攻防世界 Crypto高手进阶区 4分题 cr2-many-time-secrets

原创

思源湖的鱼 于 2020-12-25 14:52:46 发布 221 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 crypto xor加密

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111679437

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的4分题

本篇是cr2-many-time-secrets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

得到一串十六进制

```
0529242a631234122d2b36697f13272c207f2021283a6b0c7908
2f28202a302029142c653f3c7f2a2636273e3f2d653e25217908
322921780c3a235b3c2c3f207f372e21733a3a2b37263b313012
2f6c363b2b312b1e64651b6537222e37377f2020242b6b2c2d5d
283f652c2b31661426292b653a292c372a2f20212a316b283c09
29232178373c270f682c216532263b2d3632353c2c3c2a293504
613c37373531285b3c2a72273a67212a277f373a243c20203d5d
243a202a633d205b3c2d3765342236653a2c7423202f3f652a18
2239373d6f740a1e3c651f207f2c212a247f3d2e65262430791c
263e203d63232f0f20653f207f332065262c3168313722367918
2f2f372133202f1426652126372222220733e383f2426386b
```

第一反应

ascii码

2f6c363b2b312b1e64651b6537222e37377f2020242b6b2c2d5d
283f652c2b31661426292b653a292c372a2f20212a316b283c09
29232178373c270f682c216532263b2d3632353c2c3c2a293504
613c37373531285b3c2a72273a67212a277f373a243c20203d5d
243a202a633d205b3c2d3765342236653a2c7423202f3f652a18
2239373d6f740a1e3c651f207f2c212a247f3d2e65262430791c
263e203d63232f0f20653f207f332065262c3168313722367918
2f2f372133202f1426652126372222207 33e383f2426386b

□)$*c□4□-+6i □', !
(:ky□□□□□□B□S□□□cbs□□□S□R□□□2)!x:#
[<,?
7.!s::+7&;10□□□□c□□□□FQ□Sr"□sw□□□B□□□□
(?e,+1f□&)+e:),7*/ !*1k(< □
□2□□s□p□□□□S"c□□c#S□□ç□P□a<7751([<*r':g!*'
7:$<
=]□C□□□3□□□□□vSB#fS□□B2□□□R□□"97=ot
□<e□
,.!*$ =.e&$0y□□c□□□22□□□S□□□2□Rb□□□□r#g□
□//7!3 /□&e!&7"" s>8?$&8k

一堆乱码

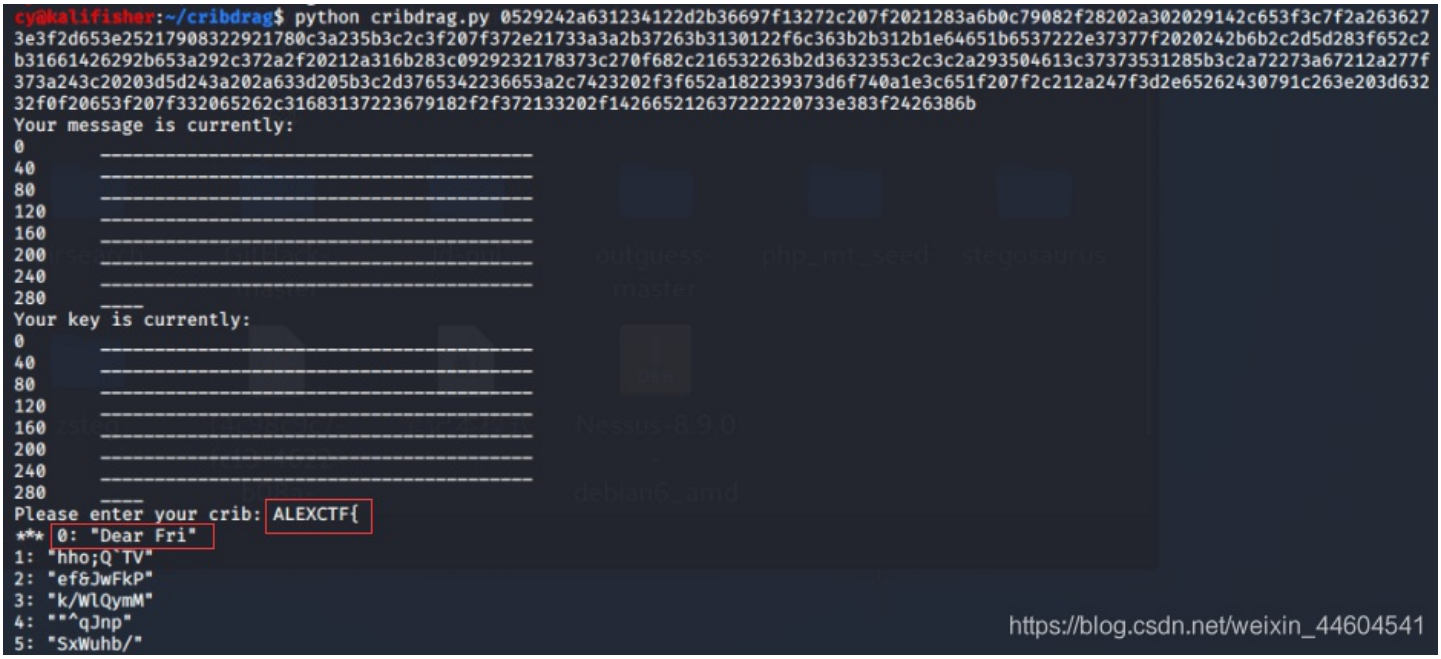
查了查

是OTP 密钥重用

加密101-异或（xor）

工具

https://github.com/SpiderLabs/cribdrag



如是寻找合理的一步步下去

最终的得到flag：`ALEXCTF{HERE_GOES_THE_KEY}AL`

结语

参考

- ALEXCTF CR2: MANY TIME SECRETS

知识点

- 多字节XOR加密方式
- 加密101-异或（xor）
- 工具：https://github.com/SpiderLabs/cribdrag