CTF——MISC——zip伪加密总结

原创

Captain Hammer 于 2019-08-20 16:22:42 发布 4398 收藏 31
分类专栏： web安全 CTF 类型题总结

本文链接：https://blog.csdn.net/vhkjhwbs/article/details/99851686


web安全 同时被 2 个专栏收录
19 篇文章 5 订阅
订阅专栏


CTF 类型题总结
11 篇文章 35 订阅
订阅专栏

看了好多博文总结一下吧

zip 伪加密原理：

zip伪加密是在**文件头的加密标志位做修改**，进而再打开文件时识被别为加密压缩包。

把 **压缩源文件目录区** 的 **全局方式位标记** 的 01 00 或 09 00 改为 00 00 就可以**去除**密码

把 **压缩源文件目录区** 的 **全局方式位标记** 的 00 00 改为 01 00 或 09 00 就可以**添加**密码 提示

zip 文件

一个 **ZIP** 文件由三个部分组成：

压缩源文件数据区 + **压缩源文件目录区** + **压缩源文件目录结束标志**

这里附上一篇说明博文：https://blog.csdn.net/wclxyn/article/details/7288994

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	50	4B	03	04	14	00	01	00	08	00	5A	7E	F7	46	16	B5
00000010	80	14	19	00	00	00	17	00	00	00	07	00	00	00	6B	65
00000020	79	2E	74	78	74	0B	CE	CC	75	0E	71	AB	CE	48	CD	C9
00000030	C9	57	28	CE	CC	2D	C8	49	AD	28	4D	AD	05	00	50	4B
00000040	01	02	3F	00	14	00	09	00	08	00	5A	7E	F7	46	16	B5
00000050	80	14	19	00	00	00	17	00	00	00	07	00	24	00	00	00
00000060	00	00	00	00	20	00	00	00	00	00	00	00	6B	65	79	2E
00000070	74	78	74	0A	00	20	00	00	00	00	00	01	00	18	00	65
00000080	58	F0	4A	1C	C5	D0	01	BD	EB	DD	3B	1C	C5	D0	01	BD
00000090	EB	DD	3B	1C	C5	D0	01	50	4B	05	06	00	00	00	00	01
000000A0	00	01	00	59	00	00	00	3E	00	00	00	00	00			

压缩源文件数据区：

50 4B 03 04：这是头文件标记（0x04034b50）
14 00：解压文件所需 pkware 版本
00 00：全局方式位标记（有无加密）
08 00：压缩方式
5A 7E：最后修改文件时间
F7 46：最后修改文件日期
16 B5 80 14：CRC-32校验（1480B516）
19 00 00 00：压缩后尺寸（25）
17 00 00 00：未压缩尺寸（23）
07 00：文件名长度
00 00：扩展记录长度
6B65792E7478740BCECC750E71ABCE48CDC9C95728CECC2DC849AD284DAD0500

压缩源文件目录区：

50 4B 01 02：目录中文件文件头标记(0x02014b50)
3F 00：压缩使用的 pkware 版本
14 00：解压文件所需 pkware 版本
00 00：全局方式位标记（有无加密，这个更改这里进行伪加密，改为09 00打开就会提示有密码了）
08 00：压缩方式
5A 7E：最后修改文件时间
F7 46：最后修改文件日期
16 B5 80 14：CRC-32校验（1480B516）
19 00 00 00：压缩后尺寸（25）
17 00 00 00：未压缩尺寸（23）
07 00：文件名长度
24 00：扩展字段长度
00 00：文件注释长度
00 00：磁盘开始号
00 00：内部文件属性
20 00 00 00：外部文件属性
00 00 00 00：局部头部偏移量
6B65792E7478740A00200000000000010018006558F04A1CC5D001BDEBDD3B1CC5D001BDEBDD3B1C0

压缩源文件目录结束标志：

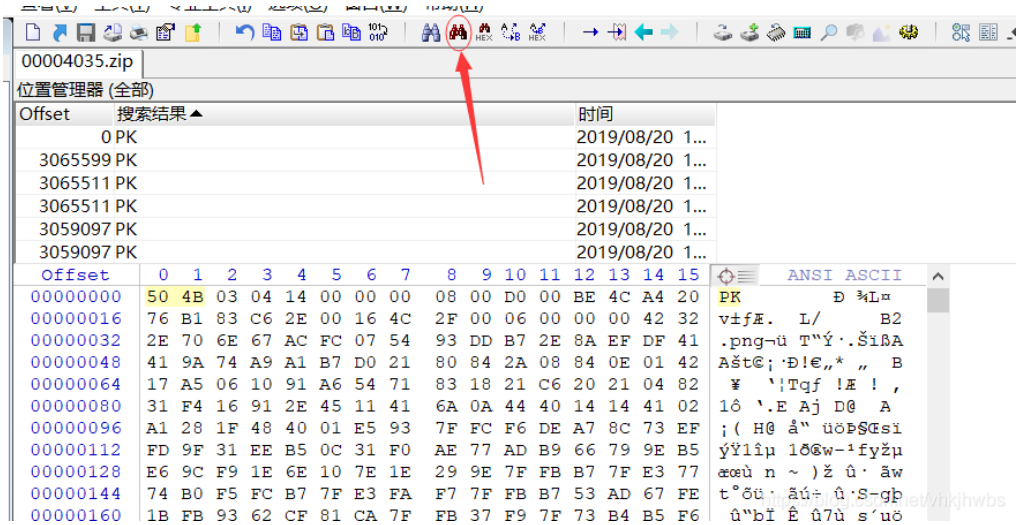
50 4B 05 06：目录结束标记
00 00：当前磁盘编号
00 00：目录区开始磁盘编号
01 00：本磁盘上纪录总数
01 00：目录区中纪录总数
59 00 00 00：目录区尺寸大小
3E 00 00 00：目录区对第一张磁盘的偏移量
00 00：ZIP 文件注释长度

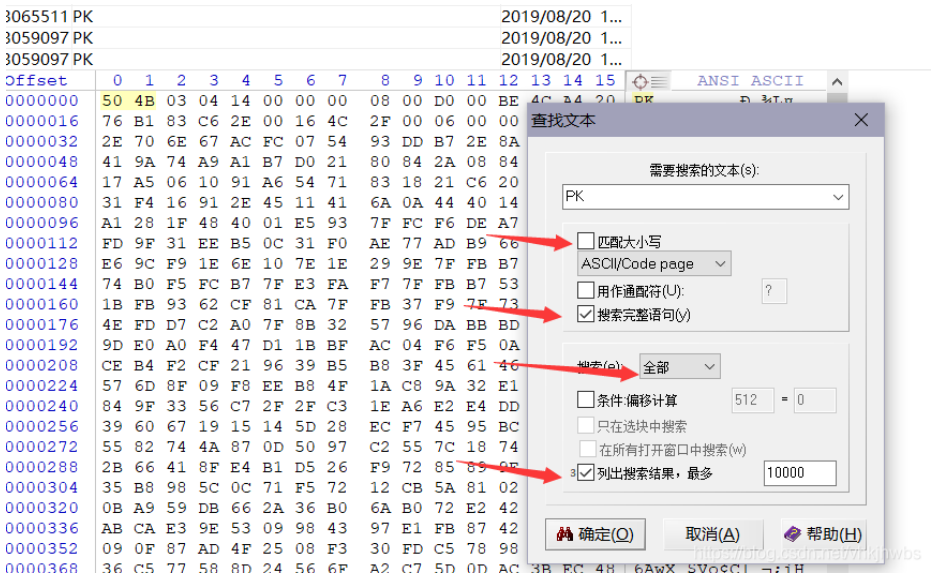
查找压缩文件目录区：

一般面对一些小的文件时 很容易就找到 压缩文件目录区 的文件头

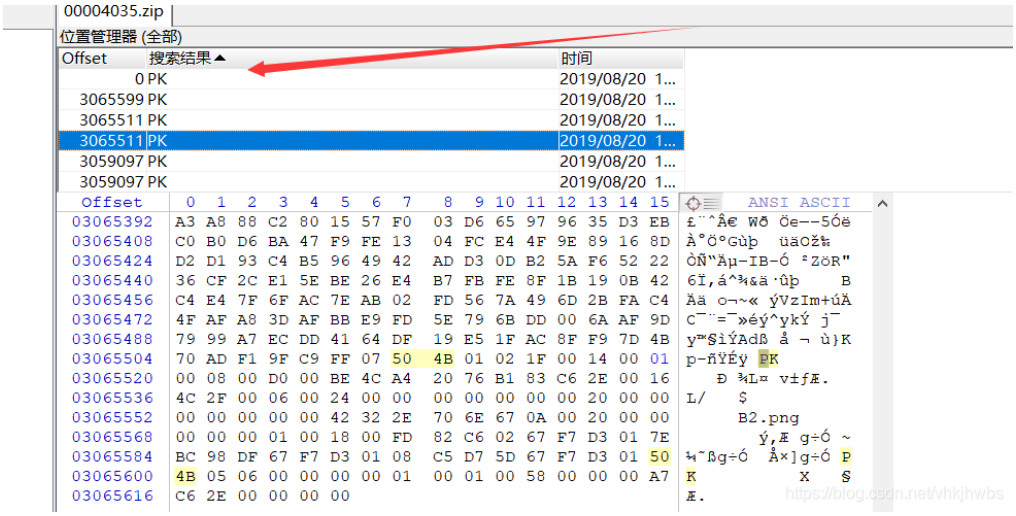
但是当我们面对一些较大的文件 找 压缩文件目录区的 文件头 50 4B 01 02 就有点麻烦了

我们可以利用 winhex 中的查找 字符查找 快速找到 压缩文件目录区 的文件头



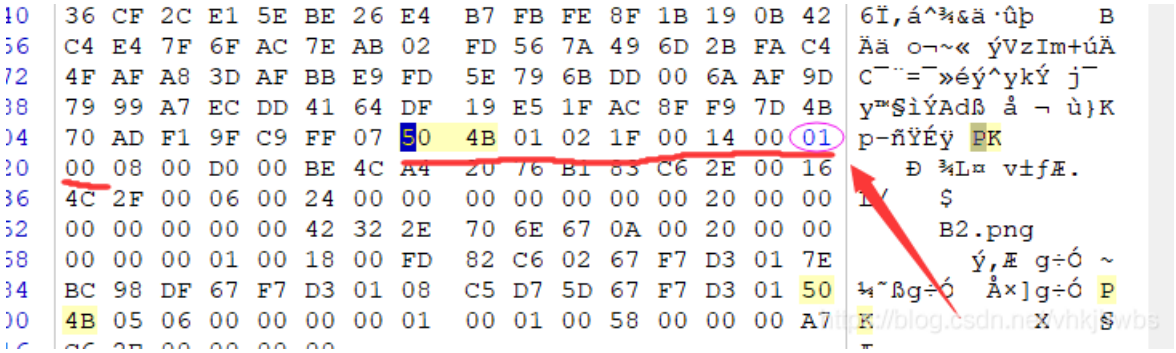


然后搜索的结果就会被列出来 点击 后快速定位到相应位置



这样就能快找到 50 4B 01 02 头了

然后把 后面的 全方位标记区 的 01 00 或 09 00 改为 00 00 保存 后就可以打开压缩包了



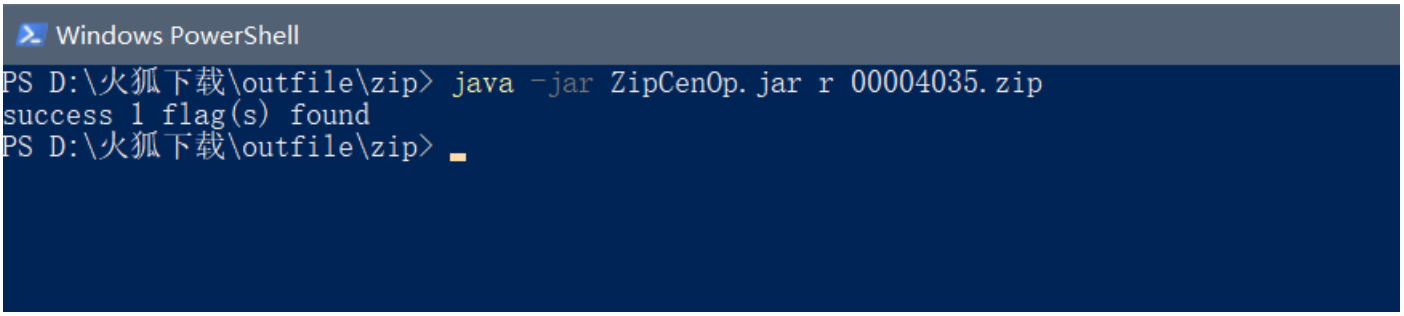
如果不想用手工修改 也可以用工具 修改

使用ZipCenOp.jar清除密码

ZipCenOp.jar 下载地址：https://pan.baidu.com/s/1GHcUYA36X9reZL7rcmWNfA 提取码：ugyn

下载后 把它和压缩包放在同一个文件夹里 打开cmd 切换到 这个文件夹 （或者直接用 powershall） 执行：

```
java -jar ZipCenOp.jar r 00004035.zip
```



就 可以修复文件头 了

（注意：工具不是万能的，手工比较可靠）