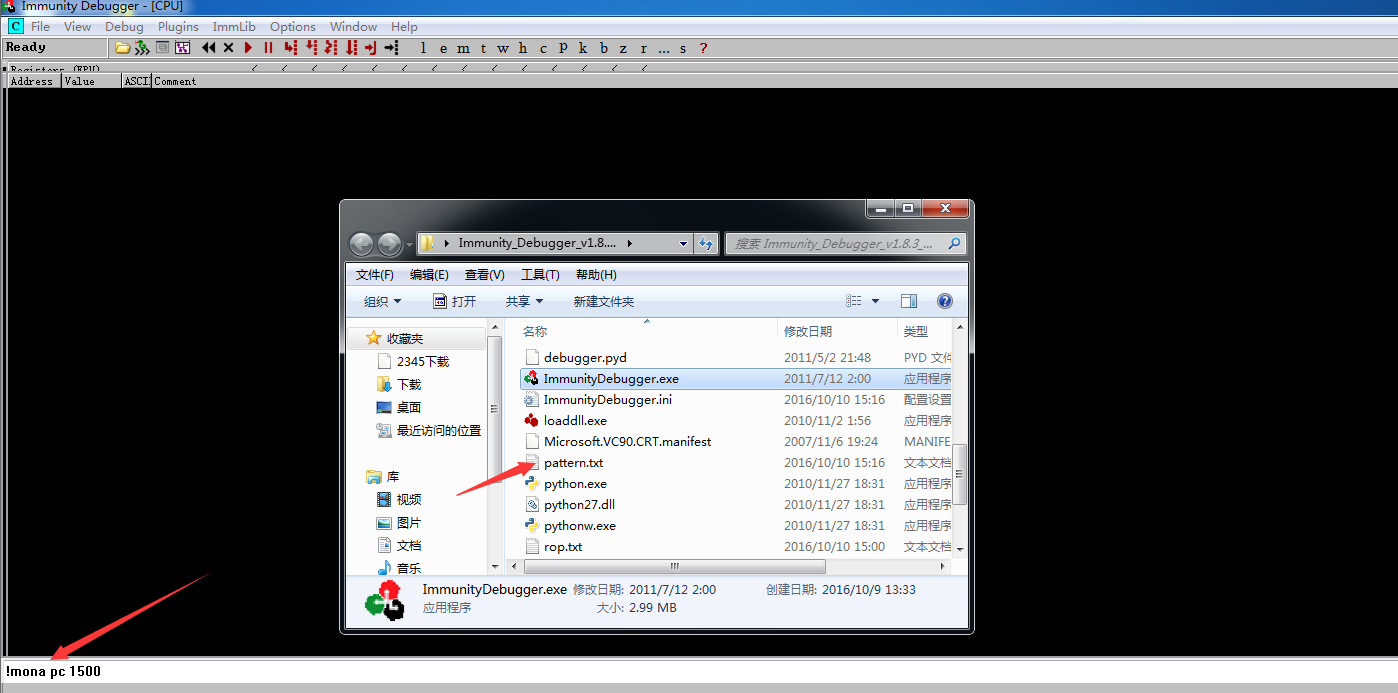
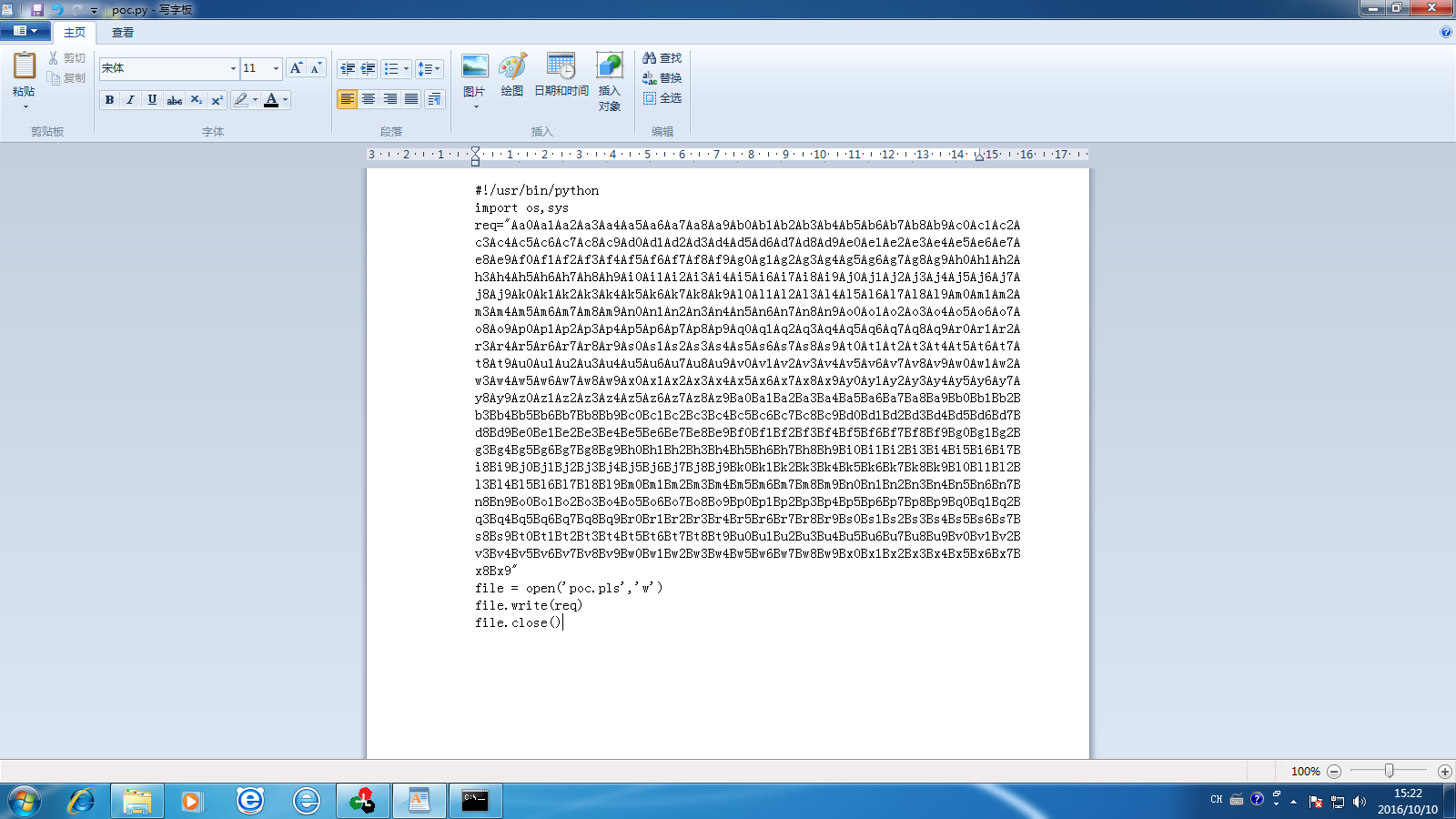
**VUPlayer 2.49 - '.pls' Stack Buffer Overflow (DEP Bypass)**

本漏洞是栈溢出漏洞，具体分析我没分析，只是自己尝试着学习一下rop绕过dep保护机制。

由于这是一个栈溢出漏洞。我们只要劫持eip就能够执行任意代码，漏洞利用还是immunity debugger方便一点，首先利用mona脚本生成pattern.txt

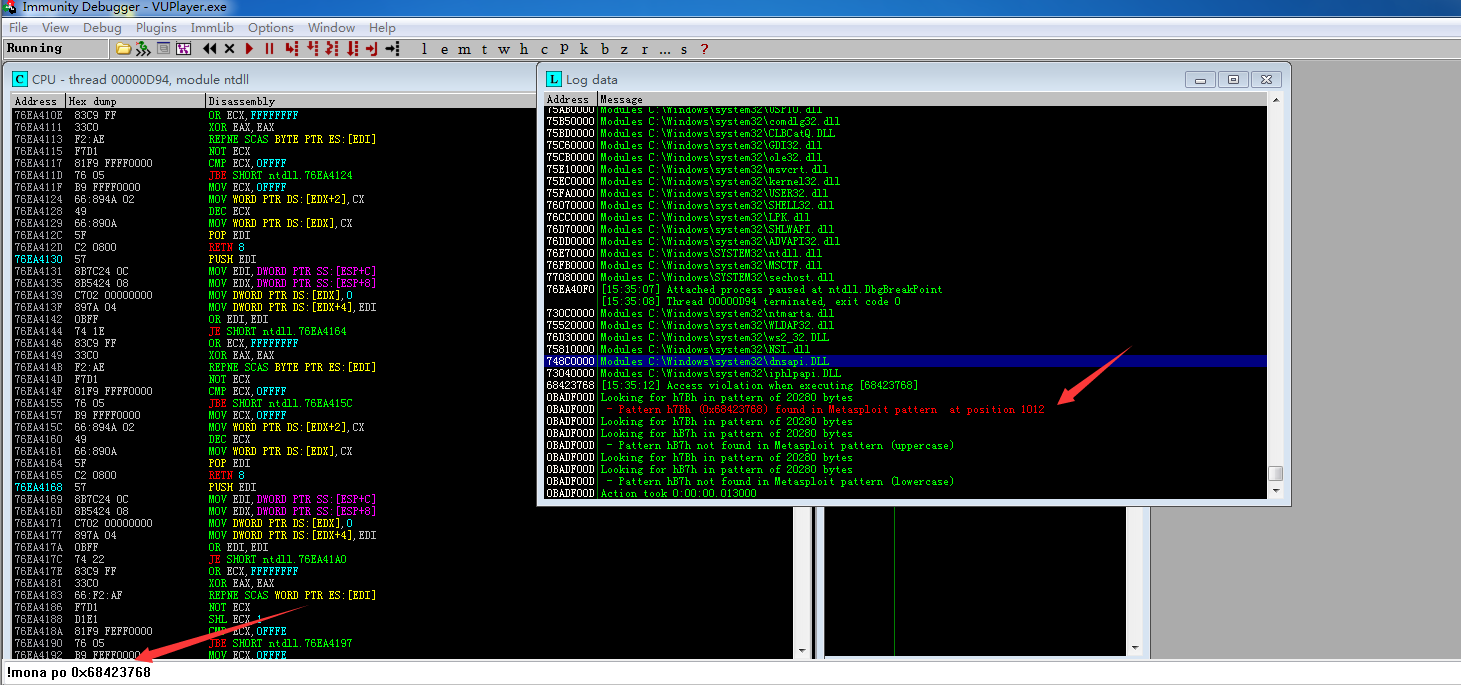


然后将里面的字符串复制到poc里面

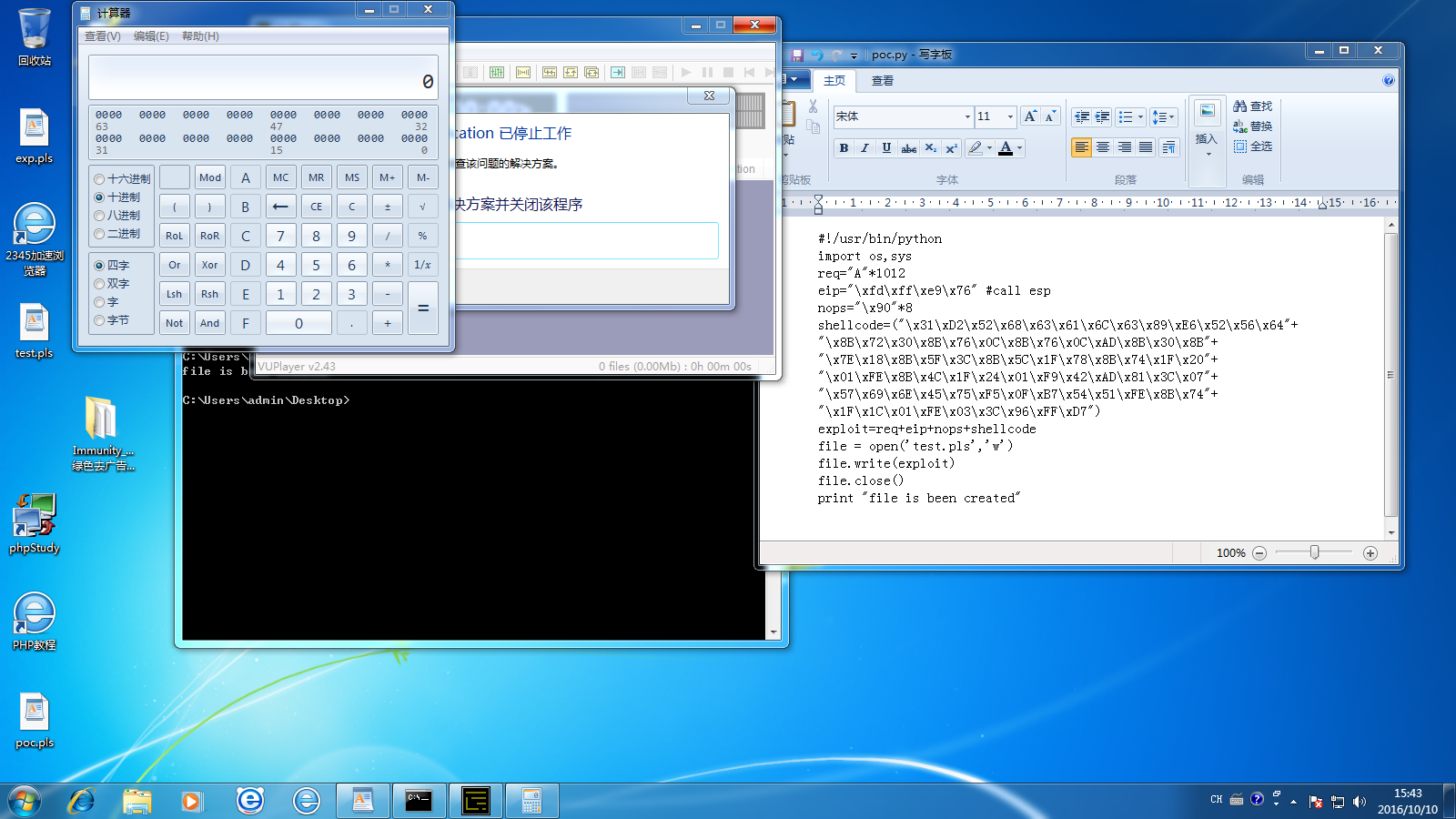


接着运行python脚本会在当前路径生成poc.pls,然后我们打开我们的调试工具

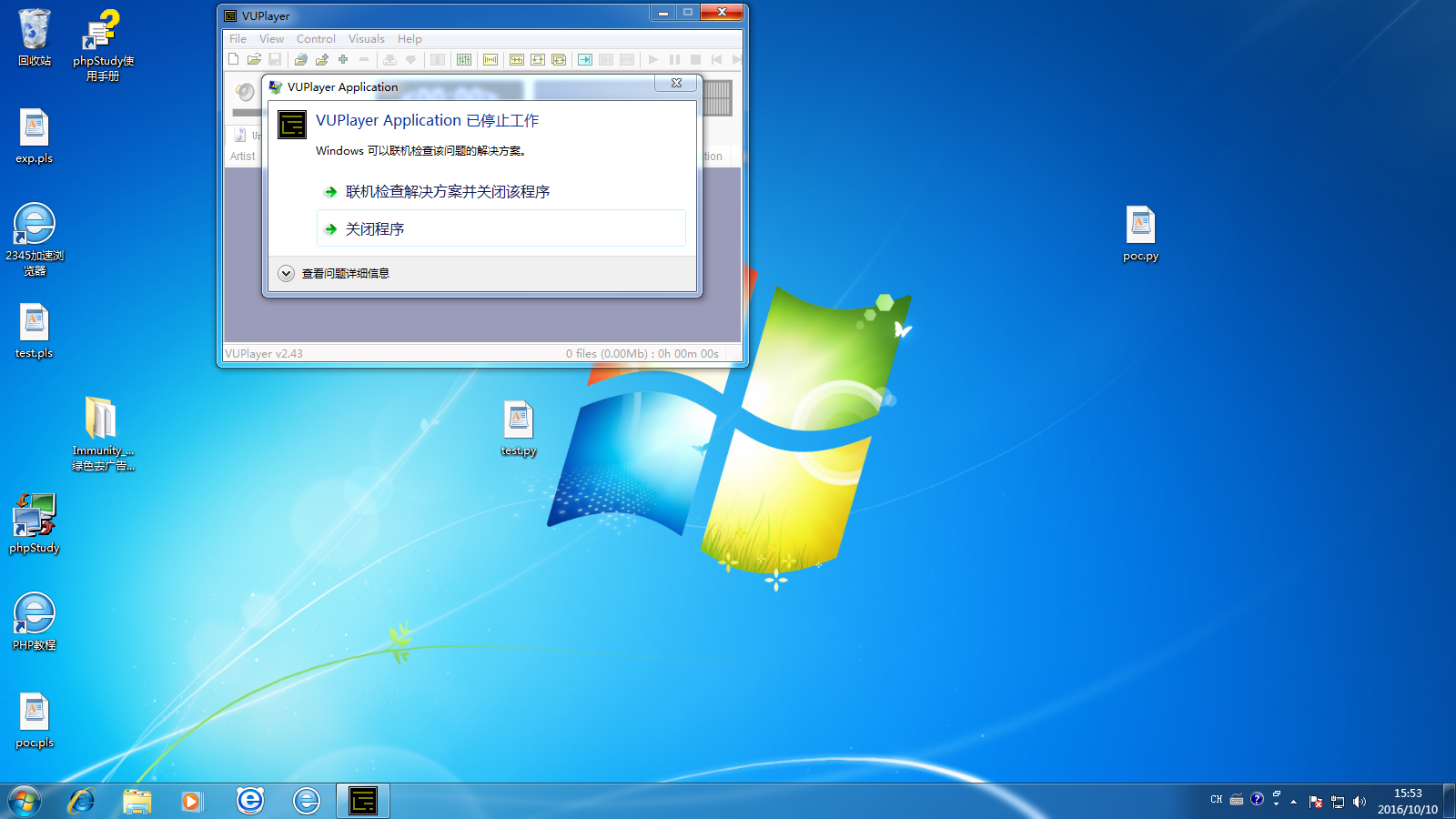
附加到vuplayer进程上去，按f9运行后，把poc.pls拖到vuplayer里面去，然后产生异常，然后距离eip相差1012字节



接下来就可以构造exp了



然后我们开启dep试试，无法成功弹出calc



然后我们利用mona插件构造rop chain，接着跳出calc，不过aslr有点蛋疼，rop只是个半成品，没有绕过aslr，rop并不是很懂，重启后exp就没用了。

