

【愚公系列】2022年02月 攻防世界-进阶题-MISC-86(picture2)

原创

愚公搬代码 于 2022-02-19 17:01:40 发布 5666 收藏

分类专栏: #CTF-攻防世界-MISC 文章标签: 网络安全

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/aa2528877987/article/details/123019801>

版权



[CTF-攻防世界-MISC 专栏收录该内容](#)

98 篇文章 0 订阅

订阅专栏

文章目录

[前言](#)

[一、picture2](#)

[二、答题步骤](#)

[1.下载附件](#)

[2.binwalk](#)

[3.python脚本](#)

[4.winhex](#)

[5.UUencode](#)

[总结](#)

前言

UUencode是二进制信息和文字信息之间的转换编码，也就是机器和人眼识别的转换。UUencode编码方案常见于电子邮件信息的传输，目前已被多用途互联网邮件扩展（MIME）大量取代。

UUencode将输入文字以每三个字节为单位进行编码，如此重复进行。如果最后剩下的文字少于三个字节，不够的部份用零补齐。这三个字节共有24个Bit，以6-bit为单位分为4个群组，每个群组以十进制来表示所出现的数值只会落在0到63之间。将每个数加上32，所产生的结果刚好落在ASCII字符集中可打印字符（32-空白...95-底线）的范围之中。

UUencode编码每60个将输出为独立的一行（相当于45个输入字节），每行的开头会加上长度字符，除了最后一行之外，长度字符都应该是“M”这个ASCII字符（77=32+45），最后一行的长度字符为32+剩下的字节数目这个ASCII字符。

一、picture2

题目链接: https://adworld.xctf.org.cn/task/task_list?type=misc&number=1&grade=1&page=5

The screenshot shows the XCTF platform interface. At the top, there are navigation links: 答题 (Answer), 竞赛 (Competition), 排行榜 (Ranking), 队伍 (Team), 商城 (Commerce), 消息 (Message) with a notification count of 1, and 豆公搬代码 (Doubgong搬代码) with a language switch (中 / En). The user's current status is shown as misc 积分: 235分 and 本题金币: 5个.

The main content area displays the challenge details for "picture2". It includes:

- 返回 (Back) button and a sun icon.
- 本题用时: 2分27秒 (Time spent: 2 minutes 27 seconds).
- 难度系数: ★★★★★ 5.0 (Difficulty coefficient: ★★★★★ 5.0).
- 题目来源: CISCN-2018-Quals (Source: CISCN-2018-Quals).
- 题目描述: 暂无 (Description: None).
- 题目场景: 暂无 (Scenario: None).
- 题目附件: 附件1 (Attachment 1).
- A large input field at the bottom labeled flag..

To the right, there is a "实时消息" (Real-time Message) panel showing two messages from other users:

- 用户薔薇花解出Web方向《Confusion1》,获得4.0积分,4金币,耗时9分1秒 (User Rosehua solved the Web direction of Confusion1, earning 4.0 points and 4 gold coins, taking 9 minutes and 1 second.) - 2022-02-19 16:09:01
- 用户LiShui解出Web方向《weak_auth》,获得1.0积分,1金币,耗时59分0秒 (User LiShui solved the Web direction of weak_auth, earning 1.0 points and 1 gold coin, taking 59 minutes and 0 seconds.) - 2022-02-19 16:09:01

The bottom right corner features the XCTF logo with the text "XCTF 高校网络安全专题挑战赛" and "©豆公搬代码".

二、答题步骤

1. 下载附件

得到一张png图片



CSDN @愚公搬代码

2.binwalk

winhex和Stegsolve看不出问题，上binwalk

```
binwalk e4103617b4a6476fb7aa8f862f2ee400.png  
binwalk -e e4103617b4a6476fb7aa8f862f2ee400.png
```

```

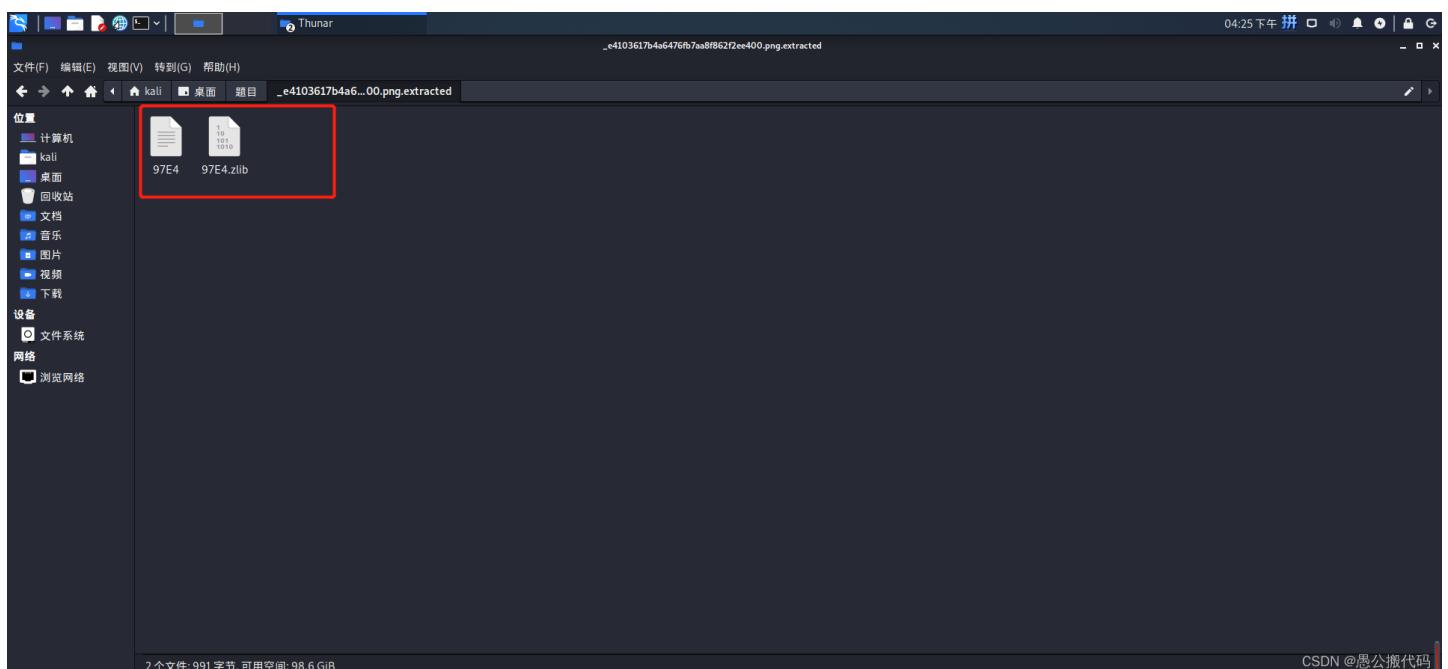
文件 动作 编辑 查看 帮助 帮助
(kali㉿kali)-[~/桌面/题目]
$ binwalk e4103617b4a6476fb7aa8f862f2ee400.png.extracted
DECIMAL      HEXADECIMAL      DESCRIPTION
0             0x0              JPEG image data, JFIF standard 1.01
38884        0x97E4           Zlib compressed data, default compression
97E4          97E4.zlib

(kali㉿kali)-[~/桌面/题目]
$ binwalk -e e4103617b4a6476fb7aa8f862f2ee400.png
DECIMAL      HEXADECIMAL      DESCRIPTION
0             0x0              JPEG image data, JFIF standard 1.01
38884        0x97E4           Zlib compressed data, default compression

```

CSDN @愚公搬代码

得到



打开文件得到

```
S1ADBBQAAQAAADkwI0xs4x98WgAAAEE4AAAAEAAAAY29kZePegfAPrkdnhMG2gb86/AHHpS0GMqCrR9s21bP43SqmesL+oQGo501jz4zIctqxIsTH
V25+1mTE7vFc9gl5IUif7f1/rHIpHq17nqKPb+2M6nRLuhU8mb/w1BLAQI/ABQAAQAAADkwI0xs4x98WgAAAEE4AAAAEACQAAAAAAAAIAAAAAAA
AABjb2R1CgAgAAAAAAABAgAAFvDg4Xa0wE8gAmth9rTATyACa2H2tMBUEsFBgAAAAABAAEAVgAAAHwAAADcAFtQeXRob24gMi43XQ0KPj4+IKh9
qH2ofQ0KDQpUcmFjZWJhY2sgKG1vc3QgcmVjZW50IGNhbGwgbGFzdCk6DQogIEZpbGUgIjxweXNoZWxsIzA+IiwegbGluZSAxLCBpbIA8bW9kdWx1
Pg0KICAgIKh9qH2ofQ0KwVmVyb0RpdmIzaW9uRXJyb3I6IKh9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofah9
qH2ofah9qH2ofSA8LSBwYXNzd29yZCA7KQ0KPj4+IAA=
```

3.python脚本

```

import base64

t = "S1ADBBQAAQAAADkwI0xs4x98WgAAAE4AAAAEAAAAY29kZePegfAPrkdnhMG2gb86/AHHpS0GMqCrR9s21bP43SqmesL+oQGo50ljz4zIctq
xIsTHV25+1mTE7vFc9g15IUif7f1/rHIpHq17nqKPb+2M6nRLuhU8mb/w1BLAQI/ABQAAQAAADkwI0xs4x98WgAAAE4AAAAEACQAAAAAAIAA
AAAAAAABjb2R1CgAgAAAAAABgAAFvDg4Xa0wE8gAmth9rTATyACa2H2tMBUEsFBgAAAAABAAEVgAAAHwAAADcAFtQeXRob24gMi43XQ0KPj4
+IKh9qH2ofQ0KDQpUcmfjZWJhY2sgKG1vc3QgcmVjZW50IGNhbGwgbGFzdCk6DQogIEZpbGUgIjxweXNoZWxsIzA+IiwgbGluZSAxLCBpbIA8bw9
kdWxlPg0KICAgIKh9qH2ofQ0KwlmVyb0Rpdm1zaW9uRXJyb3I6IKh9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2
ofah9qH2ofah9qH2ofSA8LSBwYXNzd29yZCA7KQ0KPj4+IAA="

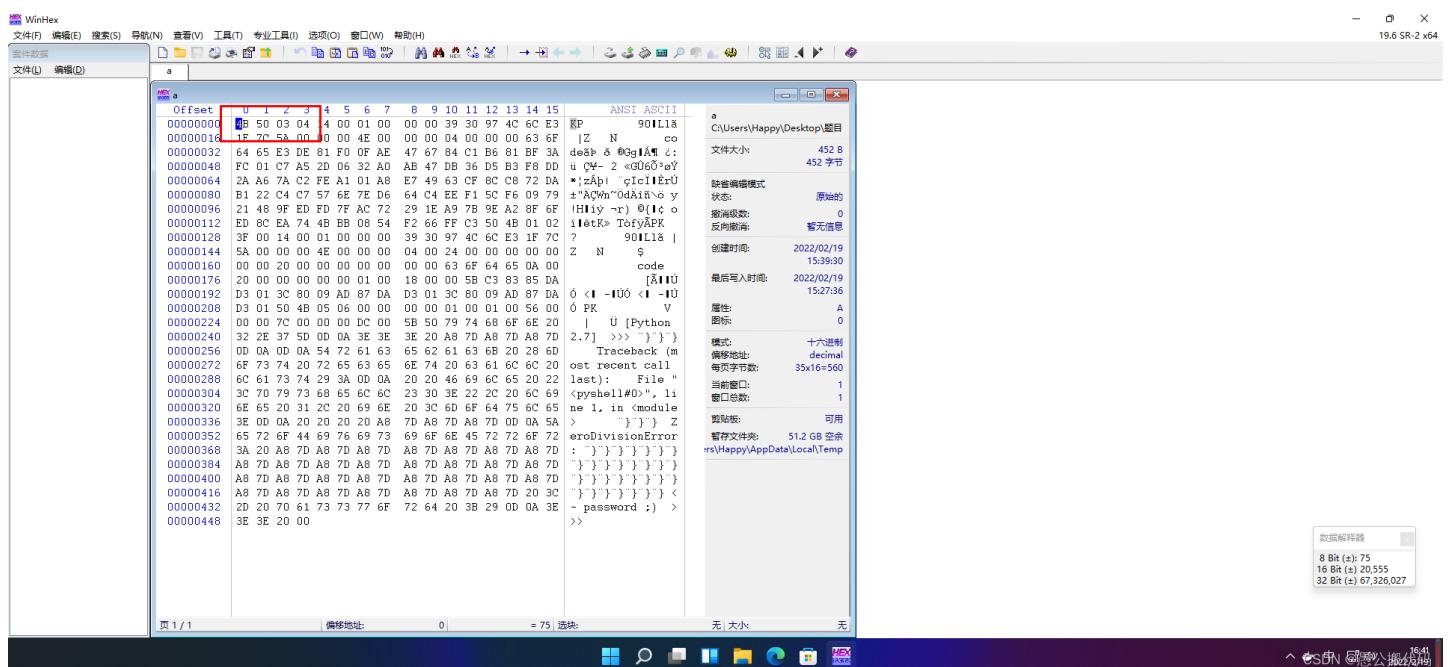
a = base64.b64decode(t)
with open('a', "bw") as f:
    f.write(a)
    f.close()

```

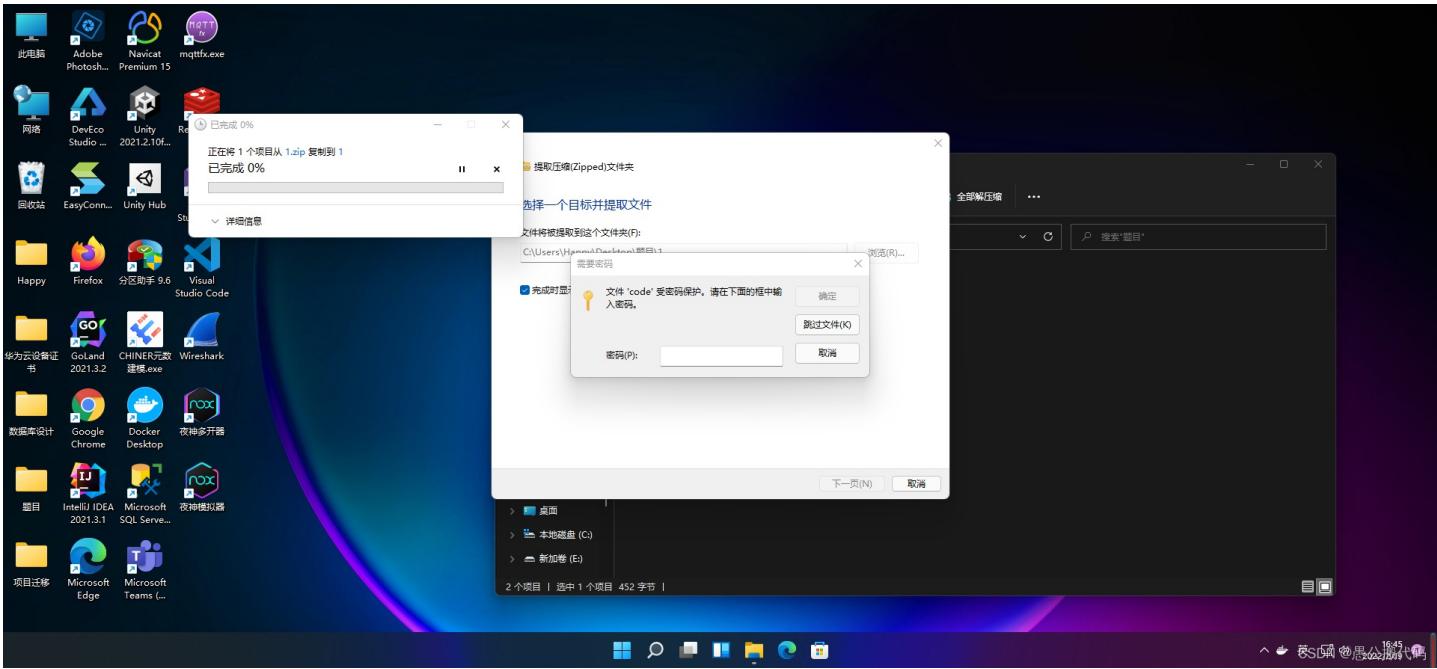
得到解压文件

4.winhex

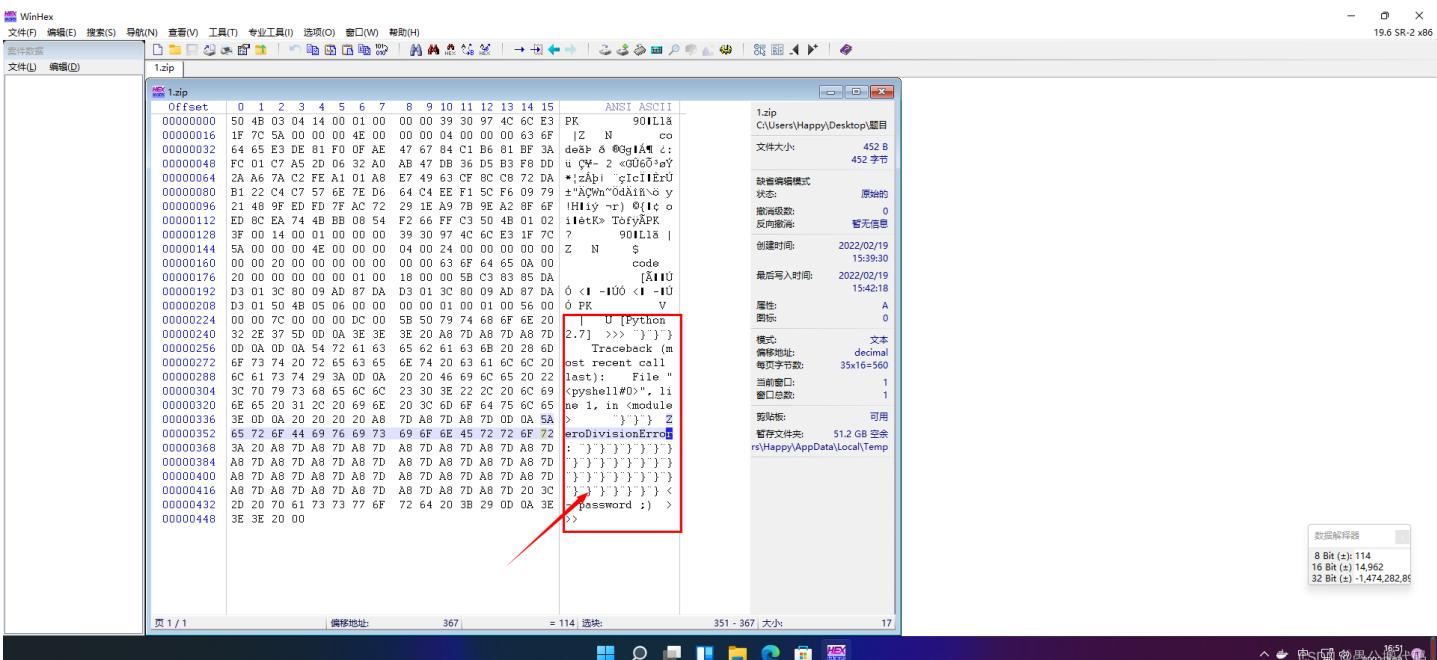
用winhex打开文件、发现开头变成4b 50 03 04改成50 4b 03 04后文件后缀改成zip格式



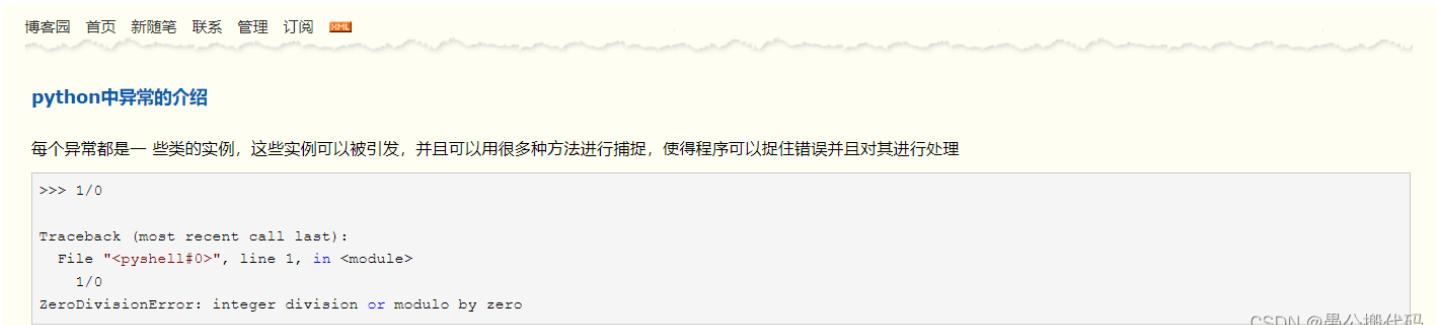
解压文件，发现需要密码



根据提示，密码是py2.7的一个报错提示



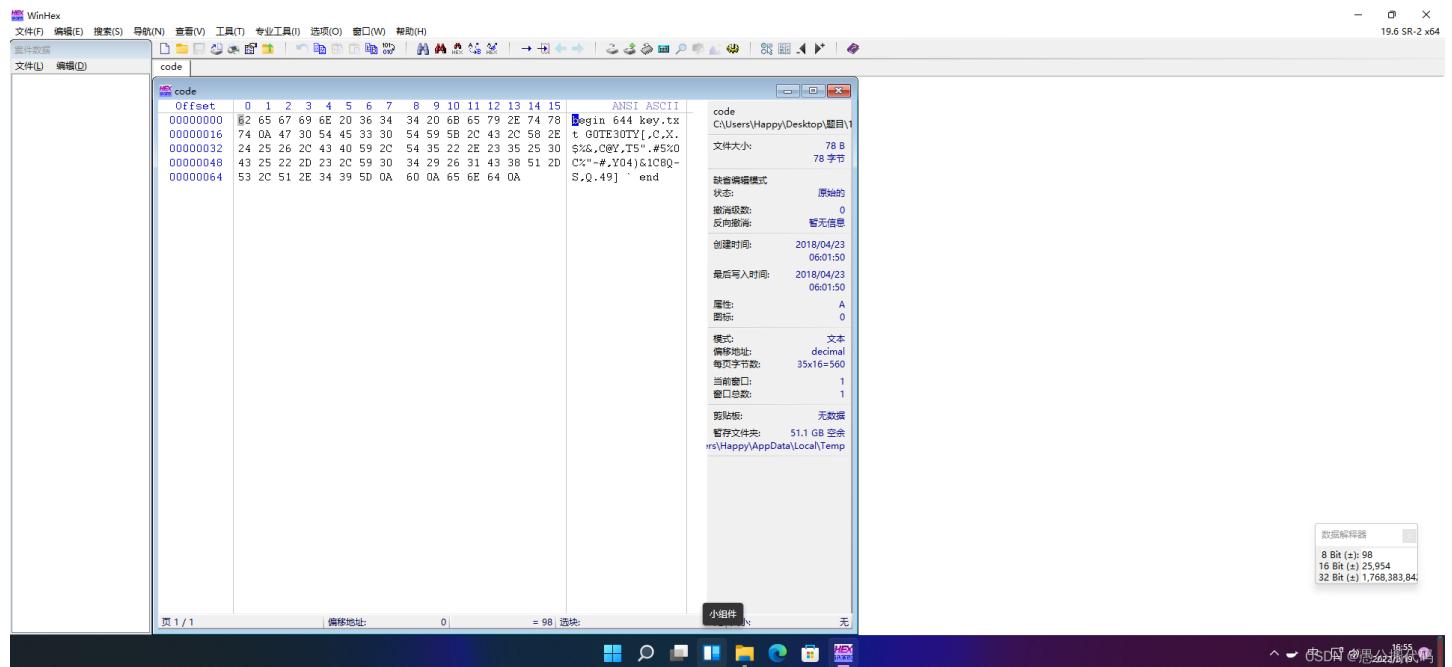
经过百度，得知该提示为 `integer division or modulo by zero`



输入 `integer division or modulo by zero` 解压得到加密过的字符串

winhex打开解密后的code文件

得到: `GOTE30TY[,C,X.$%&,C@Y,T5".#5%0C%"-#,Y04)&1C8Q-S,Q.49]`



5.UUencode

这是UUencode编码进行解密网址: <https://www.qqxiuzi.cn/bianma/uuencode.php>

The screenshot shows a web-based tool for decoding uuencoded files. It has tabs for '加密' (Encrypt) and '解密' (Decrypt). The '解密' tab is active. In the input field, the encoded string `GOTE30TY[,C,X.$%&,C@Y,T5".#5%0C%"-#,Y04)&1C8Q-S,Q.49]` is pasted. Below the input field, the decoded output is shown: `CISCN{2388AF2893EB85EB1B439ABFF617319F}`. The bottom right corner of the page includes a watermark: 'CSDN @愚公搬代码'.

得到flag: `CISCN{2388AF2893EB85EB1B439ABFF617319F}`

总结

- binwalk
- python
- winhex
- UUencode