Aesop_secret的writeup

原创

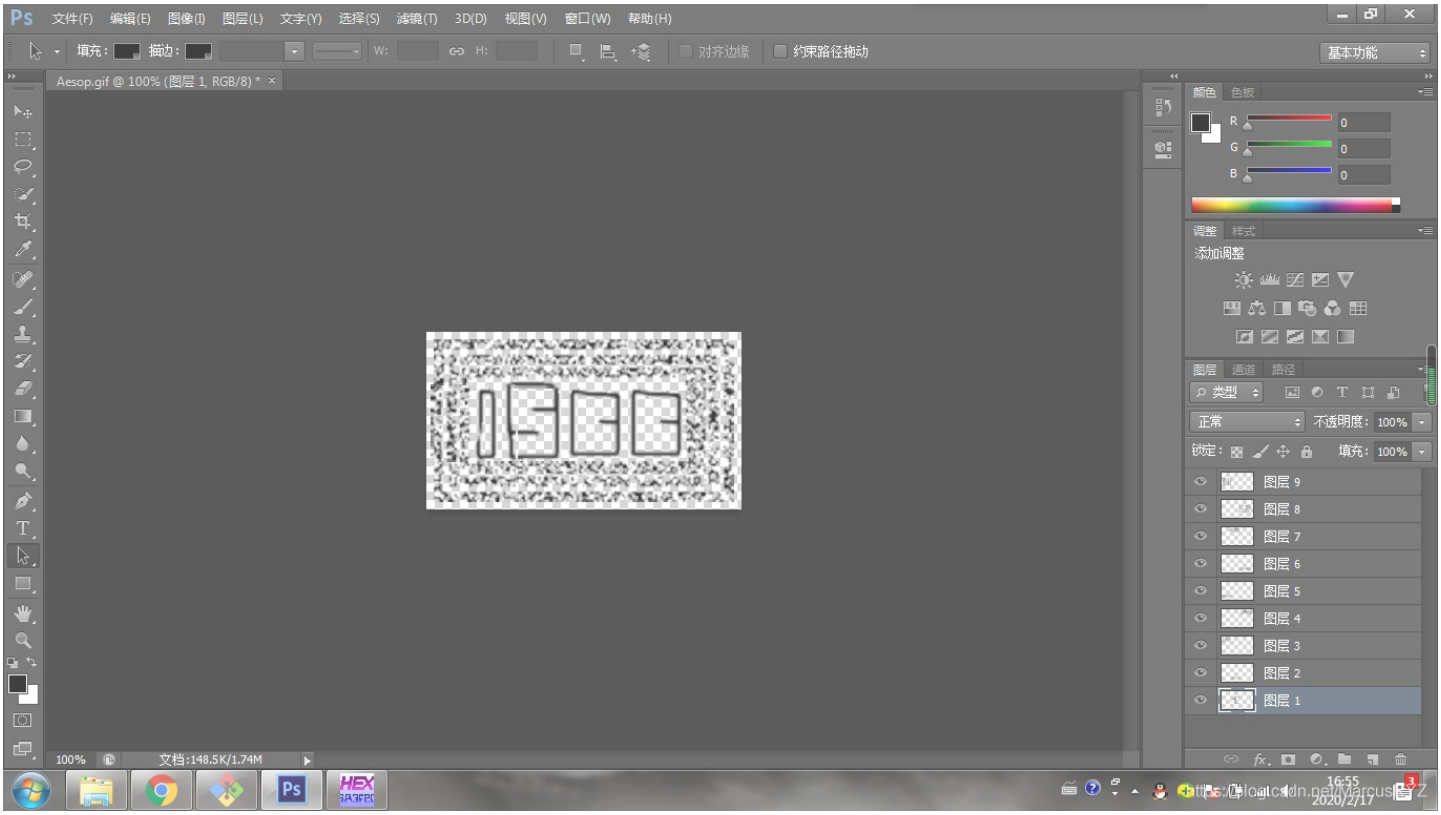
MarcusRYZ 于 2020-02-17 17:14:27 发布 3253 收藏 3

分类专栏： 攻防世界MISC高手进阶区 文章标签： 安全

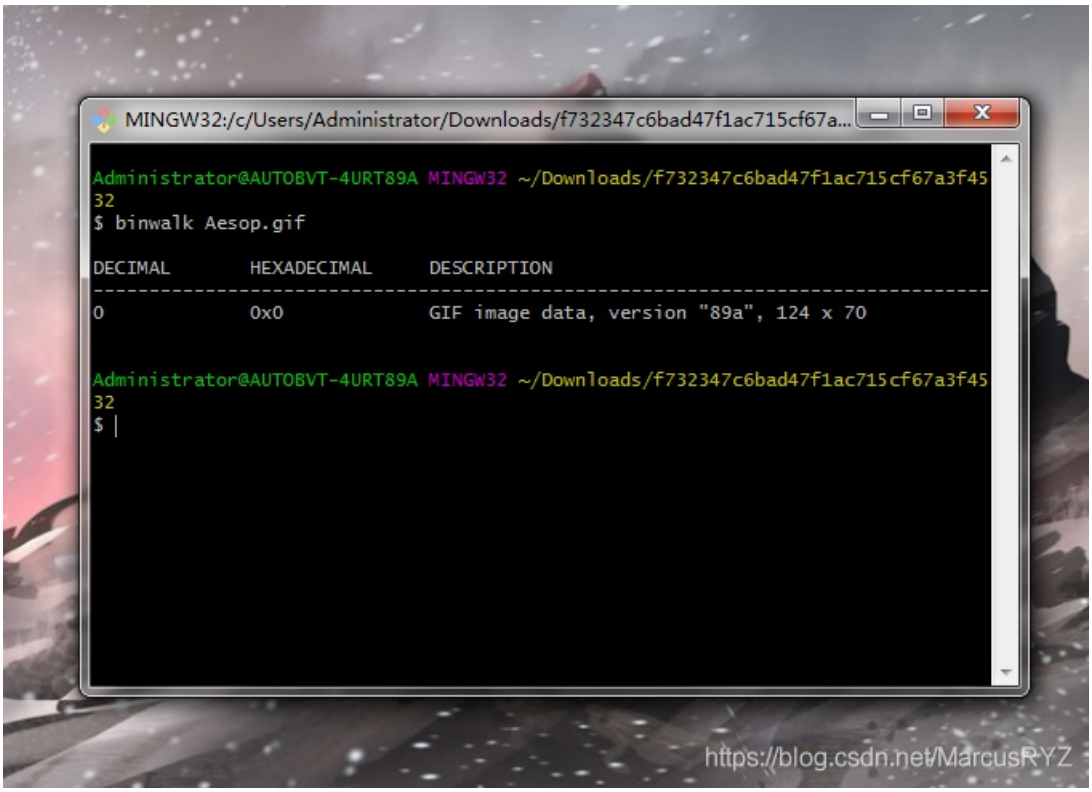
本文链接：https://blog.csdn.net/MarcusRYZ/article/details/104360845

大家好，这次我为大家带来的是攻防世界misc部分Aesop_secret的writeup。

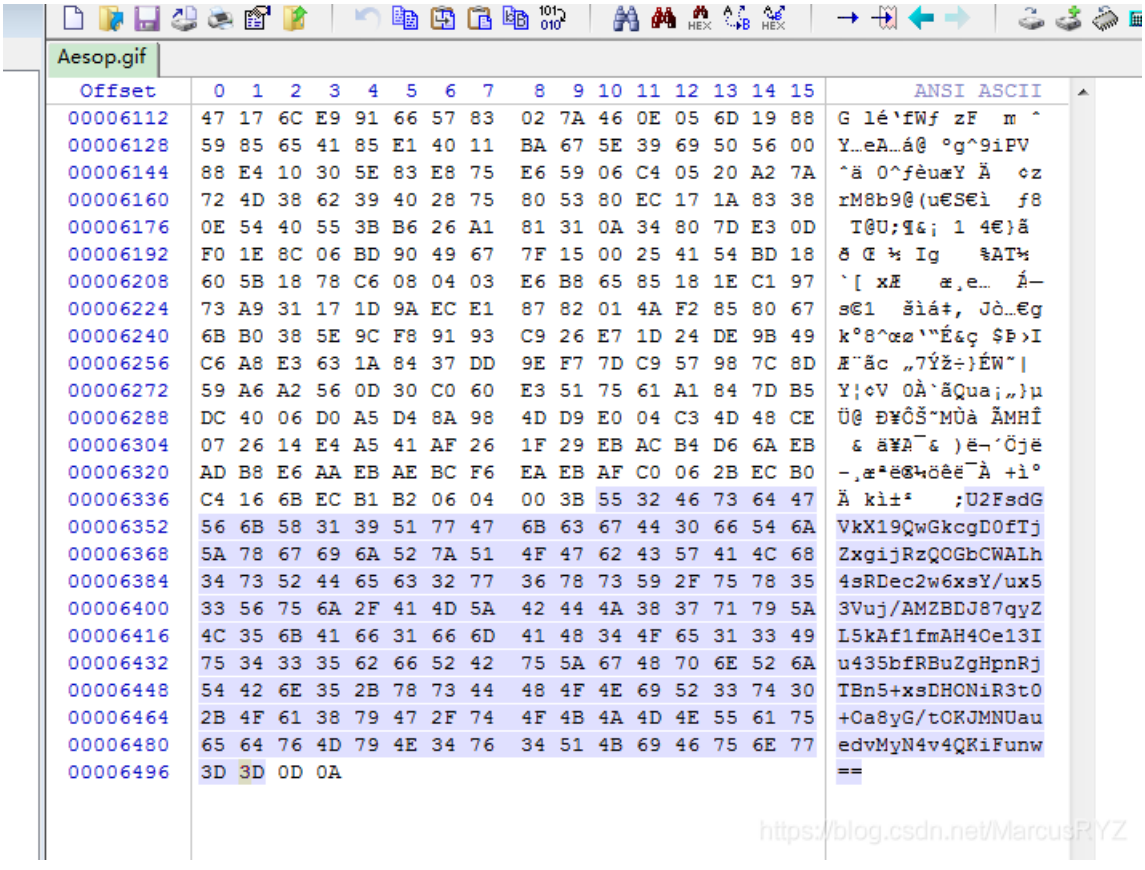
先下载附件，是一个压缩包，紧接着解压，发现一个gif文件。用浏览器打开，注意到这个gif文件播放时每一帧的位置都不一样，想到如果把每一帧的图像同时显现出来会怎么样。于是我们用Photoshop打开这个文件，显现每一帧图像。



看到一个字符串：ISCC，莫非这就是flag，然而尝试了无数次后都没有用。于是再看看题目，想到有一个加密方式叫AES加密，ISCC应该是密钥。这么一想，我们还需要找到加密后的字符串。尝试一下binwalk。

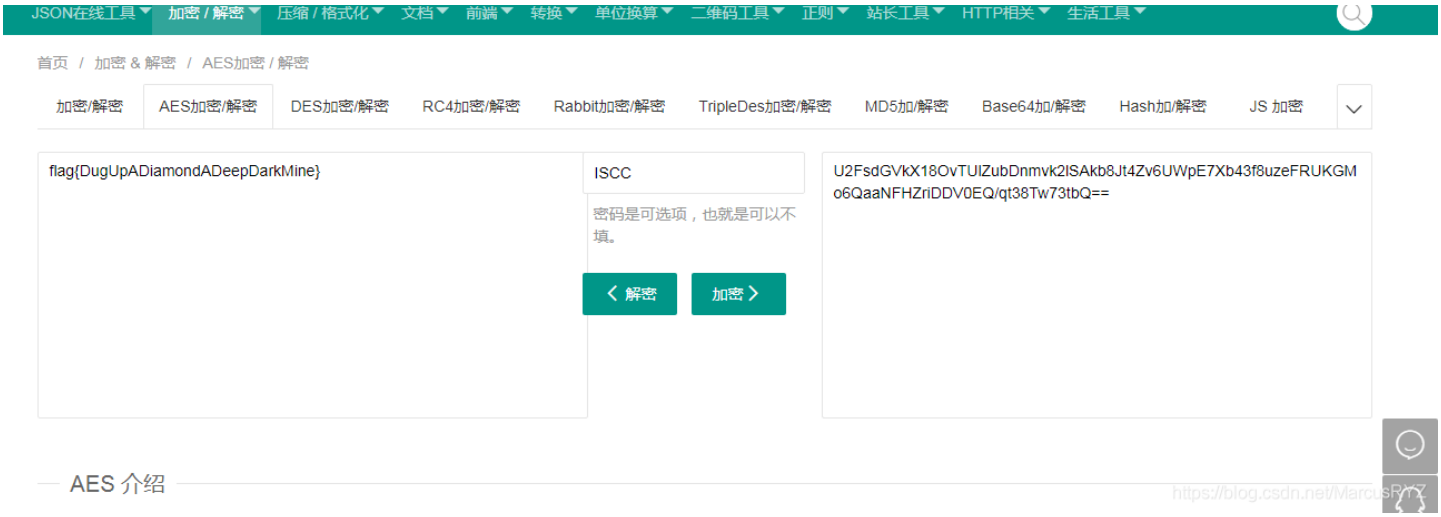


然而binwalk并没啥用，说明这个gif文件中没有混着其他文件。我们还有一个办法，就是将其放入winhex中查看一下。



功夫不负有心人，我们在gif文件的末尾找到了加密后的字符串。于是我们进行一下ASE在线解密。

这里是网址。



AES 介绍

连续解密两次后得到flag：DugUpADiamondADeepDarkMine。