

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](#)

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/pone2233/article/details/108601733>

版权



[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:



hh.jpg

pwd.txt

https://blog.csdn.net/pone2233

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') □ ~!+ // *'v '*/ ['_']; o=(□□□) =_3; c=(□□□) =(□□□)-(□□□); (□□□) =(□□□) = (o^_^o)/ (o^_^o); (□□□)={□□□: '_ ', □ω□□ : ((
□ω□□==3) +'_') [□□□], □□□□ :(□ω□□+ '_')[o^_^o -(□□□)], □□□□:(□□□□==3) +'_')[□□□□]; (□□□) [□□□] =(□ω□□==3) +'_') [c^_^o]; (□□□)
['c'] = ((□□□+ '_') [ (□□□)+(□□□)-(□□□) ]; (□□□) ['o'] = ((□□□+ '_') [□□□]; (□□□) =(□□□) ['c']+(□□□) ['o']+(□ω□□ +'_')[□□□]+ ((□ω□□==3) +'_')
[□□□] + ((□□□) +'_') [(□□□)+(□□□)]+ ((□□□==3) +'_') [□□□]+((□□□==3) +'_') [(□□□) - (□□□)]+(□□□) ['c']+(□□□+ '_') [(□□□)+(□□□)]+ (□□□)
['o']+(□□□==3) +'_') [□□□]; (□□□) ['_'] =(o^_^o) [□□□] [□□□]; (□□□) =(□□□==3) +'_') [□□□]+ (□□□) .□□□□+(□□□+ '_') [(□□□) + (□□□)]+(□□□)
□□□==3) +'_') [o^_^o -□□□]+((□□□==3) +'_') [□□□]+ (□ω□□ +'_') [□□□]; (□□□)+(□□□); (□□□)[□□□]='\\'; (□□□).□□□□=(□□□+ □□□)[o^_^o -(□
□□□)]; (o□□□□) =(□ω□□ +'_')[c^_^o]; (□□□) [□□□]='\\'; (□□□) ['_'] ( (□□□) ['_'] (□□□)+(□□□)[□□□]+ (□□□)[□□□]+(□□□) + ((o^_^o) + (o^_^o)) + ((□
□□□) + (o^_^o)) + (□□□)[□□□]+(□□□) + (□□□) + ((□□□) + (□□□)) + (□□□)[□□□]+(□□□) + ((□□□) + (□□□)) + (□□□) + (□□□)[□□□]+(□□□) + (□□□) +
(o^_^o) + (□□□)[□□□]+(□□□) + ((□□□) + (□□□)) + ((□□□) + (o^_^o)) + (□□□)[□□□]+(□□□) + ((□□□) + (□□□)) + ((□□□) + (□□□)) + (□□□)[□
□□□]+((o^_^o) + (o^_^o)) + (o^_^o) + (□□□)[□□□]+(□□□) + (□□□) + (□□□)[□□□] (□□□) ('_');

```

https://blog.csdn.net/pone2233

我们放在控制台输入就行

```

MyDy1KX/7BYTt0n1kU0w8b+Zbz1q-gig0wVAM9q8= Note that 'style-src-elem' was not explicitly set, so 'style-src' is used as a fallback.
> 'w' / '^m') / ~!+ // *'v '*/ ['_']; o=(□□□) =_3; c=(□□□) =(□□□)-(□□□); (□□□) =(□□□) = (o^_^o)/ (o^_^o); (□□□)={□□□: '_ ', □ω□□ : ((
□ω□□==3) +'_') [□□□], □□□□ :(□ω□□+ '_')[o^_^o -(□□□)], □□□□:(□□□□==3) +'_')[□□□□]; (□□□) [□□□] =(□ω□□==3) +'_') [c^_^o]; (□□□)
['c'] = ((□□□+ '_') [ (□□□)+(□□□)-(□□□) ]; (□□□) ['o'] = ((□□□+ '_') [□□□]; (□□□) =(□□□) ['c']+(□□□) ['o']+(□ω□□ +'_')[□□□]+ ((□ω□□==3) +'_')
[□□□] + ((□□□) +'_') [(□□□)+(□□□)]+ ((□□□==3) +'_') [□□□]+((□□□==3) +'_') [(□□□) - (□□□)]+(□□□) ['c']+(□□□+ '_') [(□□□)+(□□□)]+ (□□□)
['o']+(□□□==3) +'_') [□□□]; (□□□) ['_'] =(o^_^o) [□□□] [□□□]; (□□□) =(□□□==3) +'_') [□□□]+ (□□□) .□□□□+(□□□+ '_') [(□□□) + (□□□)]+(□□□)
□□□==3) +'_') [o^_^o -□□□]+((□□□==3) +'_') [□□□]+ (□ω□□ +'_') [□□□]; (□□□)+(□□□); (□□□)[□□□]='\\'; (□□□).□□□□=(□□□+ □□□)[o^_^o -(□
□□□)]; (o□□□□) =(□ω□□ +'_')[c^_^o]; (□□□) [□□□]='\\'; (□□□) ['_'] ( (□□□) ['_'] (□□□)+(□□□)[□□□]+ (□□□)[□□□]+(□□□) + ((o^_^o) + (o^_^o)) + ((□
□□□) + (o^_^o)) + (□□□)[□□□]+(□□□) + (□□□) + ((□□□) + (□□□)) + (□□□)[□□□]+(□□□) + ((□□□) + (□□□)) + (□□□) + (□□□)[□□□]+(□□□) + (□□□) +
(o^_^o) + (□□□)[□□□]+(□□□) + ((□□□) + (□□□)) + ((□□□) + (o^_^o)) + (□□□)[□□□]+(□□□) + ((□□□) + (□□□)) + ((□□□) + (□□□)) + (□□□)[□
□□□]+((o^_^o) + (o^_^o)) + (o^_^o) + (□□□)[□□□]+(□□□) + (□□□) + (□□□)[□□□] (□□□) ('_');

```

得到了密码

```

1 (function anonymous(
2 ) {
3   welcom3!
4 })

```

welcom3!

我们接着看图片，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\hh.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

secret.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

想要flag吗？解出我的密文吧~

U2FsdGVkX1/7KeHVI5984OsGUVSanPfPednHpK9IKvp0kdrxO4Tj/Q==

<https://blog.csdn.net/pone2233>

我们就获得了密文密钥是在图片属性里面

hh.jpg 属性

常规 安全 详细信息 以前的版本

| 属性 | 值 |
|----|---|
| 说明 | |
| 标题 | 这里有密钥 |
| 主题 | @#%\$^&%%\$) |
| 分级 | ☆☆☆☆☆ |
| 标记 | https://blog.csdn.net/pone2233 |

密文：U2FsdGVkX1/7KeHVI5984OsGUVSanPfPednHpK9IKvp0kdrxO4Tj/Q==

密钥：@#)

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

加密/解密 AES加密/解密 DES加密/解密 RC4加密/解密 Rabbit加密/解密 TripleDes加密/解密 MD5加/解密 Base64加/解密 Hash加/解密 JS 加密 JS 解密

think about stegosaurus

@#%\$^&%%\$)

密码是可选项，也就是可以不填。

< 解密 加密 >

U2FsdGVkX1/7KeHVI5984OsGUVSanPfPednHpK9IKvp0kdrxO4Tj/Q==

<https://blog.csdn.net/pone2233>

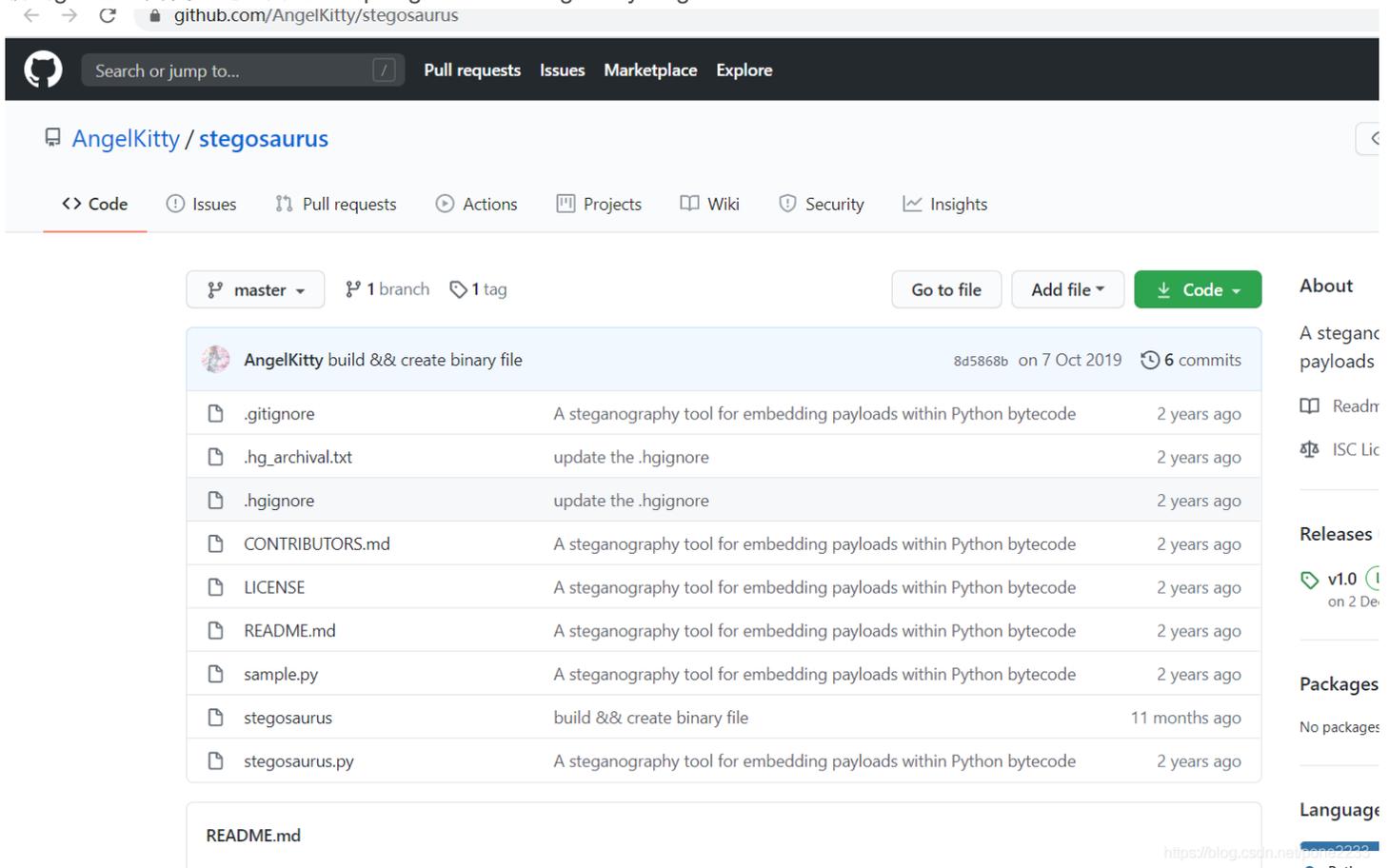
P3:

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>



AngelKitty / stegosaurus

<> Code Issues Pull requests Actions Projects Wiki Security Insights

master 1 branch 1 tag Go to file Add file Code

| File Name | Description | Last Commit |
|------------------|--|---------------|
| .gitignore | A steganography tool for embedding payloads within Python bytecode | 2 years ago |
| .hg_archival.txt | update the .hgignore | 2 years ago |
| .hgignore | update the .hgignore | 2 years ago |
| CONTRIBUTORS.md | A steganography tool for embedding payloads within Python bytecode | 2 years ago |
| LICENSE | A steganography tool for embedding payloads within Python bytecode | 2 years ago |
| README.md | A steganography tool for embedding payloads within Python bytecode | 2 years ago |
| sample.py | A steganography tool for embedding payloads within Python bytecode | 2 years ago |
| stegosaurus | build && create binary file | 11 months ago |
| stegosaurus.py | A steganography tool for embedding payloads within Python bytecode | 2 years ago |

README.md

https://blog.csdn.net/qq_32222222

```
python3 stegosaurus.py -x O_O.pyc
```

记得提前改一下文件的后缀名哟

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_0.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_0
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



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)