**题目名称：加密的压缩包**

**类型：Misc**

**介绍：**

本题考查CTF Misc分类的压缩包CRC32爆破。

详细介绍链接：<https://wiki.x10sec.org/misc/archive/zip-zh/#crc32>

原理 [¶](https://wiki.x10sec.org/misc/archive/zip-zh/#_4)

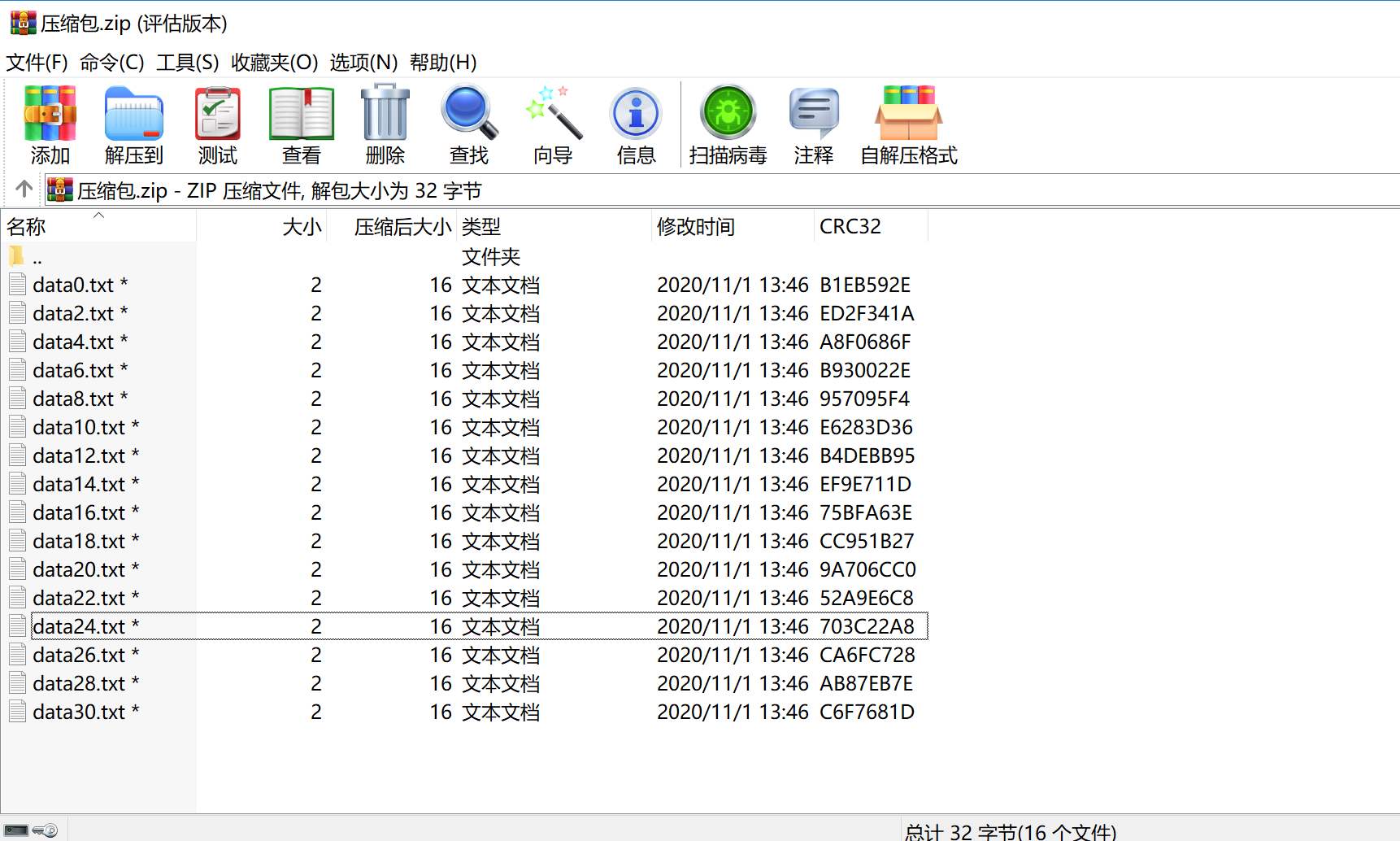
CRC 本身是「冗余校验码」的意思，CRC32 则表示会产生一个 32 bit ( 8 位十六进制数) 的校验值。由于 CRC32 产生校验值时源数据块的每一个 bit (位) 都参与了计算，所以数据块中即使只有一位发生了变化，也会得到不同的 CRC32 值。

CRC32 校验码出现在很多文件中比如 png 文件，同样 zip 中也有 CRC32 校验码。值得注意的是 zip 中的 CRC32 是未加密文件的校验值。

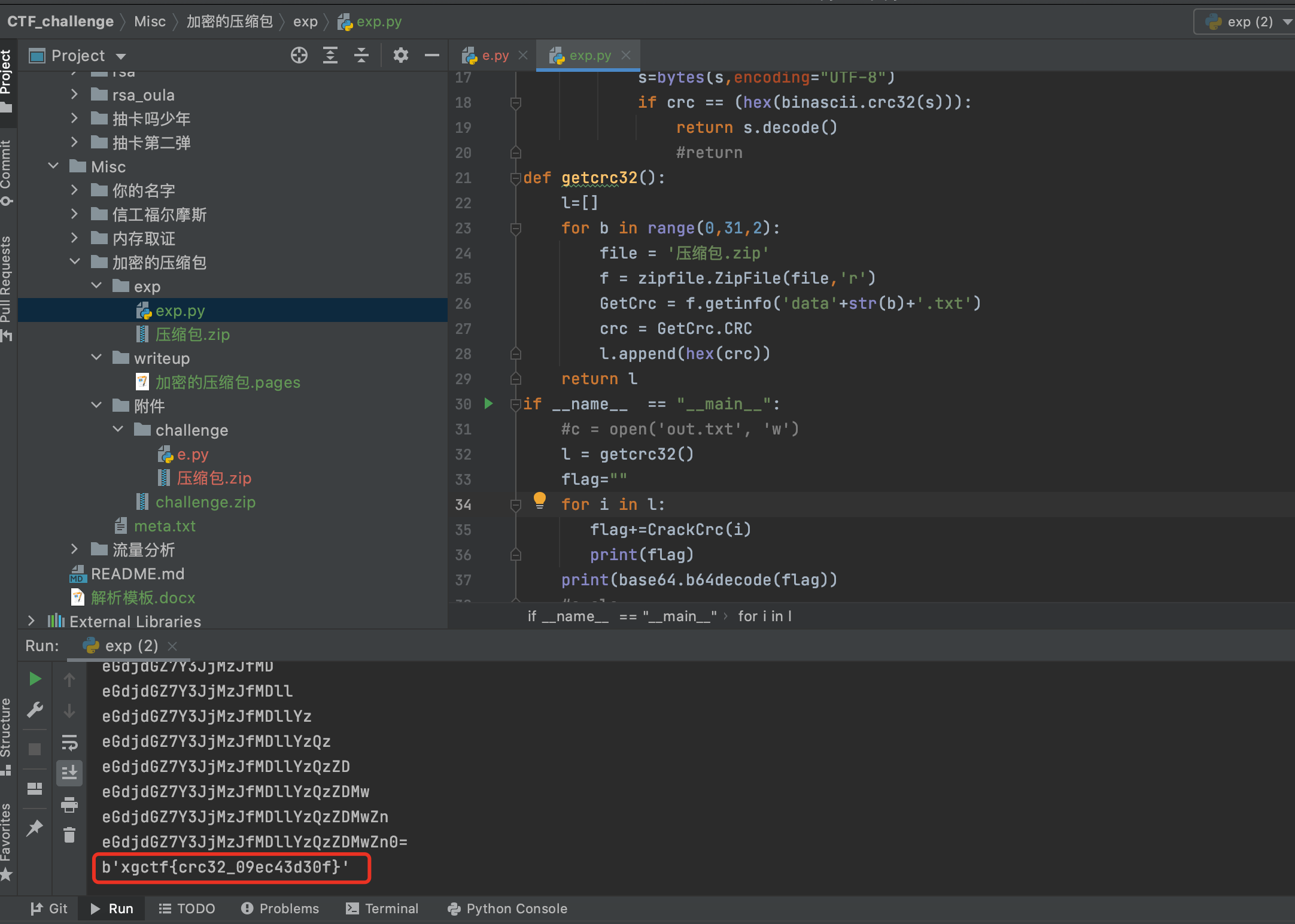
这也就导致了基于 CRC32 的攻击手法。

* 文件内内容很少 (一般比赛中大多为 4 字节左右)
* 加密的密码很长

**解题步骤：**

**第一步：**题目给出脚本如下，分析压缩包中的文件内容为flag，且每个文件存储两位数据

**第二步：**根据CRC原理，爆破文件内容令其压缩后的CRC32值相同即可。



**简要总结：**在加密压缩文本内容时，文本内容很少的情况下存在爆破泄露数据的风险。