

XCTF练习题---MISC---小小的PDF

原创

Hskb 于 2021-04-28 14:56:52 发布 139 收藏

分类专栏: [XCTF](#) 文章标签: [信息安全](#) [安全](#)

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/liu914589417/article/details/116233434>

版权



[XCTF 专栏收录该内容](#)

24 篇文章 1 订阅

订阅专栏

XCTF练习题—MISC—小小的PDF

flag: flag: SYC{so_so_so_easy}

解题步骤:

1、观察题目, 下载附件

小小的PDF

最佳Writeup由 [Nepnep](#) • [aaaaa12138](#) 提供

难度系数: ★ ★ ★ 2.0

题目来源: [CUIT-2017](#)

题目描述: 暂无

题目场景: 暂无

题目附件: [附件1](#)

[WP](#) [建议](#)

<https://blog.csdn.net/liu914589417>

2、下载完发现是一个PDF文件, 经过转Word, 查看属性, 十六进制查看后一无所获



同学! 我帮你卸了MS17-010

关了WIN10自动更新 开了445 还连上了校园网！



不怕，我装了360

<https://blog.csdn.net/liu914589417>

3、经过判断，尝试看看Kali的Binwalk，开启Kali，直接扔进去进行拆解，命令：binwalk a4f37ec070974eadab9b96abd5ddffed.pdf

```
root@kali:~# 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

```
root@kali:~#
```

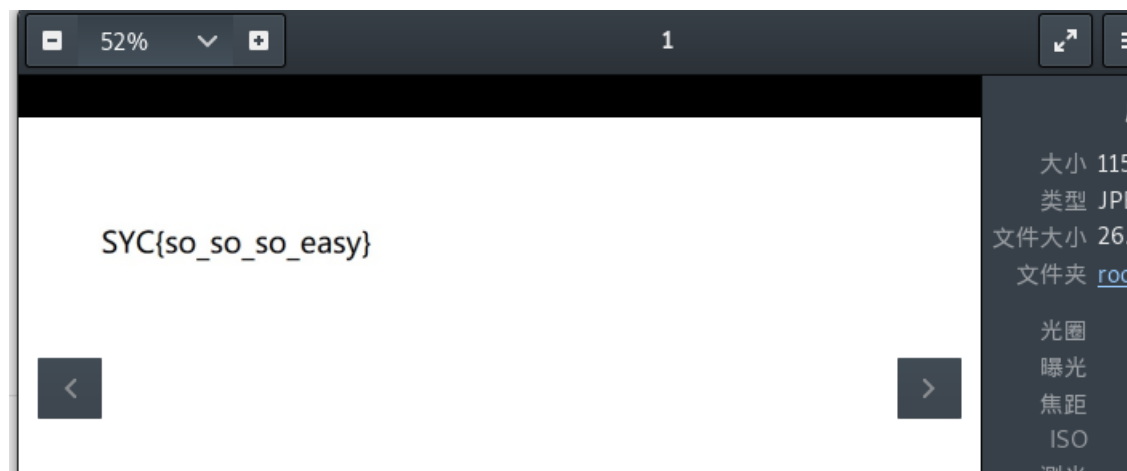
<https://blog.csdn.net/liu914589417>

4、经过拆分发现其中有3个图片，而PDF里只有两张图片，从而推测第三张图片就是flag，直接dd拷贝出来。命令如下：dd if=a4f37ec070974eadab9b96abd5ddffed.pdf of=1 skip=82150 bs=1

```
root@kali:~# dd if=a4f37ec070974eadab9b96abd5ddffed.pdf of=1 skip=82150 bs=1
```

记录了26695+0 的读入
记录了26695+0 的写出
26695 bytes (27 kB, 26 KiB) copied, 0.158957 s, 168 kB/s

5、直接回到PDF存放的根目录，直接把三张图片拷贝出来，果断获得Flag



6、提交答案，完成

恭喜您答对了

难度 ★★

耗时: 11分23秒

积分: 2.00

金币: 2 +1

以下是您获得的额外奖励

额外金币加 1

上传Writeup

讨论本题

下一题

<https://blog.csdn.net/liu914589417>

博客园地址: <https://www.cnblogs.com/redHskb/>

知乎地址: <https://www.zhihu.com/people/yi-kuai-xiao-bing-gan-43-64/posts>

欢迎关注评论, 耶斯莫拉