Write Flash Poc

1. 参考文章：<http://blogs.360.cn/post/indepth_CVE-2018-5002.html>

https://www.freebuf.com/vuls/174206.html

1. 题目说明：

该题是一道漏洞分析题（非re ，非pwn类型），贴近实际情况，建议大家详细阅读参考文章。**允许多种解法 ~ ~**

题目链接里提供了一个Demo.swf， IE flash 29.0.0.171 的安装包。只要Flash版本比29.0.0.171还低，可以不使用提供的flash安装包。

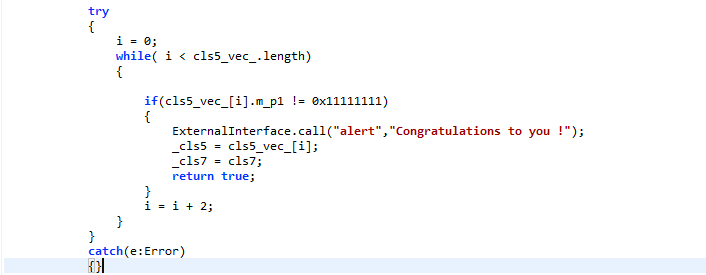
1. 要求：

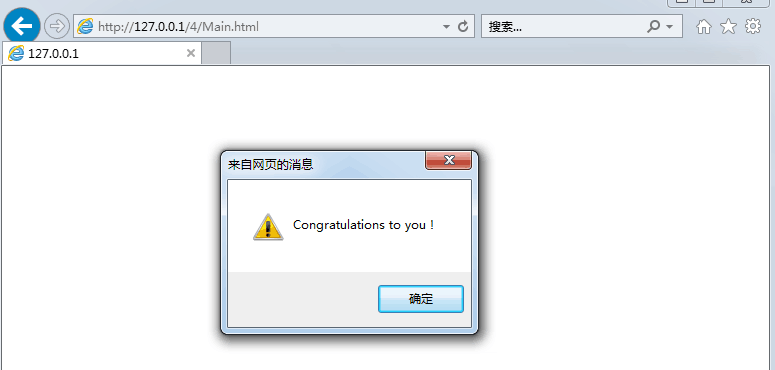
根据提供的Demo.swf，与参考文章。

自己动手编写能触发漏洞的POC，并在验证漏洞触发成功后的部分加入弹窗代码：

ExternalInterface.call("alert","Congratulations to you !");

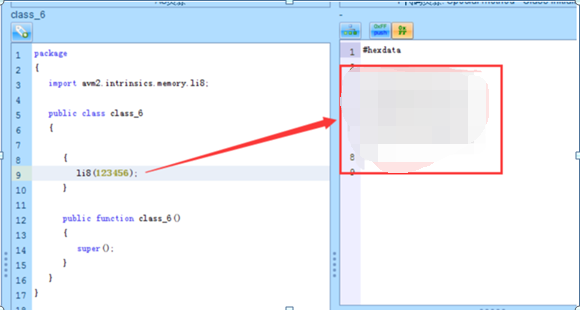
可参照下图写：



构造成功之后，在IE中加载并运行起来，可以得到如下弹窗：  


1. 最终的Flag ：

4.1由Class\_6类处的字节码，即右侧红框，如下图：



取其最后9个字节，假设为：11 22 33 44 55 66 60 70 47

4.2 alert 弹窗处的最后3个字节，如下图：

C:\Users\ply\Documents\Tencent Files\759907319\Image\C2C\Image1\8NP3GGO2(UUT}$}J`DQH9)6.png

假设为：2c 00 01 02 03，则取：01 02 03

那么flag 为 ：D0g3{010203112233445566607047}