

# xctf攻防世界 MISC高手进阶区 小小的PDF

原创

[18947943](#) 已于 2022-01-23 17:55:32 修改 154 收藏

分类专栏: [攻防世界misc之路](#) 文章标签: [misc](#)

于 2022-01-23 17:54:34 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/18947943/article/details/122654468>

版权



[攻防世界misc之路](#) 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

## 1. 进入环境，下载附件

题目给的是一个pdf文件，打开如图：



两页pdf，怀疑有东西

## 2. 问题分析

扔到kali中，binwalk发现一下，如图：

```
(zhangfa@kali)~[~/下载]
$ binwalk a4f37ec070974eadab9b96abd5ddffed.pdf

DECIMAL      HEXADECIMAL     DESCRIPTION
-----
0            0x0             PDF document, version: "1.4"
452         0x1C4          JPEG image data, JFIF standard 1.01
73254      0x11E26        JPEG image data, JFIF standard 1.01
81606      0x13EC6        Zlib compressed data, default compression
82150      0x140E6        JPEG image data, JFIF standard 1.01
104469     0x19815        Zlib compressed data, default compression
105134     0x19AAE        Zlib compressed data, default compression

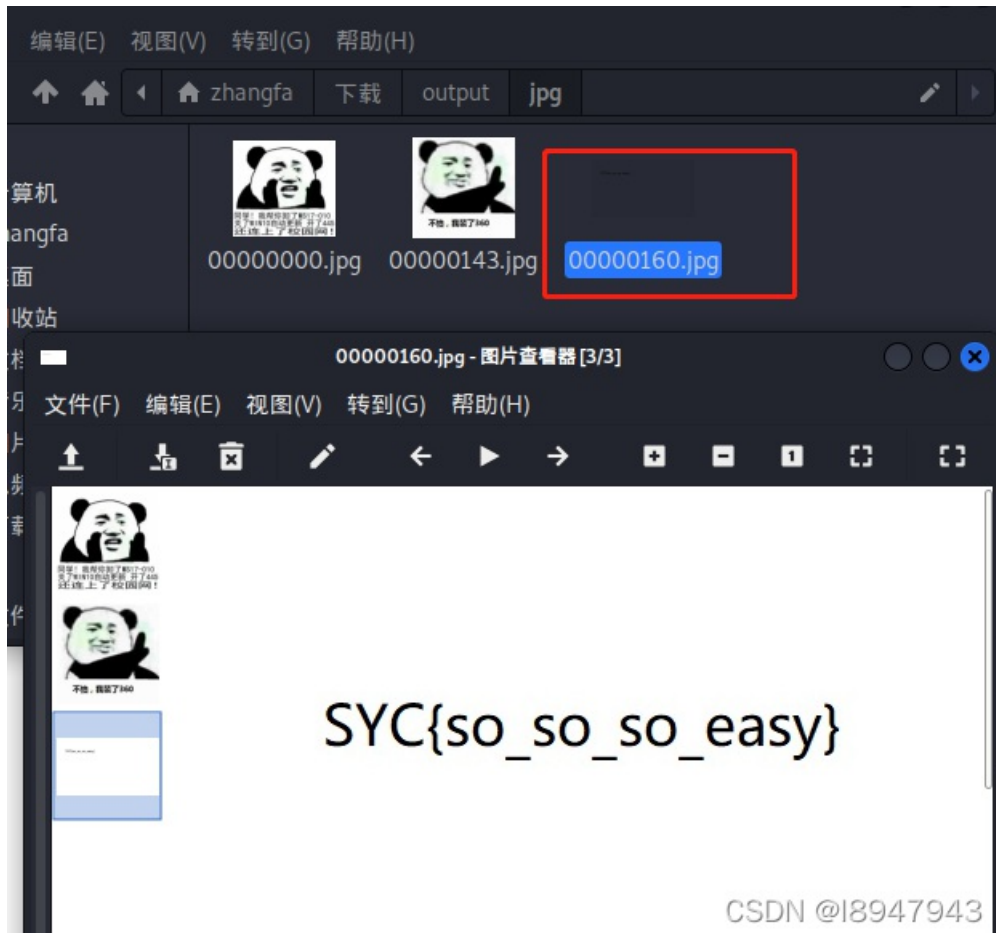
(zhangfa@kali)~[~/下载] CSDN @I8947943
```

发现有三个JPEG文件，但是文件显示只有两个，我们使用foremost分离一下，如图：

```
(zhangfa@kali)~[~/下载]
$ foremost a4f37ec070974eadab9b96abd5ddffed.pdf
Processing: a4f37ec070974eadab9b96abd5ddffed.pdf
|*|

(zhangfa@kali)~[~/下载]
```

打开分离的文件，打开发现如图：



最终答案为：SYC{so\_so\_so\_easy}

### 3. 方法二

参考网上wp，使用命令dd：

```
dd if=a4f37ec070974eadab9b96abd5ddffed.pdf of=1 skip=82150 bs=1
```

