

攻防世界 Crypto高手进阶区 3分题 fanfie

原创

思源湖的鱼  于 2020-12-12 14:55:19 发布  264  收藏

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [crypto](#)

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/weixin_44604541/article/details/111059888

版权

CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的3分题

本篇是fanfie的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

得到一串字符

```
MZYVMIWLGBL7CIJOGJQVOA3IN5BLYC3NHI
```

瞅着像base64

尝试下无果

这就抓瞎了

查了查

原题有提示

标志被转换为base32并以某种方式加密

又最后的flag是 `BITSCTF{***}` 的形式

所以对 `BITSCTF` 进行Base32加密

```
IJEVIU2DKRDA=====
```

两者放在一起对比下

```
MZYVMIWLGBL7CIJOGJQVOA3IN5BLYC3NHI
IJEVIU2DKRDA=====
```

发现是对应的

也就是仿射密码

理一理得到密码表

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	2	3	4	5	6	7
4	17	30	11	24	5	18	31	12	25	6	19	0	13	26	7	20	1	14	27	8	21	2	15	28	9	22	3	16	29	10	23
E	R	6	L	Y	F	S	7	M	Z	G	T	A	N	2	H	U	B	O	3	I	V	C	P	4	J	W	D	Q	5	K	X

于是

```
MZYVMIWLGBL7CIJOGJQVOA3IN5BLYC3NHI
->
IJEVIU2DKRDHWUZSKZ4VSM TUN5RDEWTNPU
```

再进行base32解密

得到 `BITSCTF{S2VyY2tob2Zm}`

结语

攻防世界少了提示就很抓瞎