BuuCTF难题详解| Misc | [ACTF新生赛2020]剑龙

原创

水星Sur 于 2020-09-15 16:15:15 发布 990 收藏 1

分类专栏： BUUCTF Misc 文章标签： 安全

本文链接：https://blog.csdn.net/pone2233/article/details/108601733

BUUCTF 同时被 2 个专栏收录

21 篇文章 2 订阅

订阅专栏

Misc

22 篇文章 0 订阅

订阅专栏

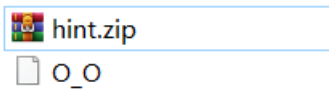
栏目介绍

难度简单，这题目提示给的很明显

BuuCTF难题详解| Misc | [ACTF新生赛2020]剑龙

P1：

他给了



2个文件解压，我们从o_o上面找不到东西，我们先解开zip

P2：

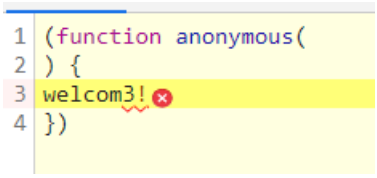
我们先打开pwd看看发现是js加密一种

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
□ω□□= / ｀m´) □ ~ㅗㅗ  //*´∇ ｀*/ ['_']; o=(□□□)  =_=3; c=(□Θ□) =(□□□)-(□□□); (□Д□) =(□Θ□)= (o^_^o)/ (o^_^o);(□Д□)={□Θ□: '_' ,□ω□□ : ((□ω□□==3) +'_') [□Θ□] ,□□□□ :(□ω□□+ '_')[o^_^o -(□Θ□)] ,□Д□□:((□□□==3) +'_')[□□□] }; (□Д□) [□Θ□] =((□ω□□==3) +'_') [c^_^o];(□Д□) ['c'] = ((□Д□)+'_') [ (□□□)+(□□□)-(□Θ□) ];(□Д□) ['o'] = ((□Д□)+'_') [□Θ□];(□o□)=(□Д□) ['c']+(□Д□) ['o']+(□ω□□ +'_')[□Θ□]+ ((□ω□□==3) +'_') [□□□] + ((□Д□) +'_') [(□□□)+(□□□)]+ ((□□□==3) +'_') [□Θ□]+((□□□==3) +'_') [(□□□) - (□Θ□)]+(□Д□) ['c']+((□Д□)+'_') [(□□□)+(□□□)]+ (□Д□) ['o']+((□□□==3) +'_') [□Θ□];(□Д□) ['_'] =(o^_^o) [□o□] [□o□];(□ε□)=((□□□==3) +'_') [□Θ□]+ (□Д□) .□Д□□+((□Д□)+'_') [(□□□) + (□□□)]+((□□□==3) +'_') [o^_^o -□Θ□]+((□□□==3) +'_') [□Θ□]+ (□ω□□ +'_') [□Θ□]; (□□□)+=(□Θ□); (□Д□)[□ε□]='\\'; (□Д□).□Θ□□=(□Д□+ □□□)[o^_^o -(□Θ□)];(o□□□o)=(□ω□□ +'_')[c^_^o];(□Д□) [□o□]='\"';(□Д□) ['_'] ( (□Д□) ['_'] (□ε□+(□Д□)[□o□]+ (□Д□)[□ε□]+(□Θ□)+ ((o^_^o) +(o^_^o))+ ((□□□) + (o^_^o))+ (□Д□)[□ε□]+(□Θ□)+ (□□□)+ ((□□□) + (□Θ□))+ (□Д□)[□ε□]+(□Θ□)+ (□□□)+ (□Д□)[□ε□]+(□Θ□)+ ((□□□) + (□Θ□))+ ((□□□) + (o^_^o))+ (□Д□)[□ε□]+(□Θ□)+ ((□□□) + (□Θ□))+ ((□□□) + (□Θ□))+ (□Д□)[□ε□]+((o^_^o) +(o^_^o))+ (o^_^o)+ (□Д□)[□ε□]+(□□□)+ (□Θ□)+ (□Д□)[□o□]) (□Θ□)) ('_');
```


我们放在控制台输入就行

得到了密码



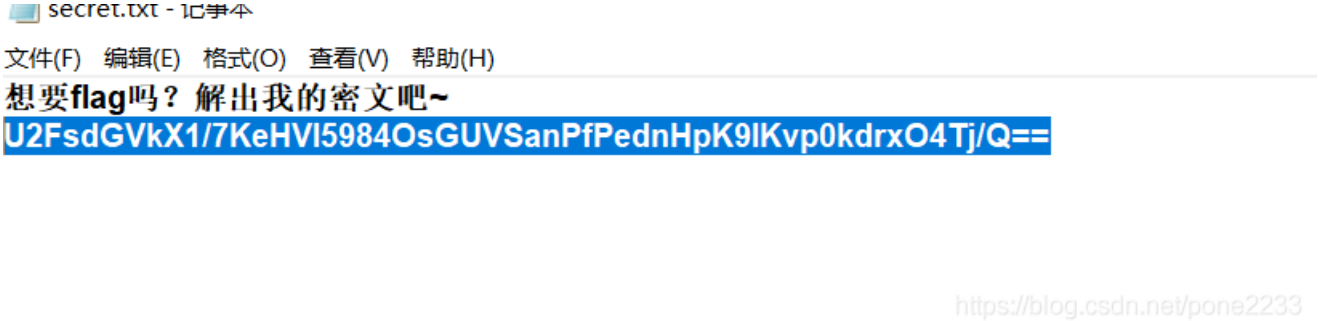
> welcom3!

我们接下看图片，有密码就知道了这个加密是**[隐写方案]steghide**

这个隐写我们破解一下

```
C:\Users\Administrator>E:\桌面\CTF工具包\[隐写工具]steghide\steghide.exe extract -sf E:\桌面\暑期CTF\9-15\剑龙\tmp\www\h
h.jpg
Enter passphrase:
the file "secret.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "secret.txt".
```

然后在打开这个文件看一下



我们就获得了密文密钥是在图片属性里面

> 密文：U2FsdGVkX1/7KeHVl5984OsGUVSanPfPednHpK9lKvp0kdrxO4Tj/Q==
> 密钥：@#)

解开 送上网址：https://www.sojson.com/encrypt_des.html

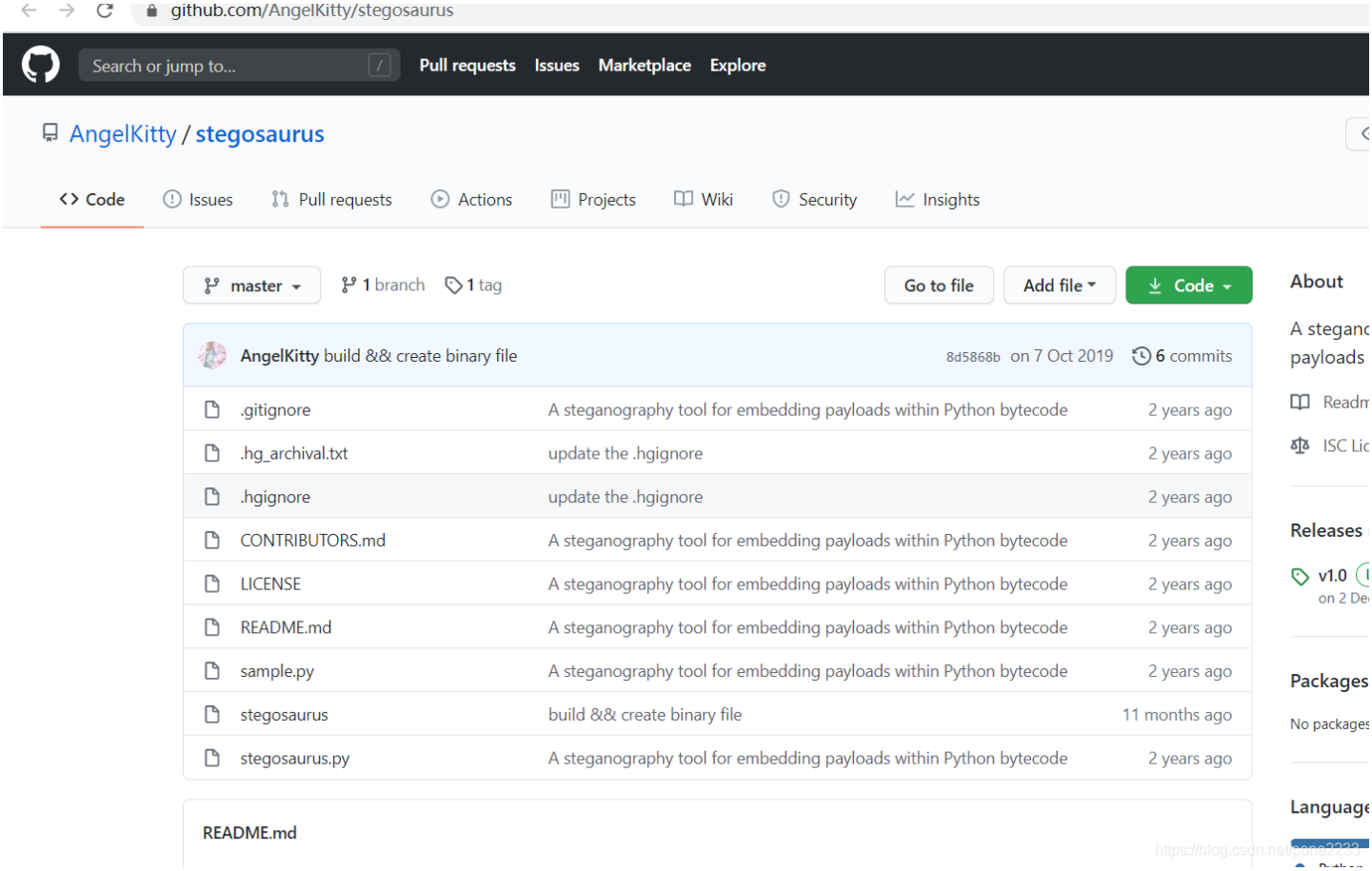
P3：

他和我们说是

think about stegosaurus

这个加密

就去github上面找，送上网址：https://github.com/AngelKitty/stegosaurus



python3 stegosaurus.py -x O_O.pyc

记得提前改一下文件的后缀名呦

脚本跑一下就有了

```
E:\桌面\CTF工具包\[隐写工具]steghide>python3 E:\桌面\CTF工具包\[剑龙隐写pyc]stegosaurus-master\stegosaurus.py -x E:\桌面
\CTF工具包\[剑龙隐写pyc]stegosaurus-master\O_O.pyc
Extracted payload: flag{3teg0Sauru3_!1}
```

Extracted payload: flag{3teg0Sauru3_!1}

这里知识点就是，大家要知道这个剑龙加密stegosaurus

是只能对

```
E:\桌面\CTF工具包\[隐写工具]steghide>python3 E:\桌面\CTF工具包\[剑龙隐写pyc]stegosaurus-master\stegosaurus.py -x
\暑期CTF\9-15\剑龙\tmp\www\O_O
Fatal error: Carrier file must be one of the following types: {'.pyc', '.pyo', '.py'}, got:
Use -h or --help for usage
```

pyc pyo py文件才有用的