misc/fo-dao/writeup

原创

温酒的周同学 于 2019-08-29 21:03:41 发布 136 收藏

分类专栏： Linux misc ctf

本文链接：https://blog.csdn.net/qq_38834590/article/details/100144359

版权

Linux 同时被 3 个专栏收录

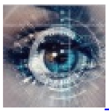
8 篇文章 0 订阅

订阅专栏

misc

1 篇文章 0 订阅

订阅专栏

 ctf

1 篇文章 0 订阅

订阅专栏

文章目录

- 题目描述(资源待上传)
- 操作环境
- 步骤
  - fo.doc
  - dao.doc
  - flag提交
- 小结

题目描述(资源待上传)

题目资源：fo.doc、dao.doc

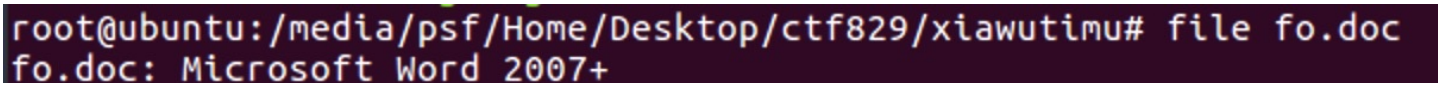
操作环境

Linux＋Windows

步骤

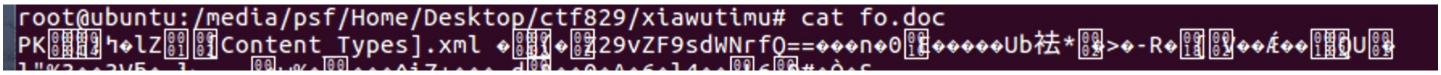
fo.doc

工具：Windows下的`010editor`
首先在Linux下查看文件类型：



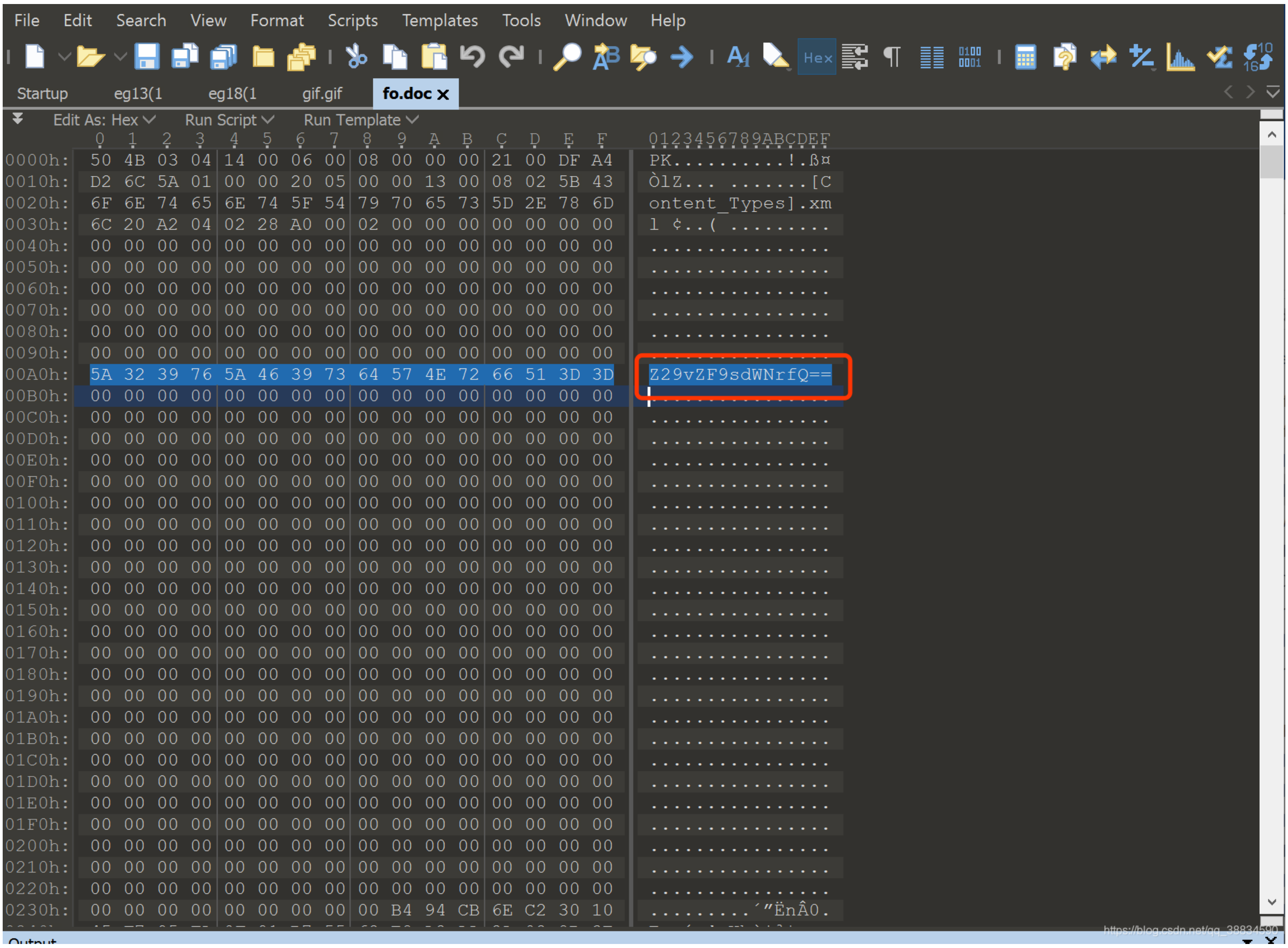
```
root@ubuntu:/media/psf/Home/Desktop/ctf829/xiawutimu# file fo.doc
fo.doc: Microsoft Word 2007+
```

似乎看不出什么东西，那么直接查看内容：



```
root@ubuntu:/media/psf/Home/Desktop/ctf829/xiawutimu# cat fo.doc
PK����ｈ�lZ����Content_Types].xml ����Z29vZF9sdWNrfQ==���n�0�������Ub祛*��>�-R������É����QU��
```

后面一大串乱码不用管，开局是`PK`就可以看出这是个`.zip`文件，原因可以参考【CTF 攻略】CTF比赛中关于zip的总结。我们在Windows下用`010editor`打开该文件，嗯，如下图，红框部分一看就是个`base64`的密文，原因可自行搜索base64的末尾字节补足规则。

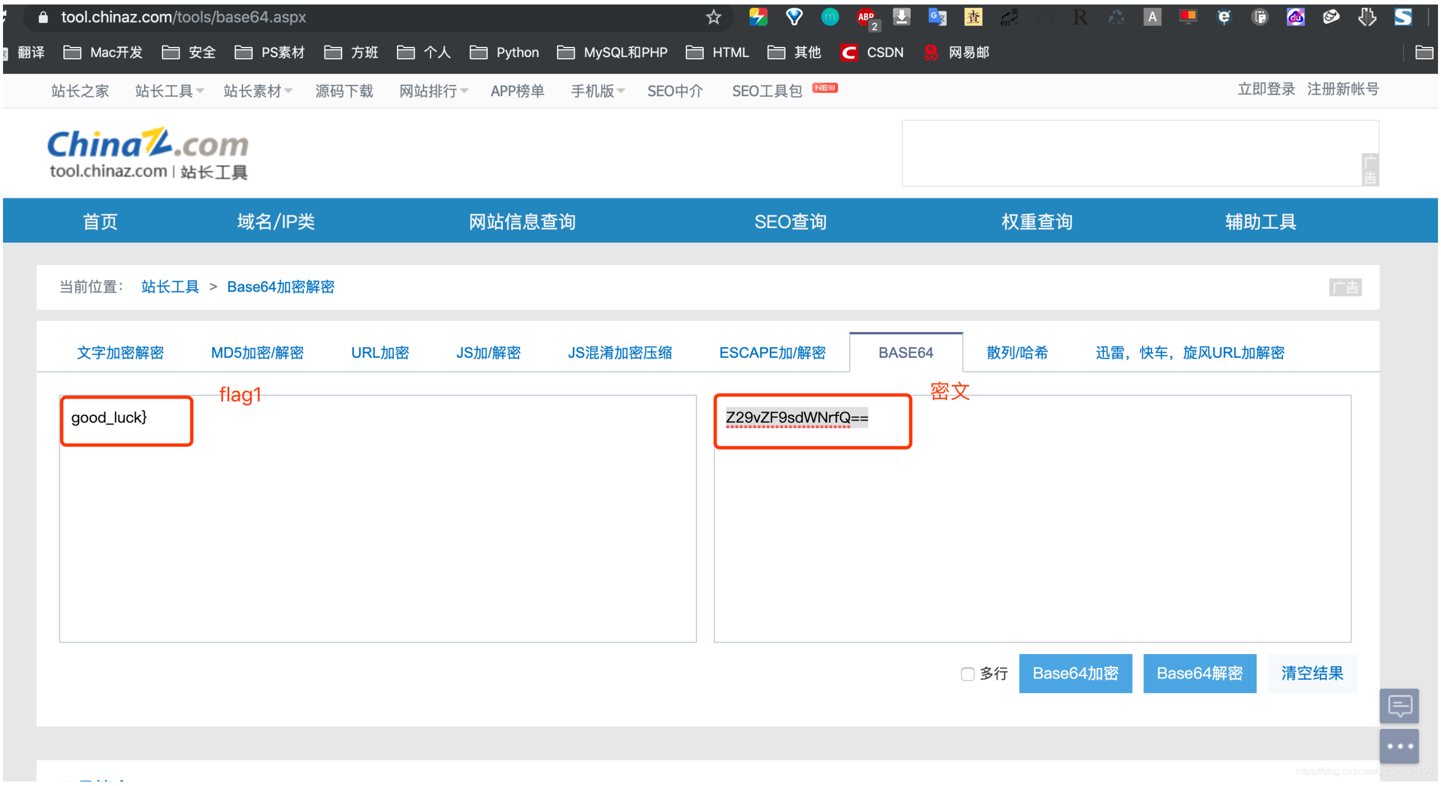


```
         0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h:  50 4B 03 04 14 00 06 00 08 00 00 00 21 00 DF A4   PK..........!.ß¤
0010h:  D2 6C 5A 01 00 00 20 05 00 00 13 00 08 02 5B 43   ÒlZ... .......[C
0020h:  6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D   ontent_Types].xm
0030h:  6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00   l ¢..( .........
0040h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0050h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0060h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0070h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0080h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0090h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00A0h:  5A 32 39 76 5A 46 39 73 64 57 4E 72 66 51 3D 3D   Z29vZF9sdWNrfQ==
00B0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00C0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00D0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00E0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00F0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0100h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0110h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0120h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0130h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0140h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0150h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0160h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0170h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0180h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0190h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01A0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01B0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01C0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01D0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01E0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01F0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0200h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0210h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0220h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0230h:  00 00 00 00 00 00 00 00 00 B4 94 CB 6E C2 30 10   .........´"ËnÂ0.
```

拿到的加密字符串如下：

```
Z29vZF9sdWNrfQ==
```

依据字符串的特征，末尾有两个`=`f符号，我们选择用base64进行解密：
使用站长工具：


tool.chinaz.com/tools/base64.aspx
翻译 Mac开发 安全 PS素材 方班 个人 Python MySQL和PHP HTML 其他 CSDN 网易邮
站长之家 站长工具 站长素材 源码下载 网站排行 APP榜单 手机版 SEO中介 SEO工具包 NEW 立即登录 注册新帐号
ChinaZ.com tool.chinaz.com | 站长工具
首页 域名/IP类 网站信息查询 SEO查询 权重查询 辅助工具
当前位置： 站长工具 > Base64加密解密
文字加密解密 MD5加密/解密 URL加密 JS加/解密 JS混淆加密压缩 ESCAPE加/解密 BASE64 散列/哈希 迅雷，快车，旋风URL加解密
□ 多行 Base64加密 Base64解密 清空结果

good_luck}

flag1

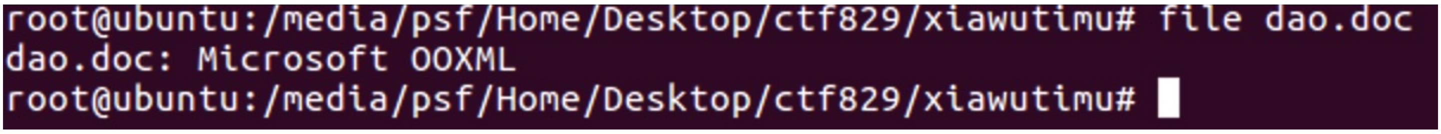
Z29vZF9sdWNrfQ==

密文

如上图所述是部分flag1: `good_luck}`

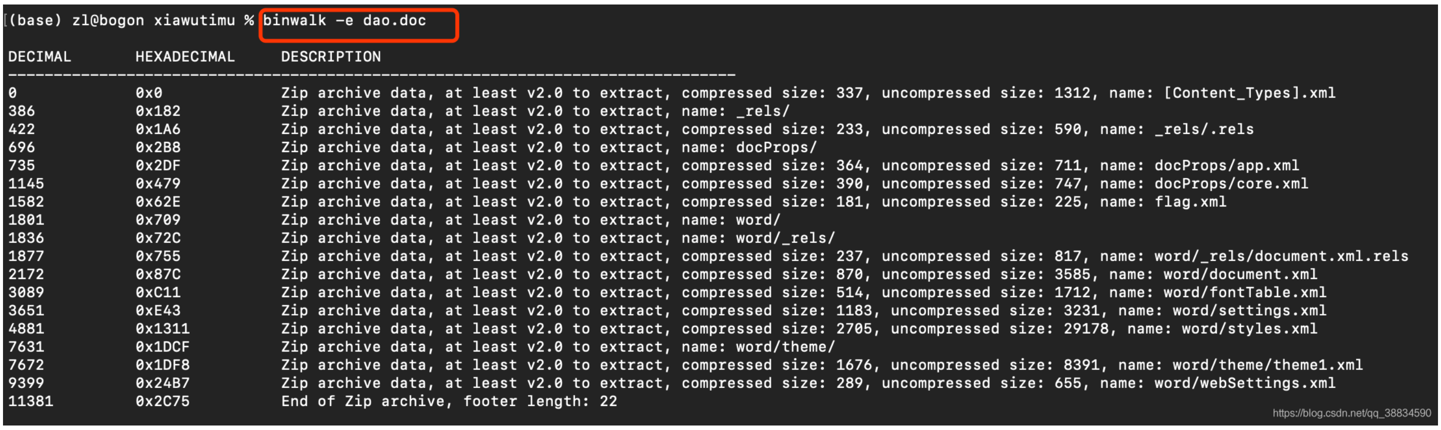
dao.doc

工具：Linux下的binwalk工具
首先查看文件类型：



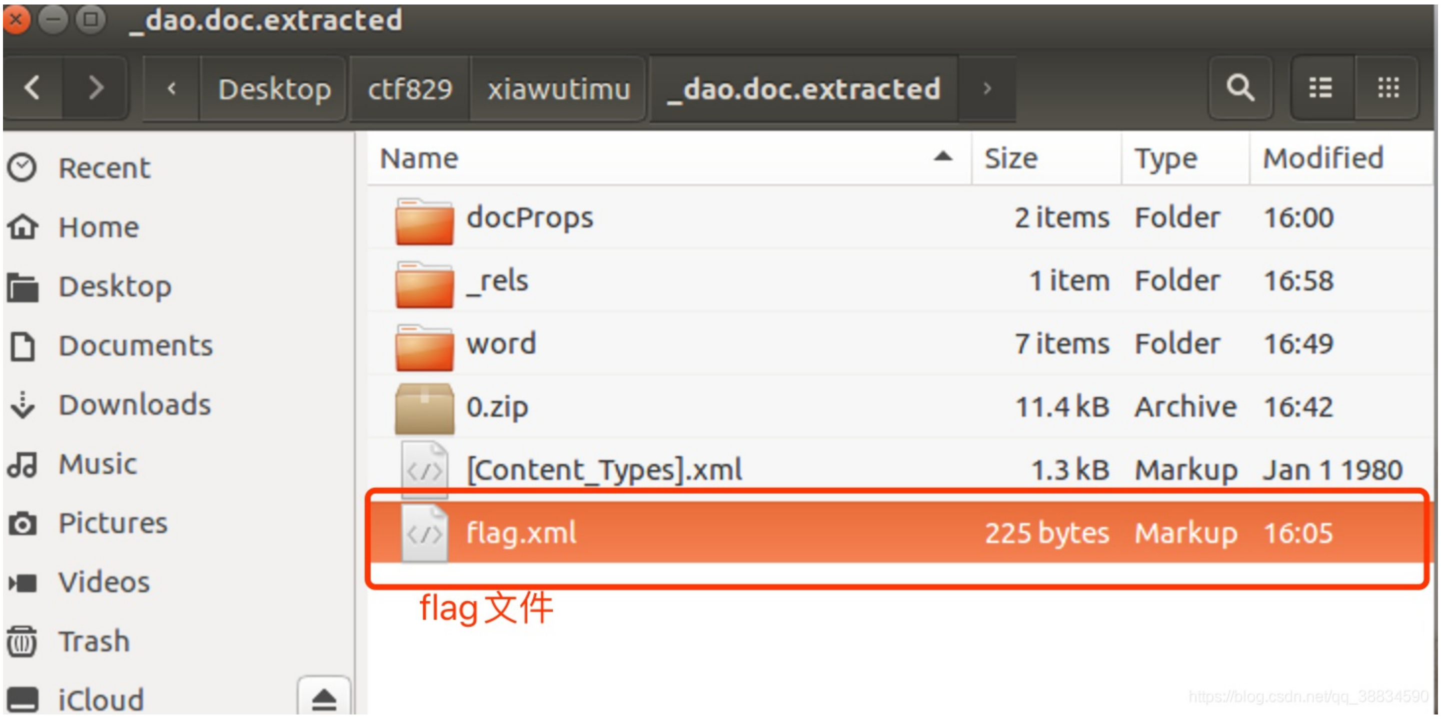
```
root@ubuntu:/media/psf/Home/Desktop/ctf829/xiawutimu# file dao.doc
dao.doc: Microsoft OOXML
root@ubuntu:/media/psf/Home/Desktop/ctf829/xiawutimu# 
```

看起来似乎就是跟后缀名一样的文件，那么我们直接压查看文件:



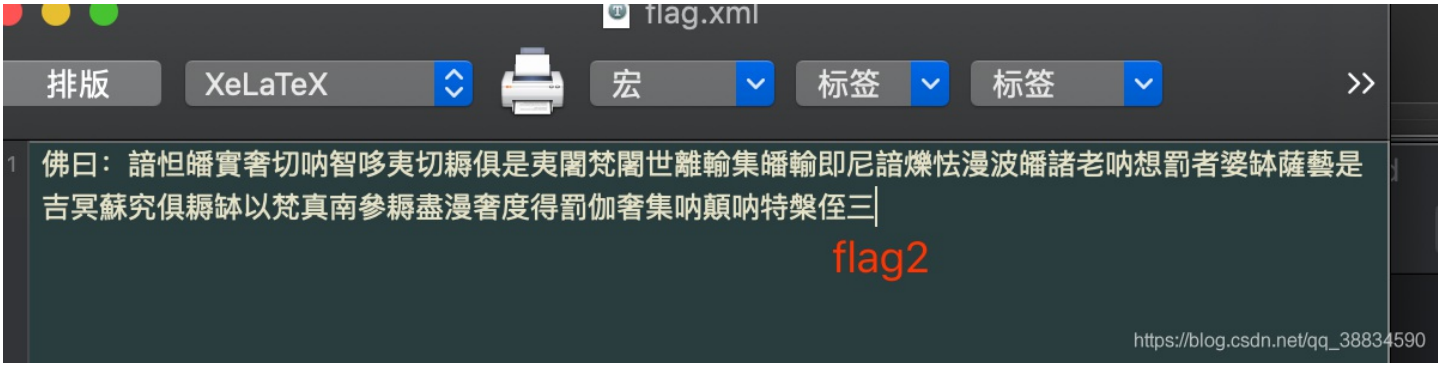
```
(base) zl@bogon xiawutimu % binwalk -e dao.doc

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compressed size: 337, uncompressed size: 1312, name: [Content_Types].xml
386           0x182           Zip archive data, at least v2.0 to extract, name: _rels/
422           0x1A6           Zip archive data, at least v2.0 to extract, compressed size: 233, uncompressed size: 590, name: _rels/.rels
696           0x2B8           Zip archive data, at least v2.0 to extract, name: docProps/
735           0x2DF           Zip archive data, at least v2.0 to extract, compressed size: 364, uncompressed size: 711, name: docProps/app.xml
1145          0x479           Zip archive data, at least v2.0 to extract, compressed size: 390, uncompressed size: 747, name: docProps/core.xml
1582          0x62E           Zip archive data, at least v2.0 to extract, compressed size: 181, uncompressed size: 225, name: flag.xml
1801          0x709           Zip archive data, at least v2.0 to extract, name: word/
1836          0x72C           Zip archive data, at least v2.0 to extract, name: word/_rels/
1877          0x755           Zip archive data, at least v2.0 to extract, compressed size: 237, uncompressed size: 817, name: word/_rels/document.xml.rels
2172          0x87C           Zip archive data, at least v2.0 to extract, compressed size: 870, uncompressed size: 3585, name: word/document.xml
3089          0xC11           Zip archive data, at least v2.0 to extract, compressed size: 514, uncompressed size: 1712, name: word/fontTable.xml
3651          0xE43           Zip archive data, at least v2.0 to extract, compressed size: 1183, uncompressed size: 3231, name: word/settings.xml
4881          0x1311          Zip archive data, at least v2.0 to extract, compressed size: 2705, uncompressed size: 29178, name: word/styles.xml
7631          0x1DCF          Zip archive data, at least v2.0 to extract, name: word/theme/
7672          0x1DF8          Zip archive data, at least v2.0 to extract, compressed size: 1676, uncompressed size: 8391, name: word/theme/theme1.xml
9399          0x24B7          Zip archive data, at least v2.0 to extract, compressed size: 289, uncompressed size: 655, name: word/webSettings.xml
11381         0x2C75          End of Zip archive, footer length: 22
```

使用binwalk工具解压后得到flag文件：



Name	Size	Type	Modified
docProps	2 items	Folder	16:00
_rels	1 item	Folder	16:58
word	7 items	Folder	16:49
0.zip	11.4 kB	Archive	16:42
[Content_Types].xml	1.3 kB	Markup	Jan 1 1980
flag.xml	225 bytes	Markup	16:05

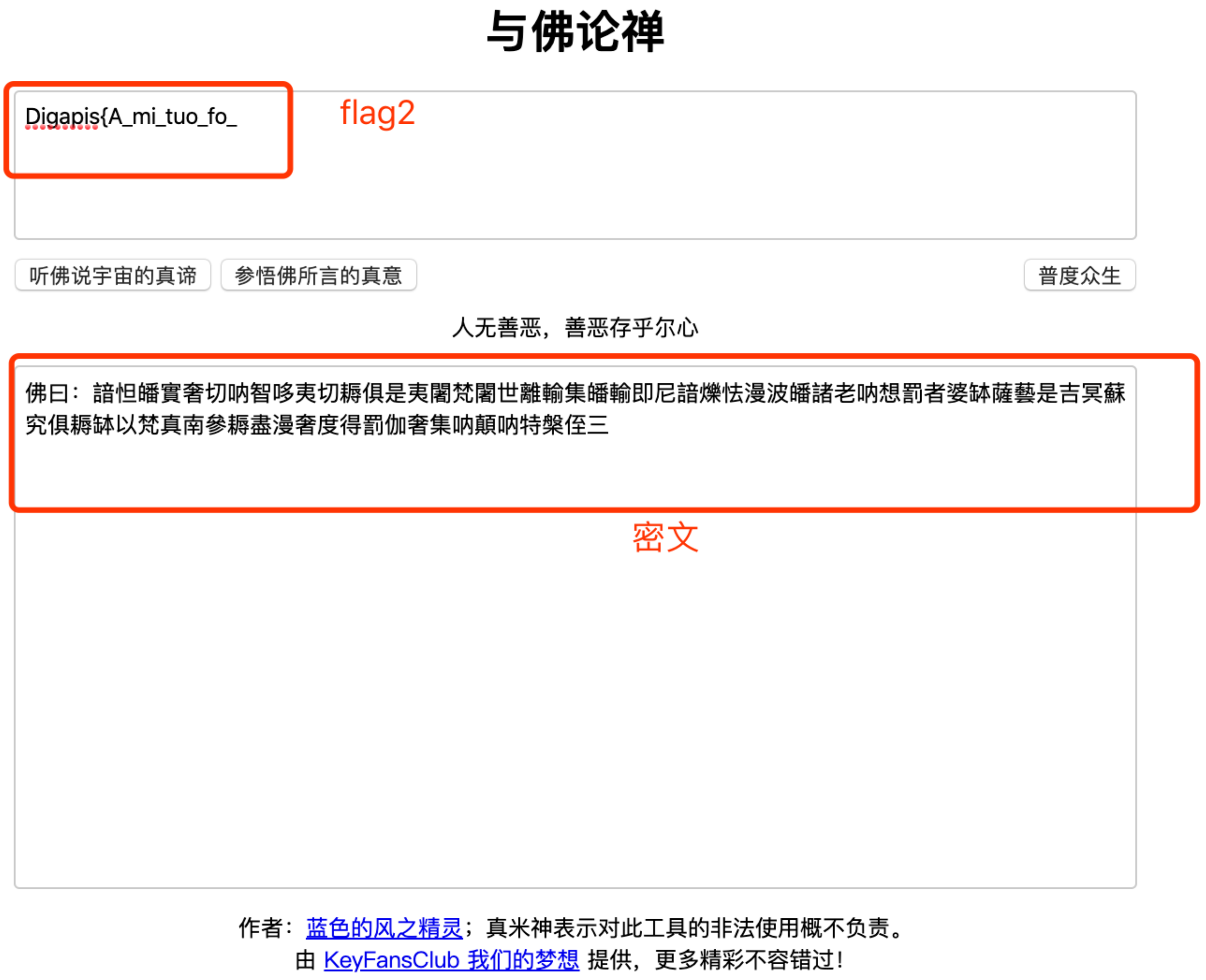
点开文件查看一下：



```
佛曰：諳怛皤實奢切吶智哆夷切耨俱是夷闍梵闍世離輸集皤輸即尼諳爍怯漫波皤諸老吶想罰者婆缽薩藝是吉冥蘇究俱耨缽以梵真南參耨盡漫奢度得罰伽奢集吶顛吶特槃侄三
```

嗯，这个确实很佛，那我们佛系找工具，随手网上搜索与佛论禅加密解密工具

> 佛曰：諳怛皤實奢切吶智哆夷切耨俱是夷闍梵闍世離輸集皤輸即尼諳爍怯漫波皤諸老吶想罰者婆缽薩藝是吉冥蘇究俱耨缽以梵真南參耨盡漫奢度得罰伽奢集吶顛吶特槃侄三



与佛论禅

Digapis{A_mi_tuo_fo_

人无善恶，善恶存乎尔心

佛曰：諳怛皤實奢切吶智哆夷切耨俱是夷闍梵闍世離輸集皤輸即尼諳爍怯漫波皤諸老吶想罰者婆缽薩藝是吉冥蘇究俱耨缽以梵真南參耨盡漫奢度得罰伽奢集吶顛吶特槃侄三

作者：蓝色的风之精灵；真米神表示对此工具的非法使用概不负责。
由 KeyFansClub 我们的梦想 提供，更多精彩不容错过！

那么我们就拿到了flag2: `Digapis{A_mi_tuo_fo_`

flag提交

flag格式一般为`flag{flagcontent}`，所以我们将前面得到的flag拼接起来提交。

> Digapis{A_mi_tuo_fo_good_luck}

小结

工具还是好用啊！