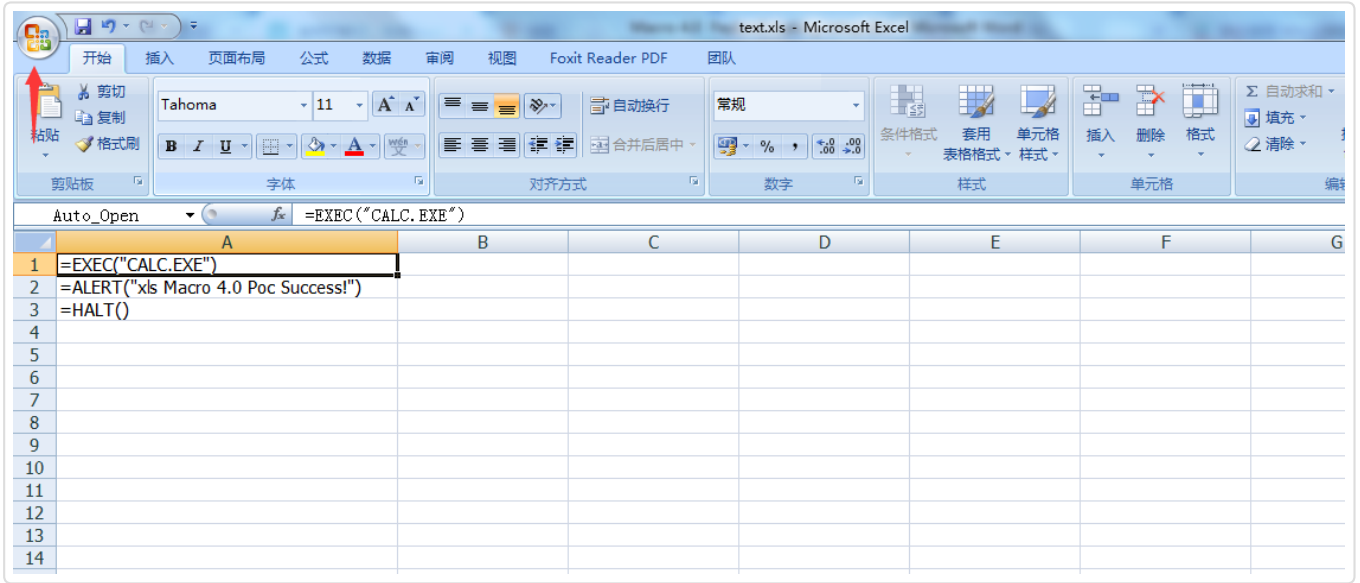
将其保存起来



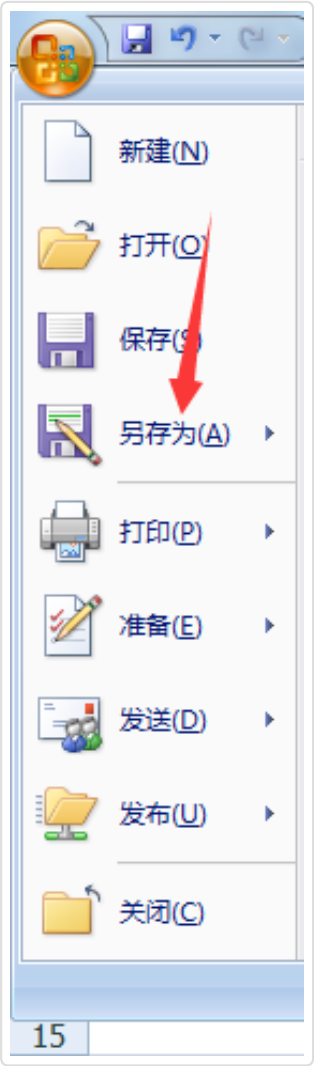
点击是(Y)



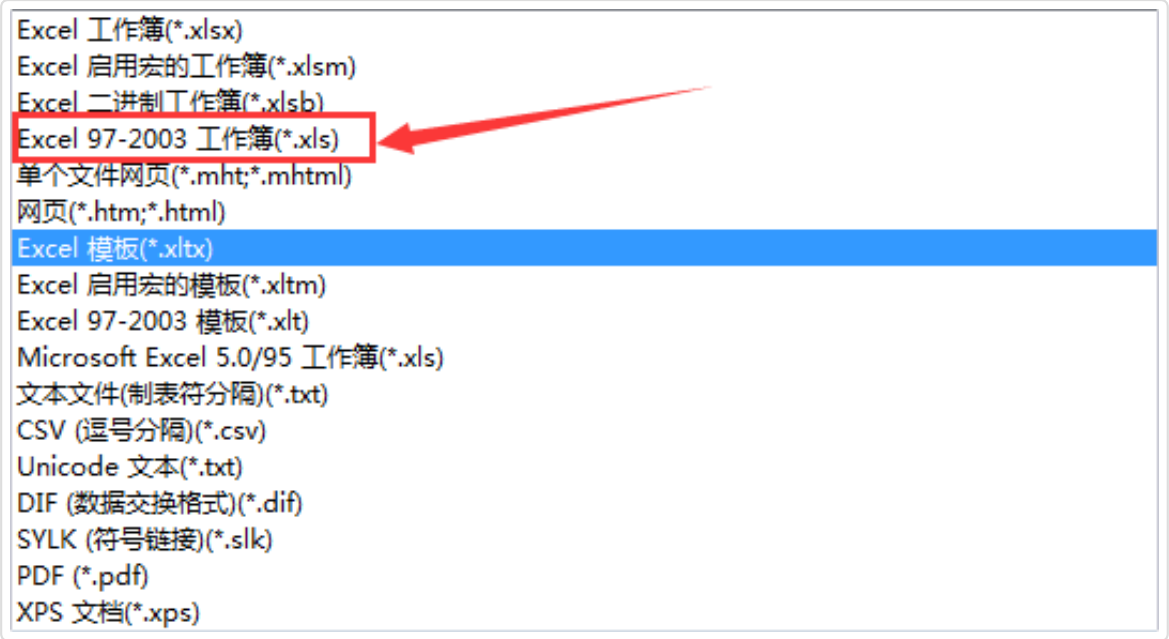
如果你用xlsx文件构造的此poc你还需要点击office的图标按钮



点击另存为

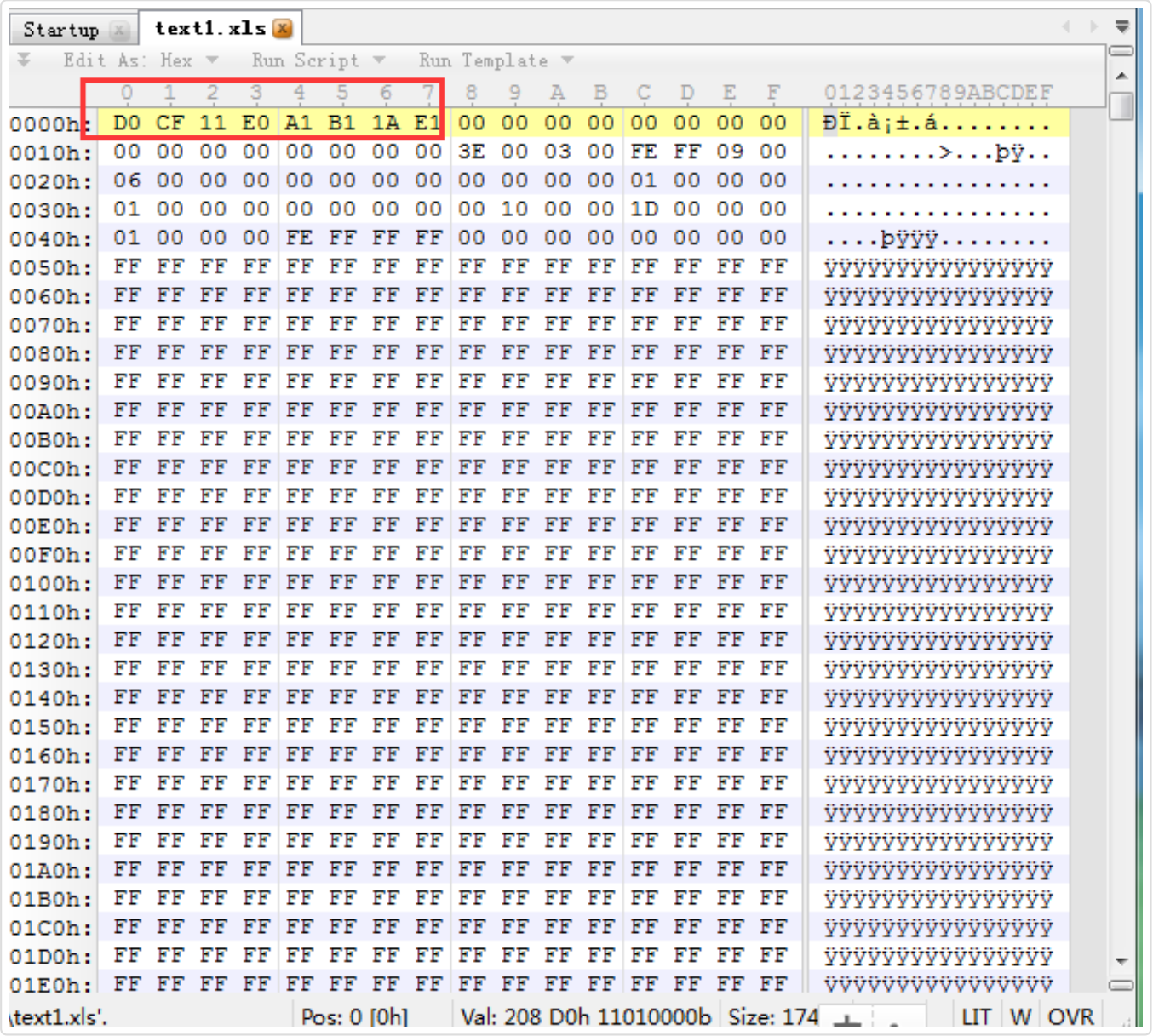


选中Excel 97-2003工作薄(*.xls)

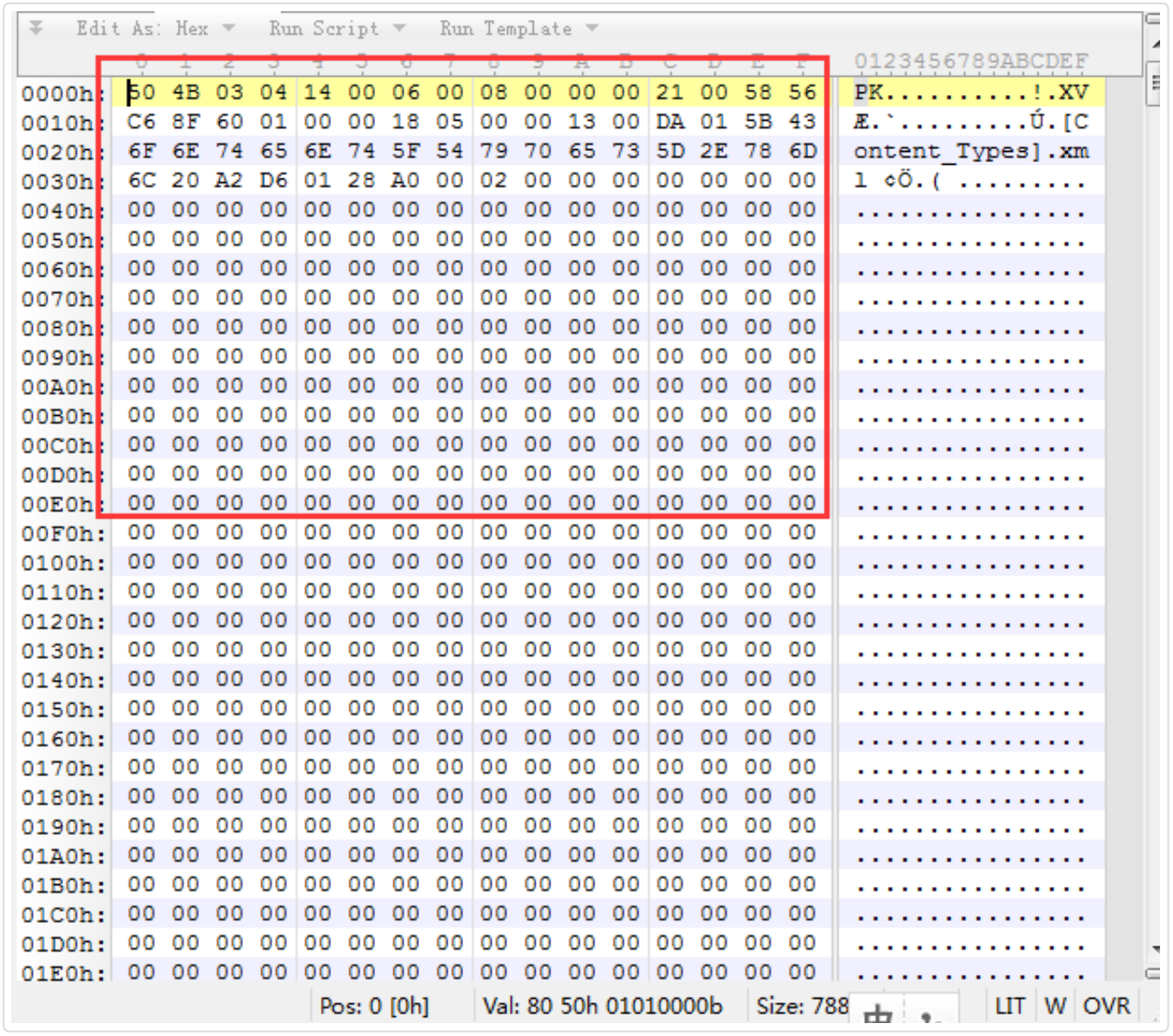


由于微软为了对抗宏所以在97-2003版的ole格式文件被他们修改后就变为了现在的文档格式,现在的文档格式不支持宏的启用

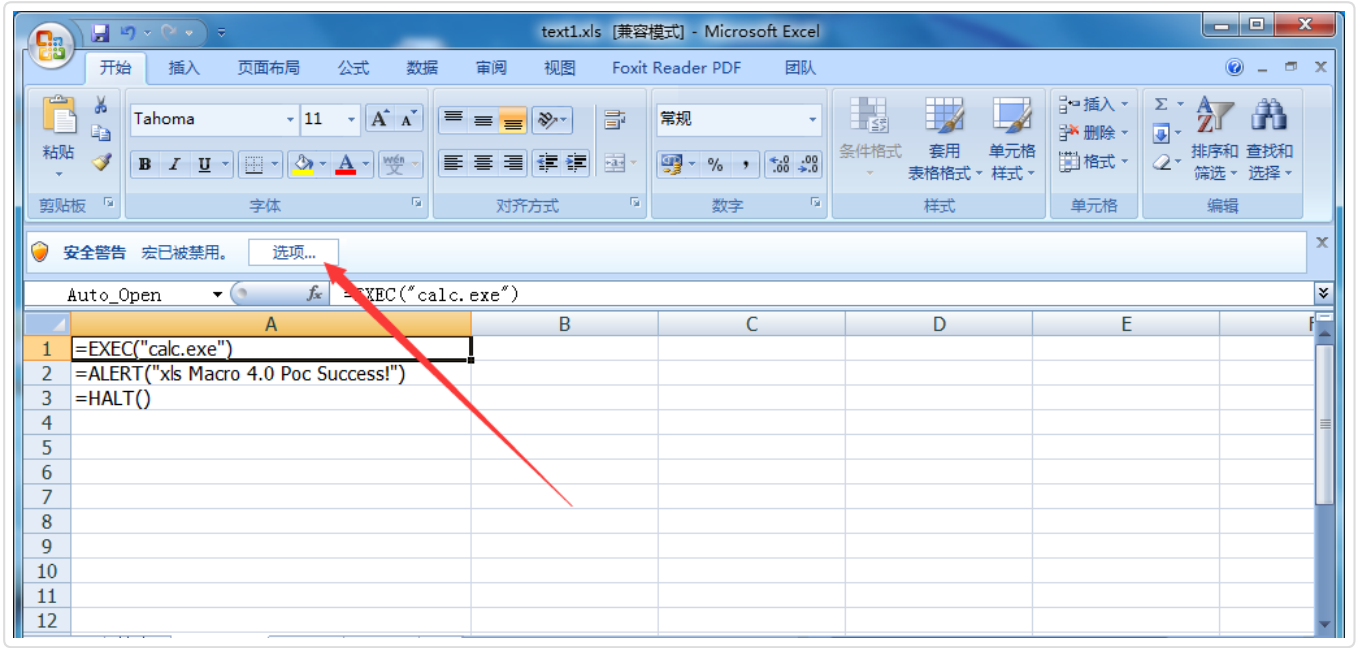
97-2003文档的格式结构:



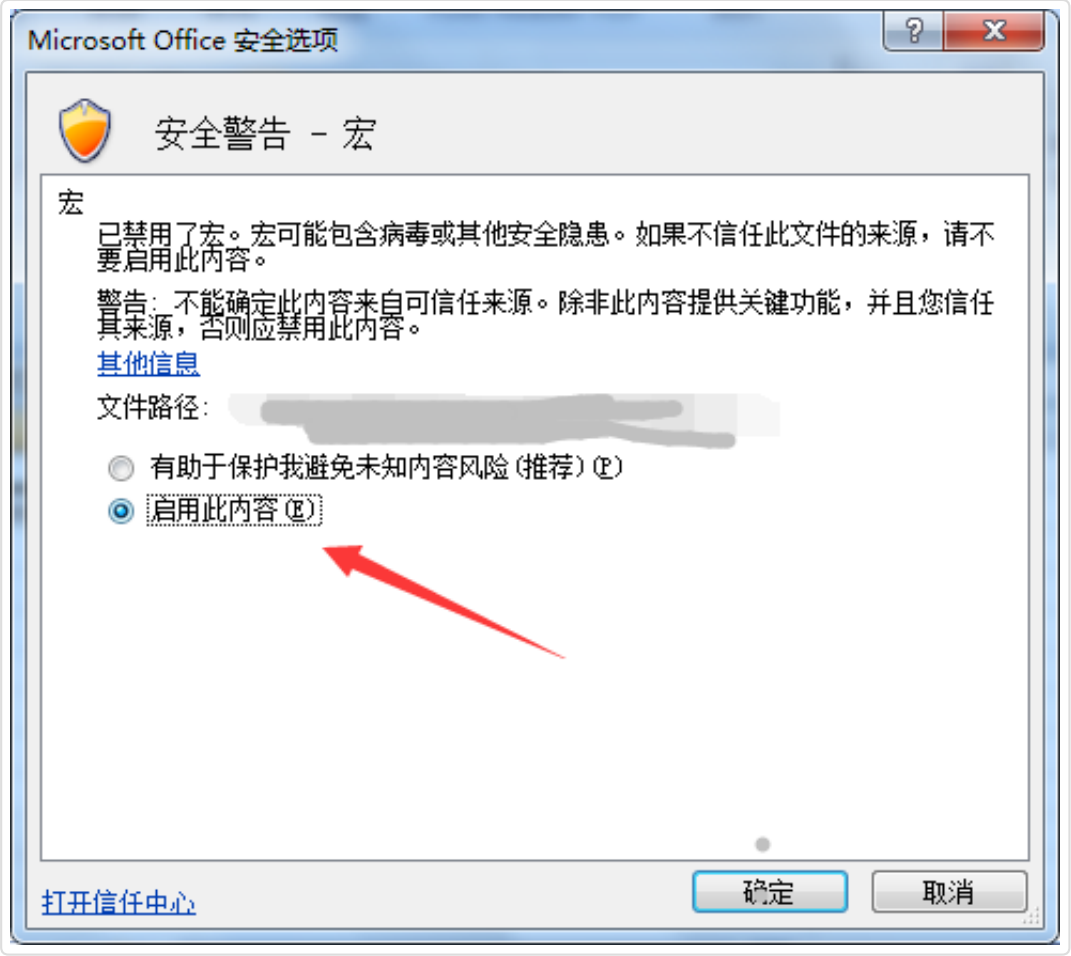
现在的文档文件结构(笔者用的2007):



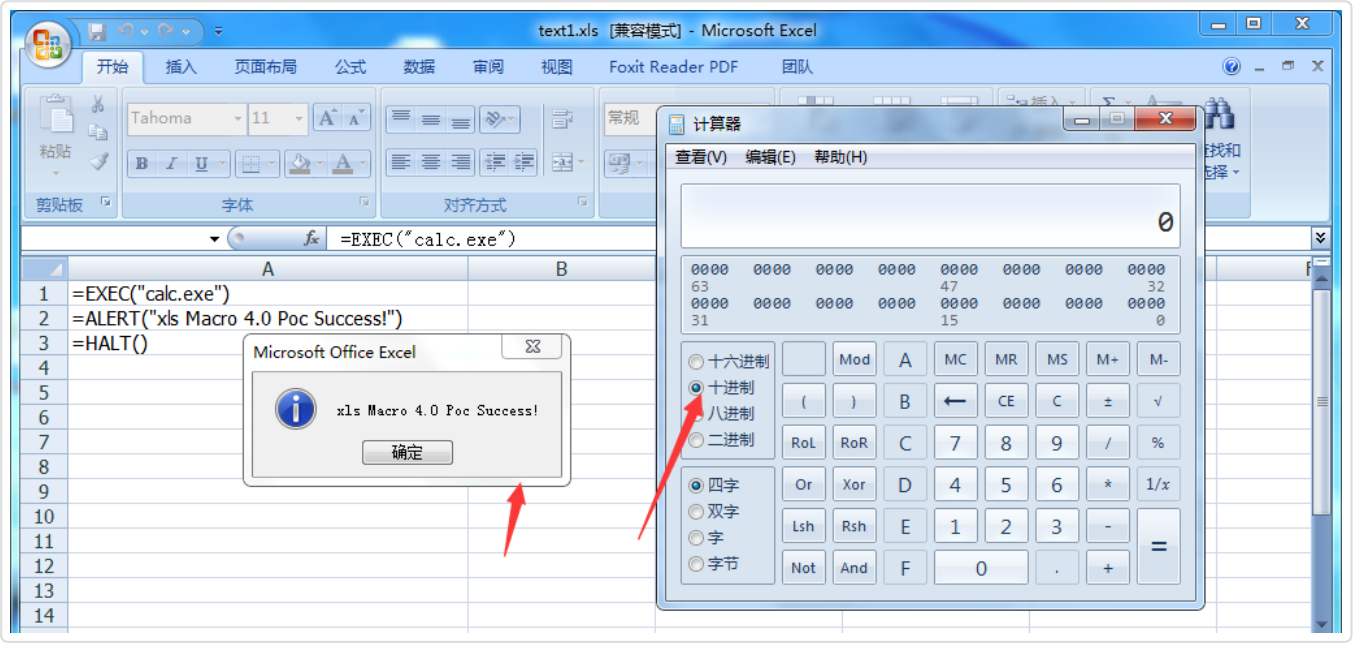
下面我们来测试一下这个POC打开刚刚我们构造的文件



点击选项 启用未知内容 确定



效果如下:



弹出了相应的弹窗以及计算器证明poc成功!


北極邊界